DIMITRI MOUTON

Préface d'Alain Bobant, président de la FNTC





Sécurité de la dématérialisation

De la signature électronique au coffre-fort numérique, une démarche de mise en œuvre

Copyright © 2012 Eyrolles.

EYROLLES

Sécurité de la dématérialisation



L'auteur

Ingénieur de Télécom Paris, **Dimitri Mouton** a été chef de projet au laboratoire Sécurité des services et des réseaux de France Télécom R&D. Concepteur d'Applatoo, premier logiciel de signature électronique certifié par l'ANSSI (services du premier ministre), il rejoint en 2003 Achatpublic.com dont il conçoit l'infrastructure de confiance, et qui devient en un an la plate-forme de dématérialisation des marchés publics de référence. Directeur R&D de CertEurope de 2006 à 2008, il crée son cabinet de conseil **Demaeter** en 2009 pour réaliser des missions d'assistance à maîtrise d'ouvrage auprès de grandes collectivités publiques et d'assistance à la R&D auprès de PME innovantes. Il est également expert indépendant en solutions de vote par Internet. Il anime auprès de la **Fédération Nationale des Tiers de Confiance** (FNTC) les groupes de travail «identité numérique et signature électronique», «e-vote» et «e-traçabilité».

demæter
tout se transforme

À qui s'adresse ce livre ?

- Aux directions informatiques (DSI), architectes du SI, responsables sécurité (RSSI) ;
- Aux experts de la gouvernance des SI ;
- Aux directeurs Recherche et développement ;
- Aux architectes fonctionnels et techniques ;
- Aux consultants, assistants à maîtrise d'ouvrage ou à maîtrise d'œuvre ;
- À tous les concepteurs d'applications de dématérialisation confrontés à la mise en œuvre de la sécurité, tant dans des administrations et grandes entreprises qu'au sein de PME innovantes.

Le guide incontournable du concepteur d'applications dématérialisées. En s'appuyant sur les textes et normes en vigueur et au travers d'exemples concrets, cet ouvrage détaille les mécanismes de sécurité indispensables aux applications web, ainsi que les méthodologies projet destinées à leur mise en œuvre, tant sous leurs aspects techniques et applicatifs que juridiques et comportementaux. Après avoir rigoureusement défini confiance et sécurité, puis détaillé les mécanismes de cryptographie qui sous-tendent la sécurisation des services, l'auteur décrit les fonctionnalités à déployer dans tout projet de dématérialisation : l'identité numérique et le contrôle d'accès, le certificat, la confidentialité, la signature électronique et le cachet, la traçabilité et l'horodatage, le coffre-fort électronique et l'archivage.

Une mise en perspective essentielle sur la dématérialisation. Grâce à de nombreux témoignages d'experts de la dématérialisation, le livre développe la nécessité de faire naître la confiance des utilisateurs pour promouvoir les usages et précise le rôle des tiers de confiance dans la chaîne de la dématérialisation, dont il rappelle les bases juridiques, telle la convention de preuve qui donne leur valeur aux échanges et aux documents.

Au sommaire

Traitement automatisé des données et suppression du papier. Sécurité technique et sécurité juridique. **Le RGS.** Les bases techniques de la cryptographie. Confiance et tiers de confiance. L'identité numérique. **Authentification faible et authentification forte.** Mot de passe à usage unique. SSL. Attaques et parades. Man in the middle. SSO. Fédération d'identités. **Certificat :** carte d'identité numérique. Chaîne de certification. **PKI.** Autorité de certification. Conserver et transmettre des secrets. Anonymisation. **Signature électronique** et signature manuscrite. Cachet et scellement électronique. **Horodatage. Traçabilité.** Tracer, conserver et certifier les données. Vote par Internet, jeux en ligne, marchés publics dématérialisés, e-commerce, e-gouvernement. **Coffre-fort électronique.** Archivage. **Convention de preuve. Mener un projet de dématérialisation.**

Copyright © 2012 Eyrolles.

Code éditeur : G13418
ISBN : 978-2-212-13418-6

www.editions-eyrolles.com

Sécurité de la dématérialisation

De la signature électronique au coffre-fort numérique, une démarche de mise en œuvre

Copyright © 2012 Eyrolles.

Chez le même éditeur

Dans la collection Solutions d'entreprise

A. Fernandez-Toro. – **Management de la sécurité de l'information.** N°12697, 2012, 344 pages.

Y. Constantinidis, préface de M. Volle. – **Expression des besoins pour le système d'information**. *L'art de recueillir et formaliser les besoins*. N°12783, 2011, 246 pages.

S. Bohnké. – **Moderniser son système d'information**. *Comprendre la valeur stratégique d'un SI*.
N°12764, 2011, 290 pages environ.

A. Lupfer, préface de H. Schauer (HSC Consultants). – **Gestion des risques en sécurité de l'information**. *Mise en œuvre de la norme ISO 27005*. N°12593, 2010, 232 pages.

E. Besluau. – **Management de la continuité d'activité**. *Assurer la pérennité de l'entreprise : planification, choix techniques et mise en œuvre*
N°12820, 2e édition, 2010, 312 pages.

S. Bordage. – **Conduite de projet web**.
N°13308, 2012, 480 pages.

Dans la collection Blanche

J. Pauli, G. Plessis, C. Pierre de Geyer. – **Audit et optimisation LAMP**.
N°12800, 2012, 300 pages environ.

R. Rimelé. – **HTML 5.** *Une référence pour le développeur web*.
N°12982, 2011, 604 pages.

F. Daoust, D. Hazaël-Massieux. – **Relever le défi du Web mobile.** *Bonnes pratiques de conception et de développement*.
N°12828, 2011, 300 pages.

D. Seguy, P. Gamache. – **Sécurité PHP 5 et MySQL**.
N°13339, 3e édition, 2011, 277 pages.

J. Chable, D. Guignard, E. Robles, N. Sorel. – **Programmation Android.**
N°13303, 2e édition, 2012, 520 pages environ.

J.-M. Defrance. –**Ajax, jQuery et PHP**.
N°13271, 3e édition, 2011, 482 pages.

T. Sarlandie, J.-M. Lacoste. – **Programmation IOS 5 pour iPhone et iPad.**
N°12799, 2e édition, 2012, 350 pages environ.

E. Sarrion. – **jQuery Mobile.** *La bibliothèque JavaScript pour le Web mobile.*
N°13388, 2012, 610 pages.

J. Stark. – **Applications iPhone avec HTML, CSS et JavaScript**. *Conversion en natifs avec PhoneGap.*
N°12745, 2010, 190 pages.

E. Daspet et C. Pierre de Geyer. – **PHP 5 avancé.**
N°13435, 6e édition, 2012, 900 pages environ.

P. Borghino, O. Dasini, A. Gadal. – **Audit et optimisation MySQL 5**.
N°12634, 2010, 282 pages

C. Porteneuve. – **Bien développer pour le Web 2.0**. *Bonnes pratiques Ajax*.
N°12391, 2e édition, 2008, 674 pages.

Autres ouvrages

V. Messager Rota. – **Gestion de projet agile.** *Avec Scrum, Lean, eXtreme Programming…*
N°12750, 3e édition, 2010, 272 pages.

A. Boucher. – **Ergonomie web illustrée**. *60 sites à la loupe*.
N°12695, 2010, 302 pages (Design & Interface).

A. Boucher. – **Ergonomie web**. *Pour des sites web efficaces.*
N°13215, 3e édition, 2011, 356 pages (Accès libre).

I. Canivet. – **Bien rédiger pour le Web**. *Stratégie de contenu pour améliorer son référencement naturel.*
N°12883, 2e édition, 2011, 552 pages (Accès libre).

E. Sarrion – **jQuery & jQuery UI.**
N°12892, 2011, 520 pages (Collection Noire).

M.-V. Blond, O. Marcellin, M. Zerbib. – **Lisibilité des sites web.** *Des choix typographiques au design d'information*.

N°12426, 2009, 326 pages (Accès libre).

E. Sloïm. – **Mémento Sites web.** *Les bonnes pratiques*.
N°12802, 3e édition, 2010, 18 pages.

O. Andrieu. – **Réussir son référencement web.** *Édition 2012*.
N°13396, 4e édition, 2011, 700 pages.

G. Swinnen. – **Apprendre à programmer avec Python 3**.
N°12708, 2e édition, 2010 (Collection Noire).

Copyright © 2012 Eyrolles.

DIMITRI **MOUTON**

Préface d'**Alain Bobant**, président de la FNTC

Sécurité de la dématérialisation

De la signature électronique au coffre-fort numérique, une démarche de mise en œuvre

Copyright © 2012 Eyrolles.

EYROLLES

ÉDITIONS EYROLLES
61, bd Saint-Germain
75240 Paris Cedex 05
www.editions-eyrolles.com

Remerciements à Stéphane Torossian
pour la réalisation des illustrations de l'ouvrage

Copyright © 2012 Eyrolles.

En application de la loi du 11 mars 1957, il est interdit de reproduire intégralement ou partiellement le présent ouvrage, sur quelque support que ce soit, sans l'autorisation de l'Éditeur ou du Centre Français d'exploitation du droit de copie, 20, rue des Grands Augustins, 75006 Paris.
© Groupe Eyrolles, 2012, ISBN : 978-2-212-13418-6

Ce livre est dédié à Alice et Bob.

Copyright © 2012 Eyrolles.

Copyright © 2012 Eyrolles.

Préface

Au fil de l'évolution de ses supports, l'écrit a été valorisé grâce à la compétence et au sérieux des scribes, des secrétaires, des clercs…, intermédiaires éclairés qui l'ont produit, et qui ont contribué à le préserver de la perte ou de la destruction. L'intervention de ces personnes consciencieuses et érudites suscitait un sentiment de sécurité et de confiance dans le public.

Le tsunami planétaire d'Internet et les violentes éruptions technologiques des quinze dernières années, ont provoqué une mutation irréversible des activités humaines au travers de l'émergence de la dématérialisation. Après que le droit a adapté un nouveau cadre juridique au phénomène, la révolution numérique a très rapidement pris de l'ampleur, s'imposant à tous irrésistiblement.

La dématérialisation de l'écrit s'est organisée autour de la mise en place d'un assortiment de processus et d'outils destiné à satisfaire les critères d'une sécurité absolue. C'est ainsi que la confiance s'est dissociée de l'élément humain qui la véhiculait, pour se raccorder aux instruments techniques que nous forgeons sans relâche.

Dimitri Mouton porte un regard expert sur cette dynamique du futur.

Son analyse méthodique, aiguisée et pertinente, clarifie le sujet.

Il nous incite à prendre le temps d'une réflexion sur la « technologisation » de la société.

Tandis que la machine à fabriquer les rêves tourne à plein régime, il est trop tôt pour savoir si nous pourrons supporter l'accélération du rythme des cycles technologiques et le raccourcissement des mutations sociétales qui en résultent. Mais il n'est pas trop tard pour s'alarmer du fait que l'homme paraît vouloir figurer désormais en simple filigrane dans la page numérique qu'il vient d'ouvrir.

Devons-nous concéder aux seuls mécanismes techniques le soin d'assumer l'énorme exigence de confiance que la dématérialisation requiert, ou tenter de rééquilibrer le rôle de l'humain dans leur mise en œuvre ?

La Fédération nationale des tiers de confiance (FNTC) s'investit aux côtés de ceux qui s'appliquent à résoudre les défis du XXIe siècle issus de ces

Copyright © 2012 Eyrolles.

bouleversements. Elle présente l'originalité de réunir dans le même cénacle des fournisseurs de solutions technologiques de sécurité, reconnus pour leur compétence, et des vecteurs traditionnels de la confiance, porteurs institutionnels des valeurs de neutralité, de pérennité et de légitimité.

En associant la multiplicité des talents, des aptitudes, des savoir-faire et des expériences de ces nouveaux « intermédiaires éclairés », la FNTC peut favoriser fortement l'essor d'une « dématérialisation en toute confiance », et permettre à l'homme de demeurer maître de son destin.

Alain Bobant

Huissier de justice

Président de la Fédération nationale des tiers de confiance

Copyright © 2012 Eyrolles.

Remerciements

Mes remerciements vont en premier lieu aux deux personnes qui m'ont appris tout ce que je sais en cryptographie et en mécanismes de sécurité : David Arditi et Gilles Macario-Rat. Débuter sa carrière avec de tels tuteurs est le rêve de tout ingénieur.

Je remercie chaleureusement tous ceux qui ont participé, directement ou indirectement, par leurs témoignages, leurs encouragements, leur relecture, à la rédaction et à la publication de cet ouvrage : Alain Bobant, Alain Borghesi, Éric Caprioli, Pascal Colin, Jean Denuzière, Charles Du Boullay, Thomas Kaeb, Cécile Lazaro, Philippe Maraval, Bertrand Maréchaux, Fabrice Mattatia, Didier Plas, Emmanuel Poidevin, Gilles Pourcher, Sylvie Robert, Jean Saphores, Hervé Schauer, Michel Treins, Armelle Trotin, Ignace Vantorre et Philip Zimmermann.

Je ne saurais trop remercier Stéphane Torossian, qui a su combiner talent artistique et rigueur technique pour réaliser les nombreuses illustrations du livre.

Enfin, mes pensées vont également aux membres de la Fédération nationale des tiers de confiance qui, par la richesse des échanges réguliers de nos groupes de travail, ont amplement contribué à alimenter le contenu de ce livre.

Copyright © 2012 Eyrolles.

Copyright © 2012 Eyrolles.

Table des matières

Avant-propos 1
Portée de l'ouvrage 1
À qui s'adresse ce livre ? 2
À propos de l'auteur 2
À propos de l'illustrateur 3

Partie 1 – Les clés de la révolution numérique

Chapitre 1 – La dématérialisation 7
Du traitement automatisé des données à la suppression du papier . . . 7
Le « zéro papier » : un mythe utile ? 8
Les composants d'un service dématérialisé 10
Internet : une zone de non-droit ? 11

Chapitre 2 – La sécurité de la dématérialisation 15
Les différents types de risques et de réponses 15
La sécurité technique 16
La sécurité applicative et juridique 18
La sécurité comportementale 19
La chaîne de la sécurité 21
Normalisation et référentiels 22
Un peu de cryptographie pour y voir plus clair 24

Chapitre 3 – La notion de confiance 35
Une définition de la confiance 35
La confiance dans l'économie numérique du point de vue juridique . 38
Le tiers de confiance 40
La chaîne de la confiance 51

Copyright © 2012 Eyrolles.

Partie 2 – L'identité numérique

Chapitre 4 – La gestion d'identités 55
La notion d'identité 55
L'identité numérique 56
Identification et authentification : quelle différence ? 58
Les différents modes d'identification et d'authentification 59
Du bon usage des identifiants et des mots de passe 72
Quelques exemples emblématiques de projets de gestion d'identités 78

Chapitre 5 – Le certificat, une carte d'identité numérique 85
Qu'est-ce qu'un certificat ? 85
Le cycle de vie du certificat 107
La chaîne de la certification 118
Identité numérique et certificats : deux exemples de projets 129
Les conséquences catastrophiques d'une sécurité insuffisante : la faillite de Diginotar 133

Chapitre 6 – La confidentialité 143
Qu'est-ce qui est confidentiel… et vis-à-vis de qui ? 143
Le cas particulier des données à caractère personnel 144
Limiter l'accès aux données : la gestion des habilitations 145
Rendre les données inintelligibles : le chiffrement 146
Transmettre des secrets 154
Conserver et utiliser des secrets 155
Rompre le lien entre les personnes et les données : l'anonymisation 157

Partie 3 – La signature électronique

Chapitre 7 – La signature électronique en pratique 161
Signature manuscrite et signature électronique : deux actes très ressemblants 161
Signature manuscrite et signature électronique : quelques différences pratiques 163
Comprendre le cadre juridique : un passage obligé 164

Chapitre 8 – La signature électronique : un objet technique 175
La réalisation technique d'une signature électronique 175
La vérification d'une signature électronique 180

Copyright © 2012 Eyrolles.

Biométrie et signature électronique 187

Chapitre 9 – Le cachet et les autres formes de signatures 191
L'ambiguïté du terme « signature électronique » 191
La signature de personne morale : le cachet 191
Les autres usages du mécanisme technique de « signature » 193

Chapitre 10 – Définir son besoin et choisir un outil de signature électronique . . . 197
Déterminer le contexte du service 197
Les différentes façons de réaliser des signatures électroniques 198

Partie 4 – Tracer, conserver et certifier les données

Chapitre 11 – La traçabilité 211
La traçabilité, définition et usages 211
Les différentes formes de traçabilité 221
Inclure la traçabilité dans son projet 227
Quelques exemples de projets incluant la traçabilité 231

Chapitre 12 – L'archivage électronique 235
Conserver à long terme les documents électroniques 235
Définir un plan d'archivage 245

Chapitre 13 – La convention de preuve 251
Une convention de preuve… Pour quoi faire ? 251
Constituer une convention de preuve 254

Partie 5 – Organiser la dématérialisation et mener son projet

Chapitre 14 – Mener un projet de dématérialisation 267
Les méthodologies normalisées 267
Les cinq axes d'approche décisionnels 268
Le déroulement d'un projet 283

Chapitre 15 – Organiser la dématérialisation 297
La dématérialisation : un projet d'entreprise transverse 297
Vers une direction de la dématérialisation ? 298

Index 301

Copyright © 2012 Eyrolles.

Copyright © 2012 Eyrolles.

Avant-propos

Portée de l'ouvrage

La dématérialisation n'est plus « en cours » : elle fait aujourd'hui partie intégrante de notre quotidien, que ce soit dans la sphère privée, la sphère professionnelle ou les relations à l'administration.

Le présent ouvrage détaille les mécanismes de sécurité destinés à créer les conditions de la confiance dans les applications web, ainsi que les méthodologies projet destinées à leur mise en œuvre efficace.

Tout d'abord, nous définirons les notions clés de dématérialisation, de sécurité et de confiance :

- les enjeux de la dématérialisation ;
- la sécurité sous ses aspects technique, applicatif, juridique et comportemental ;
- la nécessité de faire naître la confiance des utilisateurs pour promouvoir les usages ;
- le rôle des tiers de confiance dans la chaîne de la dématérialisation ;
- les mécanismes de cryptographie qui sous-tendent la sécurisation des services.

Nous détaillerons ensuite les notions essentielles de la sécurité applicative :

- l'identité numérique et le contrôle d'accès ;
- le certificat ;
- la confidentialité, *via* la gestion des droits et le chiffrement ;
- la signature électronique et ses avatars techniques ;
- la traçabilité et l'horodatage ;
- l'archivage électronique.

Après avoir décrit comment renforcer la valeur juridique des échanges dématérialisés au travers d'une convention de preuve, nous approfondirons :

Copyright © 2012 Eyrolles.

- les cinq axes d'approche de la sécurité informatique (fonctionnel, juridique, organisationnel, technique et financier) ;
- les étapes clés d'un projet de dématérialisation ;
- les impacts de cette nouvelle réalité sur l'organisation de l'entreprise.

À qui s'adresse ce livre ?

Ce livre s'adresse avant tout aux concepteurs d'applications de dématérialisation confrontés à la mise en œuvre de la sécurité, que ce soit au sein des administrations, des grandes entreprises ou des PME innovantes :

- directeurs et chefs de projet ;
- directeurs Recherche et développement ;
- architectes fonctionnels ou techniques ;
- DSI, architectes SI, RSSI ;
- consultants, assistance à maîtrise d'ouvrage ou à maîtrise d'œuvre ;
- développeurs.

Il a été conçu pour apporter aux étudiants en informatique les clés qui leur permettront d'aborder sereinement le secteur d'avenir que constitue la sécurisation des services dématérialisés.

Enfin, de par sa volonté de clarté et de pédagogie, il est également abordable sans restriction par le lecteur curieux qui souhaite en savoir plus sur la dématérialisation, la sécurité et la confiance.

À propos de l'auteur

Dimitri Mouton est ingénieur de Télécom Paris (ENST).

Il a débuté sa carrière à France Télécom R&D, au sein du laboratoire Sécurité des services et des réseaux, où il a déposé vingt brevets sur les sujets du prépaiement, de la signature électronique et de la sécurité des terminaux mobiles.

Il a ensuite été responsable Études et développement d'Achatpublic.com, où il a conçu la plate-forme de dématérialisation des marchés publics et d'enchères électroniques inversées.

Puis il a rejoint CertEurope, opérateur de services de e-confiance, en tant que directeur Recherche et développement.

Il a fondé en 2009 le cabinet de conseil en dématérialisation Demaeter, au sein duquel il accompagne de nombreux projets de conception et de sécurisation de services dématérialisés.

Copyright © 2012 Eyrolles.

Il est également expert indépendant en solutions de vote par Internet.

Dimitri Mouton est membre de la Fédération nationale des tiers de confiance depuis 2003. Il y anime trois groupes de travail consacrés au vote électronique, à la traçabilité, à l'identité numérique et la signature électronique, ainsi que des cycles de formation, notamment à la signature électronique.

Il est coauteur de l'ouvrage *Les marchés publics dématérialisés* (éd. Moniteur, Paris, 2004), et de nombreux guides de la confiance de la FNTC.

À propos de l'illustrateur

Artiste peintre, graphiste et illustrateur, Stéphane Torossian crée depuis quelques années des supports de communication, identités visuelles et solutions graphiques dans le domaine de la dématérialisation.

Copyright © 2012 Eyrolles.

Copyright © 2012 Eyrolles.

PARTIE 1

Les clés de la révolution numérique



Copyright © 2012 Eyrolles.

Copyright © 2012 Eyrolles.

Chapitre 1

La dématérialisation

Du traitement automatisé des données à la suppression du papier

La dématérialisation est le nouveau nom de l'informatique. Mais il est bien entendu possible de nuancer cette définition à l'emporte-pièce !

L'informatique est un domaine très étendu, qui concerne l'ensemble des activités nécessaires au traitement automatisé de l'information, depuis la « pascaline », première machine à calculer inventée en 1642 par Blaise Pascal, jusqu'aux supercalculateurs employés pour les prévisions météorologiques, en passant par les consoles de jeu portatives.

La dématérialisation peut être considérée comme un sous-domaine de l'informatique, qui vise à supprimer le support papier des documents au profit de fichiers purement électroniques.

À l'aube de l'an 2000, les professionnels de la conception de services à valeur ajoutée sur Internet ne se reconnaissaient plus dans le terme « informaticien », passé de mode du fait du déploiement massif au grand public de l'usage et de la compétence dans le domaine. Il a donc fallu inventer un mot pour souder une communauté de « sachants », mais aussi pour donner un nouveau souffle à un secteur en mal de valeurs positives.

Depuis la loi Informatique et libertés du 6 janvier 1978, l'informatique souffre en France d'une image de B*ig* B*rother* : elle est perçue comme un risque pour nos libertés individuelles. Si l'ordinateur nous permet d'accéder à de nouvelles informations et à de nombreuses distractions, il permet aussi aux « autres », sans que l'on sache bien qui, de savoir que nous y avons accédé… La dématérialisation se présente comme :

Le mot « ordinateur » a été choisi en 1955 pour désigner en français ce que les Anglo-Saxons appellent *computer*, c'est-à-dire « calculateur ». Le « grand ordinateur », celui qui met de l'ordre dans toute chose, est l'un des noms de Dieu. Voilà qui donne une autre dimension à l'informatique !

Copyright © 2012 Eyrolles.

- une innovation : dans le secteur public, on parle, par exemple, de « modernisation de l'État », cette notion recouvrant les deux idées d'amélioration de la productivité et de simplification des traitements ;
- une avancée écologique : l'un de ses arguments est le « zéro papier », indépendamment de l'énergie nécessaire pour faire fonctionner et refroidir les serveurs et les terminaux des utilisateurs ;
- une simplification de la vie : elle permet d'effectuer des démarches administratives sans se déplacer ;
- un agent de développement économique : elle offre désormais la possibilité d'acheter ses cadeaux de Noël sans faire les magasins ;
- un facteur de socialisation : on peut se rencontrer, échanger et discuter de manière virtuelle d'un bout à l'autre de la planète, instantanément et pour ainsi dire gratuitement.

La dématérialisation englobe bien tout cela : e-commerce, e-administration, réseaux sociaux, contractualisation en ligne, fluidification des échanges et partage des connaissances.

Elle est un outil indispensable pour les particuliers, les administrations et les entreprises.

Dans son acception de « changement du support de l'information », c'est-à-dire de remplacement, dans un processus préexistant, de documents et de flux papier par des documents et des flux nativement électroniques, il est important de noter que le « fond » ne change pas : un acte d'achat effectué sur Internet est fondamentalement le même qu'un acte d'achat effectué en magasin. Un marché public dématérialisé reste un marché public avant tout. Un contrat signé électroniquement reste un contrat.

De plus, si la dématérialisation a désormais inéluctablement pris son essor, la croissance de l'immatériel dans les activités de services ne signifie pas nécessairement la disparition totale du papier.

Le « zéro papier » : un mythe utile ?

Il existe de nombreux cas où « dématérialisation » et « papier » cohabitent nécessairement. C'est inévitable, en particulier, lorsque tous les acteurs de la chaîne métier ne sont pas équipés techniquement ou préparés de manière organisée pour traiter des documents électroniques.

Prenons le cas des justificatifs de domicile : le citoyen doit en fournir pour s'inscrire sur les listes électorales, pour ouvrir un compte bancaire, pour souscrire un abonnement de téléphonie mobile… En règle générale, ces démarches se font *via* la constitution d'un dossier papier, remis physiquement. Or, de plus en plus de justificatifs de domicile sont envoyés sous forme électronique (les factures de consommation d'énergie ou de

Copyright © 2012 Eyrolles.

télécom, par exemple). Le citoyen imprime alors son justificatif initialement électronique pour le présenter au guichet. Ce cas de figure n'est d'ailleurs pas sans poser des problèmes de fraude, tant il est facile, avec les moyens informatiques à la portée du grand public, de constituer un faux justificatif. Le « zéro papier » consiste ici à faire porter les frais d'impression sur l'utilisateur final.

A *contrario*, un deuxième cas d'usage est celui de la dématérialisation des factures entrantes : lorsqu'une entreprise met en œuvre un progiciel de gestion intégrée (PGI) pour gérer ses flux financiers, elle doit bien entendu y intégrer les factures de ses fournisseurs. Dans certains cas, il est possible d'imposer à tous les fournisseurs l'usage de la facture électronique ; cependant, il est fréquent que la dématérialisation totale des factures se fasse par étapes, les grands facturiers se l'appropriant en premier, et les petits fournisseurs plus tardivement. Un service très répandu chez les prestataires du domaine de la dématérialisation de factures est donc de recevoir les factures papier, de les scanner, d'en reconnaître les champs essentiels et de les intégrer dans le PGI du client. Il ne s'agit pas là de « dématérialisation des factures » à proprement parler, puisque le flux d'entrée est matériel. En revanche, le traitement aval (vérifications, mise en paiement, etc.), est quant à lui dématérialisé. Le « zéro papier » est ici une cible, que l'on atteint progressivement en développant peu à peu le champ d'application de la dématérialisation.

Enfin, citons un troisième exemple, le plus emblématique des limites du « zéro papier ». Lorsqu'un flux métier est dématérialisé, les documents électroniques échangés sont transmis à un agent qui doit les étudier dans le cadre de son activité professionnelle. Or, la lecture sur écran, malgré les progrès des terminaux d'affichage et des logiciels bureautiques, reste inconfortable, tant au niveau de la fatigue visuelle qu'elle provoque, que par le manque de maniabilité des fichiers informatiques : mettre de côté les pages traitant de tel sujet, feuilleter jusqu'à reconnaître le paragraphe que l'on cherche, etc. Il est donc bien plus confortable d'imprimer les documents pour les lire et les étudier ! Prenons l'exemple concret d'un acheteur qui doit analyser des mémoires techniques pour comparer les offres de différents candidats à un marché : comment se passer de la capacité à annoter le document au fil de la lecture, ou à laisser dépasser de l'un des documents les deux pages que l'on veut comparer d'un coup d'œil avec les parties correspondantes de la deuxième offre ? Nous reprendrons et développerons cet exemple dans le chapitre consacré à la conduite du changement.

Le « zéro papier » est donc une déclaration d'intention, un objectif à long terme, et rarement une cible à court terme véritablement atteignable.

Il sera ainsi souvent bien moins onéreux de concevoir un service dématérialisé traitant de manière entièrement électronique les 80 % de cas les

Copyright © 2012 Eyrolles.

plus fréquents, tout en maintenant un traitement papier pour les cas les moins répandus, plutôt que de chercher à prévoir exhaustivement tous les cas d'usage possibles.

Voyons maintenant quels sont les éléments de base constituant un service dématérialisé.

Les composants d'un service dématérialisé

On peut décomposer un service de dématérialisation en quatre grandes briques techniques, comme illustré dans la figure 1-1.

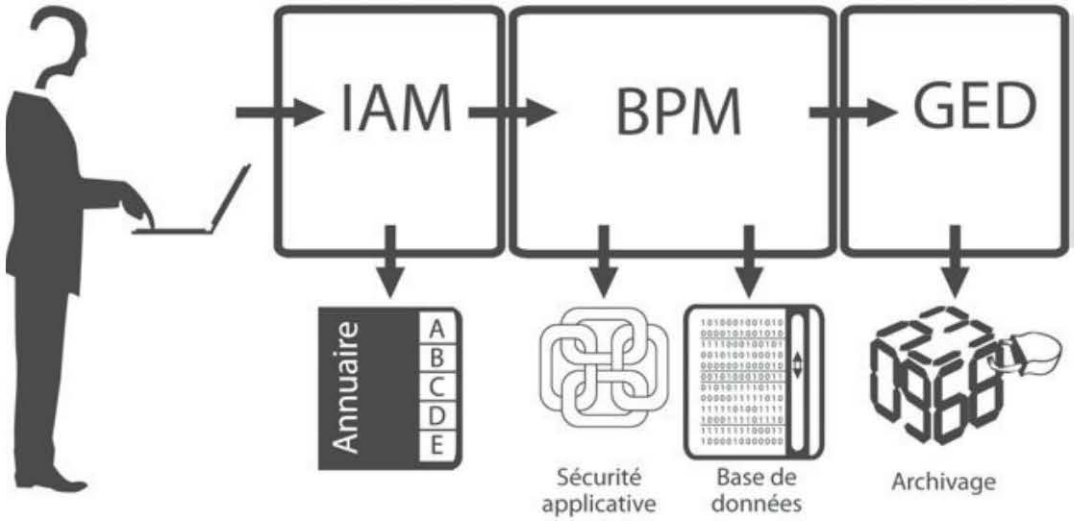


Figure 1-1 : Les composants d'un service dématérialisé

La gestion des identités et des accès (IAM, *Identity and Access Management*), sert à contrôler les utilisateurs du service, à leur attribuer des droits et à garantir leur respect et leur usage. Nous étudierons en détail cette notion dans la partie traitant de l'identité numérique.

La gestion des processus métier (BPM, *Business Process Management*), sert à définir les flux d'informations entre les utilisateurs : circulation des données, circuits de décision, travail collaboratif, traitements automatiques...

La gestion électronique de documents (GED), permet de gérer le cycle de vie de l'information. Elle peut aller d'un simple système de classement, de conservation et de recherche de fichiers, à des mécanismes évolués d'indexation riche, voire dynamique, et au stockage sur le long terme de documents dans des conditions normalisées, prenant alors le nom « d'archivage électronique ». Le chapitre 12 traite en détail de l'archivage électronique.

Copyright © 2012 Eyrolles.

Enfin, la **sécurité applicative**, fondée sur la cryptographie, regroupe les mécanismes destinés à garantir l'intégrité des documents, leur provenance, leur confidentialité, l'engagement des personnes, la traçabilité des actions… Nous développerons amplement ces mécanismes de sécurité tout au long du présent ouvrage.

Nous illustrerons la complémentarité de ces outils par le point de vue d'un éditeur de solution de Business Process Management, Didier Plas, dans le chapitre 14 consacré à l'implémentation des services dématérialisés.

À partir de ces quatre grands ensembles fonctionnels, il est possible de constituer d'innombrables services dématérialisés. Mais attention, le respect des règles juridiques est fondamental dans la mise en œuvre de la dématérialisation.

Internet : une zone de non-droit ?

On ne peut plus prétendre aujourd'hui qu'Internet soit une zone de non-droit ! En effet, l'Europe et, par contrecoup, la France, ont mis en place un arsenal juridique très riche pour permettre la dématérialisation et l'encadrer.

Dès 1978, la loi Informatique et libertés fixait des limites strictes à ce que l'on peut ou ne peut pas faire en matière de traitement (automatisé ou non) des données personnelles. Il s'agissait d'une première reconnaissance dans le droit français de l'importance de l'informatique, qui a fixé dans son article 1 le grand principe suivant :

Loi Informatique et libertés – Article 1

L'informatique doit être au service de chaque citoyen. [...] Elle ne doit porter atteinte ni à l'identité humaine, ni aux droits de l'homme, ni à la vie privée, ni aux libertés individuelles ou publiques.

Le développement des systèmes d'information (SI) des entreprises et des administrations, puis de l'Internet grand public, a permis à l'informatique de sortir des usages purement privés et anecdotiques pour accéder au domaine jusqu'ici réservé aux échanges papier : l'établissement de preuves susceptibles d'être présentées en justice. Cette irruption de l'informatique dans le domaine juridique marque le début de la dématérialisation et a été entérinée par la loi du 13 mars 2000, qui a défini le cadre légal de la « preuve par écrit » de telle manière que les documents informatiques puissent entrer dans cette catégorie. Cette loi a modifié l'article 1316 du Code civil comme suit :

Copyright © 2012 Eyrolles.

Code civil – Article 1316

La preuve littérale, ou preuve par écrit, résulte d'une suite de lettres, de caractères, de chiffres ou de tous autres signes ou symboles dotés d'une signification intelligible, quels que soient leur support et leurs modalités de transmission.

Ainsi, dire qu'un e-mail ou des traces de serveurs informatiques « n'ont aucune valeur » n'est plus recevable. Il est précisé d'emblée que la preuve peut être établie sur tout support et transmise par tout moyen. Si les parties ne contestent pas la véracité d'un e-mail, par exemple, le juge pourra alors le prendre en compte. Cela ouvre la porte au support électronique et au transfert par les réseaux de télécommunications dans le droit de la preuve.

L'article suivant précise les choses en fixant les conditions de l'admission en preuve d'un écrit sous forme électronique :

Code civil – Article 1316-1

L'écrit sous forme électronique est admis en preuve au même titre que l'écrit sur support papier, sous réserve que puisse être dûment identifiée la personne dont il émane et qu'il soit établi et conservé dans des conditions de nature à en garantir l'intégrité.

Cet article précise explicitement que la dématérialisation est possible : l'électronique prend la même valeur juridique que le papier. Toutefois, le législateur introduit des contraintes pour le support électronique : l'identification de l'auteur doit être certaine, et l'intégrité du document doit être garantie tout au long de son cycle de vie.

On peut raisonnablement penser que ces éléments de sécurité ont été introduits du fait de la grande facilité qu'il existe à créer ou modifier un document électronique.

Pour reprendre les exemples précédents, un simple e-mail ou de simples traces d'un serveur, sans garantie de leur provenance et de leur intégrité, ne constitueront pas à eux seuls une « preuve », mais ils ne seront pas non plus dénués de valeur juridique : ils constitueront un « commencement de preuve » entrant dans un « faisceau de preuves » que le juge examinera.

Le législateur insiste enfin avec l'article 1316-3 du Code civil :

Code civil – Article 1316-3

L'écrit sur support électronique a la même force probante que l'écrit sur support papier.

Cet article établit l'équivalence du papier et de l'électronique. D'un point de vue pratique, cet article lève les barrières liées à l'habitude.

Copyright © 2012 Eyrolles.

- Le papier n'est pas « plus fort » que l'électronique. Toutefois, il est « plus habituel », et l'on fait plus facilement confiance à des documents tangibles, matériels (voir à ce sujet le chapitre 3 consacré à la confiance).
- L'électronique n'est pas « plus fort » que le papier. Toutefois, il est plus facilement tracé, et des mécanismes de sécurité informatique permettent aisément de prouver la provenance et l'intégrité des documents électroniques (voir à ce sujet le chapitre 6 sur la sécurité).

Nous verrons plus loin dans le présent ouvrage les dispositions prises pour la signature électronique, et celles permettant l'établissement d'une convention de preuve qui garantira la solidité juridique d'un service dématérialisé.

Mais d'ores et déjà, nous voyons que la possibilité de dématérialiser est offerte, avec des contraintes (identification, intégrité) qui ont trait au domaine de la sécurité.

Copyright © 2012 Eyrolles.

Copyright © 2012 Eyrolles.

Chapitre 2

La sécurité de la dématérialisation

Les différents types de risques et de réponses

La dématérialisation, si elle est une source d'innombrables opportunités, est aussi le support de nombreux risques nouveaux. Nous pouvons en citer quelques-uns.

Certains dangers proviennent en général d'une attaque intentionnelle : intelligence économique (pillage des secrets d'une entreprise au profit d'un concurrent), détournement de données personnelles, vandalisme (atteinte à l'intégrité des données), atteinte à l'image de marque…

Mais les virus, vers et autres chevaux de Troie sont susceptibles de détruire ou d'altérer les données, de consommer des ressources système ou de provoquer des indisponibilités de service également de manière aveugle, touchant aussi bien le particulier que l'entreprise.

Un risque lié aux infrastructures réside dans la disponibilité des services et des données : une panne de réseau, un crash disque, un effondrement de performances dû à une « fuite mémoire », une panne d'alimentation électrique sont susceptibles de porter préjudice aux utilisateurs d'un service dématérialisé et donc au fournisseur de ce service.

Enfin, le risque le plus récemment pris en compte est celui lié à la valeur juridique des documents générés à l'aide d'un ordinateur et échangés *via* Internet : comment faire la preuve d'une action réalisée sur un système informatique ? Comment garantir l'engagement d'un utilisateur ? Comment prouver l'antériorité d'un document par rapport à un autre ? Et comment présenter tout cela devant un tribunal en cas de contentieux ?

L'ensemble des mesures prises pour diminuer les risques se divise en trois familles.

Copyright © 2012 Eyrolles.

Sécurité technique, sécurité applicative et sécurité comportementale : trois notions complémentaires qu'il convient de mettre en œuvre conjointement.

- La sécurité technique met en œuvre des infrastructures robustes, indépendamment de l'applicatif qui s'y exécute.
- La sécurité applicative consiste à employer, au sein du service lui-même, des mécanismes garantissant la sécurité des données qui y sont traitées : nous y incluons la sécurité juridique.
- La sécurité comportementale sensibilise les utilisateurs et les forme pour les amener à éviter les situations de prise de risque, consciente ou inconsciente.

Nous allons maintenant détailler ces trois notions complémentaires.

La sécurité technique

La sécurité technique des systèmes d'information est la composante qui pourra être traitée de manière identique quelle que soit l'application concernée : les mesures mises en œuvre ne seront pas spécifiques au besoin métier, aux données traitées, aux utilisateurs concernés, mais dépendront seulement du niveau de sécurité attendu, dans l'absolu, en termes de disponibilité des machines et de résistance aux attaques, aux pannes et aux autres événements nuisibles pouvant survenir.

On concevra aisément, par exemple, que le niveau de sécurité (et donc le coût induit) ne soit pas le même pour une application de vote par Internet, dans laquelle une interruption de service peut être considérée comme une entrave au droit de vote et faire naître la suspicion sur l'ensemble de l'opération électorale, que pour un service en ligne de demande de renseignements sur les fêtes organisées par la municipalité, dont l'indisponibilité pendant une demi-journée n'aura qu'un impact très limité.

En revanche, on aura des exigences de sécurité proches entre le vote par Internet et la dématérialisation des marchés publics : si le fournisseur ne peut pas se connecter pour déposer son offre dans les délais, l'ensemble de la procédure risque d'être remise en cause, avec, à la clé, une perte de temps de plusieurs mois et éventuellement une rupture d'approvisionnement.

La sécurité technique repose sur plusieurs composantes complémentaires : les aspects contractuels, les aspects organisationnels, les aspects logiques et les aspects physiques.

Les aspects contractuels

Du point de vue contractuel, la sécurité technique repose en général sur un engagement de qualité de service (SLA, *Service Level Agreement*), pris par l'hébergeur du système d'information. Cet hébergeur peut être interne (la DSI, par exemple) ou externe (un prestataire de services). Les engagements

Copyright © 2012 Eyrolles.

contractuels incluront une durée maximale d'indisponibilité des serveurs, les plages horaires de garantie de continuité de service, les temps maximaux de rétablissement en cas de panne, etc. Les aspects contractuels prévoient, en général, des pénalités applicables en cas de non-respect des engagements par l'hébergeur. Il est à noter qu'un « contrat » peut être envisagé, au sein d'une entreprise, entre la DSI et ses clients internes.

Les aspects organisationnels

Les aspects organisationnels couvrent les moyens humains mis en œuvre pour garantir le respect des engagements contractuels. Cela comporte non seulement la disponibilité et la qualification des personnels, mais également l'ensemble des procédures mises en œuvre lors de l'exploitation courante du service, les sauvegardes, le plan de continuité d'activité (PCA), les procédures d'escalade en cas d'incident et les procédures d'exception, y compris, au sein du plan de reprise d'activité (PRA), les solutions alternatives à mettre en œuvre en cas de panne totale du système d'information. Par exemple, les boutiques d'une grande enseigne peuvent-elles toujours vendre aux clients si le système d'information central gérant les caisses et les prix est indisponible ? Une procédure non informatisée est nécessaire !

Les aspects logiques

La composante logique s'intéresse d'une part aux logiciels et matériels mis en œuvre pour garantir la sécurité (pare-feu, antivirus, sondes de détection d'intrusion…), et d'autre part à l'architecture logique du système d'information : cloisonnement des sous-réseaux, adressage public/privé, zones démilitarisées…, mais également aux droits conférés aux administrateurs système et administrateurs de bases de données, ainsi qu'à la traçabilité de leurs actions et au mode d'installation des systèmes d'exploitation (physique, virtualisé, voire en « cloud »).

Les architectures techniques largement réparties, appelées « cloud », posent des problèmes spécifiques de sécurisation.

Les aspects physiques

Enfin, la sécurité physique présente deux dimensions : la sécurité des locaux (redondance de l'hébergement sur des sites distincts, protection anti-incendie, anti-inondation, contrôle d'accès physique, existence de deux adductions indépendantes d'électricité et de réseau, existence d'un générateur électrique de secours et d'une réserve de carburant suffisante…), et la sécurité des machines et de leur exploitation (redondance des serveurs et des bases de données, redondance des alimentations électriques et réseau de chaque baie, éloignement physique des serveurs redondants…).

Dans cet ouvrage, nous ne détaillerons pas davantage le sujet de la sécurité technique, notre propos principal étant la sécurité applicative.

Copyright © 2012 Eyrolles.

La sécurité applicative et juridique

La sécurité applicative regroupe les mesures prises au sein d'une application pour répondre aux besoins fonctionnels de sécurité du service rendu, c'est-à-dire ce qui est spécifique aux échanges et aux traitements réalisés au sein de ce service. Si le service comporte une dimension juridique (établissement de contrat, capacité à prouver des événements, garantie de confidentialité, conservation des documents sur le long terme…), alors les mesures de sécurité juridique entrent dans le cadre de la sécurité applicative.

Dressons la liste des actions nécessitant la mise en œuvre de la sécurité applicative, et des mécanismes correspondants.

- **Identifier une personne et déterminer ses droits :** on appliquera les concepts de la gestion d'identités et du contrôle d'accès.
- **Garantir la provenance d'un document :** on appliquera, selon les cas, un scellement par un serveur (cachet ou horodatage), la signature électronique, si l'on veut également marquer le consentement de l'utilisateur aux termes du document, ou des mécanismes de traçabilité.
- **Garantir l'intégrité d'un document :** on s'appuiera sur des mécanismes purement cryptographiques, comme le calcul d'empreinte. On appliquera, en outre, un scellement par un serveur (cachet ou horodatage), ou la signature électronique, si l'on veut également marquer le consentement de l'utilisateur aux termes du document. Le stockage dans un coffre-fort électronique permet également la conservation sur le long terme.
- **Prouver l'action d'un utilisateur ou le déroulement d'un événement automatique :** on s'appuiera sur les mécanismes de traçabilité.
- **Prouver une date :** c'est le rôle de l'horodatage.
- **Assurer la confidentialité des données :** on mettra en œuvre le contrôle d'accès et/ou le chiffrement des données.
- **Recueillir l'engagement d'un utilisateur :** on emploiera la signature électronique ou un mécanisme de traçabilité.
- **Conserver des données sur le long terme et garantir la capacité à les retrouver :** c'est à ce besoin que répond l'utilisation de l'archivage électronique.

Selon le service rendu, la mise en application de tout ou partie de ces mécanismes sera nécessaire, et les niveaux d'exigence retenus ne seront pas les mêmes. Dans la suite du présent ouvrage, nous développerons chacune de ces fonctions de sécurité, en les illustrant par des cas concrets d'usage ou de non-usage, justifiés par les besoins objectifs.

Copyright © 2012 Eyrolles.

Toutefois, la mise en œuvre de mesures techniques de sécurité est insuffisante si elle n'est pas complétée par une sensibilisation des utilisateurs aux bonnes pratiques, comme nous allons maintenant le présenter.

La sécurité comportementale

La majeure partie des attaques contre les systèmes d'information proviennent « de l'intérieur » : elles sont perpétrées soit par des employés malveillants ou inconscients des conséquences de leurs actions, soit par des ex-collaborateurs désireux de se venger, soit par des pirates extérieurs à l'organisation, mais ayant réussi à se procurer des informations confidentielles (codes d'accès, architecture technique…) grâce à l'ingénierie sociale.

La mise en place de procédures précises, connues de tous, appliquées, et dont la mise en pratique est vérifiée régulièrement, permet de se prémunir contre un grand nombre de comportements inadaptés qui créent un réel danger.

Les règles ne sont pas nécessairement complexes, ni très contraignantes. On peut en citer ici quelques-unes parmi les plus évidentes :

- ne pas inscrire son mot de passe sur un Post-it collé à côté de son poste de travail ;
- ne jamais quitter son poste de travail sans l'avoir verrouillé ;
- ne jamais exécuter de programme téléchargé depuis Internet ;
- ne jamais brancher de clé USB sur son poste de travail pour échanger des données, ni en entrée, ni en sortie ;
- ne jamais faire de copies de ses données professionnelles sur un ordinateur à usage personnel ;
- ne jamais répondre à des questions relatives à des éléments confidentiels par téléphone…

Pour mettre en place au sein de l'entreprise une véritable politique de sécurité, il ne suffit pas de rédiger un corpus de règles et de les faire signer par tous en annexe au contrat de travail. En effet, il est « naturel » que les utilisateurs du système d'information aient des habitudes comportementales issues de leur expérience de l'informatique dans le cercle privé. Pour faire évoluer ces pratiques et obtenir l'adhésion des utilisateurs aux règles, il faut un engagement fort et explicite de la direction générale, une exemplarité de la hiérarchie, et une véritable volonté de formation et d'accompagnement, dotée des moyens adéquats et inscrite dans la durée.

On veillera par ailleurs, dans la conception des services dématérialisés et leur mise en œuvre, à prendre en compte en amont l'utilisateur et son mode de travail, afin de ne pas lui créer des conditions difficiles qui pourraient l'amener à contourner les règles de sécurité. Par exemple, si le temps de transfert de documents a été sous-estimé et se trouve être trop long,

Copyright © 2012 Eyrolles.

l'utilisateur peut être tenté de copier ces documents sur une clé USB ou de les graver sur un CD-Rom pour les remettre au destinataire en dehors du cadre défini, qui était censé assurer la traçabilité et la confidentialité, contournant ainsi pour des raisons qui lui semblent légitimes (le temps perdu dans son travail) le dispositif de sécurité mis en place.

Parole d'expert

Ignace Vantorre, président de Sogelink

Sogelink est éditeur et opérateur du service DICT.fr et se positionne comme tiers de confiance. Dans ce cadre, vous avez décidé de former l'ensemble de votre personnel aux problématiques de sécurité. Pourquoi ?

Notre rôle de tiers de confiance passe par une exemplarité sans faille, qui est pour nous une priorité stratégique. La sécurité ne peut pas être vécue comme une contrainte : elle doit être une véritable culture d'entreprise.

Tout d'abord, l'inclusion de fonctions de sécurité dans nos services concerne au premier plan notre équipe R&D, qui conçoit et développe ces fonctionnalités, et nos exploitants système, qui les administrent.

Mais nos offres de services sécurisés sont élaborées par le service marketing et vendues par le service commercial, qui doivent donc disposer des compétences nécessaires. Et bien entendu, les téléopérateurs du service clients doivent être à même de répondre aux questions des utilisateurs.

Enfin, les services administratifs, s'ils ne sont pas directement au contact des applications de confiance, sont un maillon fort de la sécurité globale de l'entreprise car leur poste de travail est connecté à l'intranet et contient potentiellement des informations sensibles pour l'entreprise.

Nous n'envisageons pas la sécurité d'un pur point de vue technique, mais comme un tout englobant en premier lieu les aspects comportementaux : verrouiller son poste de travail lorsqu'on le quitte, ne pas transférer de données *via* des clés USB ou ne naviguer que sur des sites à vocation professionnelle sont autant de bonnes pratiques qui sont le premier garde-fou face aux risques de compromission de nos données, et qui s'imposent à tous sans exception.

Quels moyens avez-vous mis en œuvre pour dispenser cette « culture sécurité » dans l'entreprise ?

La première étape a consisté à adopter une charte sécurité qui fait partie du règlement intérieur de l'entreprise et qui marque la détermination de la direction à faire de ce sujet une priorité incontournable.

Nous avons ensuite organisé des séances de sensibilisation et de formation à la sécurité, adaptées à chaque catégorie de personnel. Tous nos employés se sont vu remettre, à l'issue de la formation, une fiche récapitulative des points clés qui concernent leur métier en matière de sécurité : règles comportementales pour les personnels administratifs, explications fonctionnelles pour les employés qui sont en contact avec les clients, contraintes techniques pour les informaticiens.

Des encarts dédiés à la sécurité sont systématiquement inclus dans notre lettre de communication interne.

Copyright © 2012 Eyrolles.

Enfin, ces actions donnent lieu à un suivi régulier et à des rappels périodiques.

Quels changements cela a-t-il induit dans la vie de l'entreprise ?

Les aspects sécurité s'inscrivent naturellement dans notre culture d'amélioration continue et de qualité de service. Tous nos collaborateurs ont pris conscience de l'importance des règles de sécurité, car elles leur ont été présentées et expliquées, et parce qu'elles sont suivies par la hiérarchie.

Du pur point de vue technique, notre politique de sécurité est très bien respectée et, de l'aveu même des exploitants système, respecter ces règles leur a donné une plus grande sérénité dans leur activité quotidienne.

Pour ce qui concerne les aspects comportementaux, l'accueil a également été très positif. Un jeu s'est même instauré parmi les employés : si l'un d'eux quitte son poste sans le verrouiller, il doit apporter le lendemain matin des croissants pour ses collègues de bureau !

Si la sécurité pouvait de prime abord sembler un sujet austère et contraignant, une communication adaptée nous a permis de la faire adopter par tous avec le sourire, et la conscience de bien faire est un plus pour la qualité de vie au bureau.

La chaîne de la sécurité

Les trois formes de sécurité que nous venons de décrire (technique, applicative et comportementale) ne sont pas distinctes, ni exclusives les unes des autres, bien au contraire : elles sont totalement complémentaires, et le non-respect des prescriptions de l'un des domaines suffit à affaiblir l'ensemble du système d'information.

La « chaîne de la sécurité » globale, illustrée par la figure 2-1, a la force de son maillon le plus faible. Négliger l'un des aspects de la sécurité, c'est mettre en danger l'ensemble du service dématérialisé.

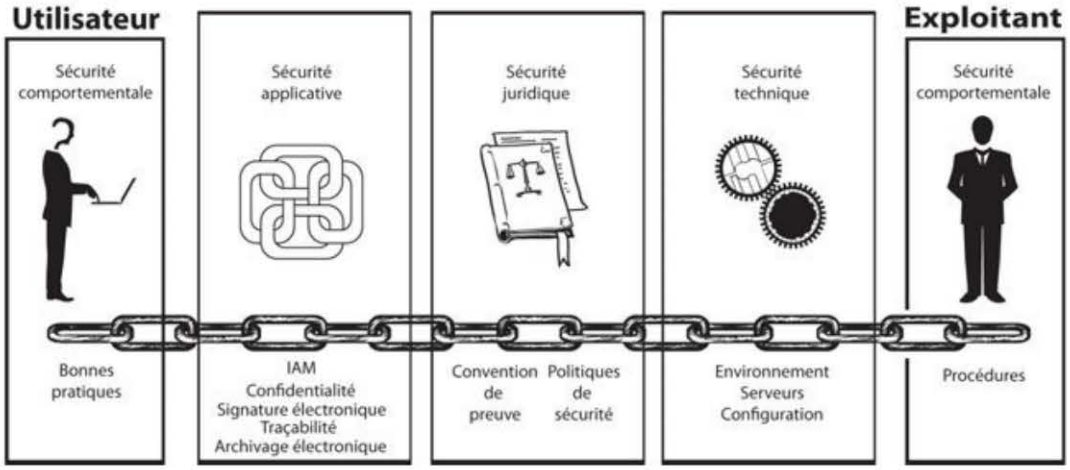


Figure 2-1 : La chaîne de la sécurité

Copyright © 2012 Eyrolles.

Pour une illustration concrète des conséquences pratiques du non-respect de la chaîne de sécurité, un exemple complet est développé dans le chapitre 5, à la section « Les conséquences catastrophiques d'une sécurité insuffisante : la faillite de Diginotar ».

Voyons maintenant quels outils normatifs permettent de guider les concepteurs et exploitants de services dématérialisés dans leur activité de sécurisation.

Normalisation et référentiels

Un secteur normatif pléthorique

Le domaine de la sécurité informatique au sens large est très normalisé, et les outils ne manquent pas. Au niveau organisationnel et technique, on citera, par exemple, les normes de la famille ISO 27000 qui définit les systèmes de gestion de la sécurité de l'information.

Pour ce qui est des mécanismes cryptographiques qui entrent en jeu dans la sécurité applicative, on peut citer de nombreuses initiatives.

- La société RSA Security a publié un ensemble de normes appelé PKCS (*Public Key Cryptographic Standard*) définissant de nombreux formats, algorithmes et protocoles employés en cryptographie.
- Les normes techniques relatives aux infrastructures à clé publique ont été rédigées au sein de l'IETF sous la forme de documents nommés RFC (*Request For Comments*) par un groupe de travail dédié appelé PKIX. Les travaux de PKIX ont notamment repris les normes PKCS pour en faire des standards publics. Parmi ces normes, on peut citer : la RFC 2527 (normalisation de la rédaction d'une politique de certification), la RFC 2560 (protocole de validation de certificat OCSP), la RFC 2630 (format d'enveloppe cryptographique CMS), la RFC 3161 (protocole d'horodatage TSP), la RFC 4055 (algorithme RSA), la RFC 5280 (format de certificats X.509)…
- Les formats de signature électronique ont été normalisés non seulement par PKIX (format CMS), mais également par le W3C (format XAdES) et par Adobe (format PDF) – puis, synthétisés par l'ETSI sous les noms CAdES, XAdES et PAdES (voir à ce sujet le chapitre 7 sur la normalisation des signatures électroniques).
- L'AFNOR a publié la norme française NF Z42-013 décrivant les « Spécifications relatives à la conception et à l'exploitation de systèmes informatiques en vue d'assurer la conservation et l'intégrité des documents stockés dans ces systèmes », c'est-à-dire l'archivage électronique. Cette norme a été transposée par l'ISO sous la référence 14641-1…

Copyright © 2012 Eyrolles.

L'objet de ce chapitre n'est pas de faire une liste exhaustive des normes applicables au domaine de la sécurité de la dématérialisation, mais d'illustrer le fait qu'il y a pléthore de normes, chacune étant adaptée à un contexte et à un besoin.

Certaines portent même sur des aspects métier très précis, comme la norme AFNOR NF Z42-025 sur la gestion du bulletin de paie électronique.

En France, les pouvoirs publics ont choisi de créer un cadre général de sécurité qui s'impose aux administrations pour la mise en œuvre de la dématérialisation : le Référentiel général de sécurité, ou RGS.

Un référentiel français incontournable : le RGS

L'ordonnance n° 2005-1516 du 8 décembre 2005 instaure, par son article 9, un Référentiel général de sécurité (RGS) qui s'impose à toutes les autorités administratives. Le RGS définit des niveaux de sécurité pour certaines fonctions de sécurité applicative : authentification des personnes et des serveurs, signature électronique, cachet, chiffrement et horodatage.

Le RGS définit des niveaux de sécurité qui lui sont propres, sous forme d'étoiles : de une étoile (*) à trois étoiles (***).

Sauf dans les cas où la loi a édicté d'autres principes, l'autorité administrative qui met en œuvre un service dématérialisé doit déterminer, *via* une analyse de risques, le niveau de sécurité requis pour ces fonctions de sécurité. Elle est alors tenue de mettre en place les dispositifs correspondants. Pour les éléments qui s'imposent aux utilisateurs, tout dispositif ou service de niveau égal ou supérieur doit être accepté.

Les prestataires de services fournissant ces fonctions de sécurité peuvent se faire qualifier afin de prouver leur conformité au RGS.

Ordonnance n° 2005-1516 du 8 décembre 2005 – Article 9

I. Un référentiel général de sécurité fixe les règles que doivent respecter les fonctions des systèmes d'information contribuant à la sécurité des informations échangées par voie électronique telles que les fonctions d'identification, de signature électronique, de confidentialité et d'horodatage. [...]

II. Lorsqu'une autorité administrative met en place un système d'information, elle détermine les fonctions de sécurité nécessaires pour protéger ce système. Pour les fonctions de sécurité traitées par le référentiel général de sécurité, elle fixe le niveau de sécurité requis parmi les niveaux prévus et respecte les règles correspondantes. [...]

III. Les produits de sécurité et les prestataires de services de confiance peuvent obtenir une qualification qui atteste de leur conformité à un niveau de sécurité du référentiel général de sécurité. [...]

Copyright © 2012 Eyrolles.

Entré en vigueur avec l'arrêté RGS du 18 mai 2010, le RGS s'impose à l'ensemble des téléservices de l'administration. Il est applicable au plus tard le 19 mai 2013 à l'ensemble des procédures d'échange de documents mettant en œuvre un système d'information.

Le RGS se veut également un recueil de bonnes pratiques à l'usage du secteur privé.

Comme nous l'avons vu, la sécurité applicative repose essentiellement sur des mécanismes cryptographiques : la compréhension des normes applicables ou des niveaux de sécurité définis par le RGS est une gageure si l'on ne maîtrise pas les notions de base de cryptographie. Nous allons maintenant en aborder les trois grandes familles : les fonctions de hash, la cryptographie asymétrique et la cryptographie symétrique.

Un peu de cryptographie pour y voir plus clair

Un outil indispensable : les fonctions de hash

Les propriétés du hash

Le premier outil cryptographique que nous allons aborder porte plusieurs noms : calcul d'empreinte, condensation, ou hash, qui est le terme que nous emploierons le plus généralement.

L'algorithme de hash actuellement recommandé est SHA256 (pour *Standard Hash Algorithm*, 256 bits étant la taille des données obtenues en sortie).

Les fonctions de hash sont des algorithmes mathématiques qui prennent en entrée une donnée qui peut avoir n'importe quelle taille, et qui rendent en sortie une chaîne d'octets de longueur fixe qui dépend de chacun des bits de l'entrée mais ne permet pas de retrouver l'entrée.

Voyons quelles sont les principales propriétés des fonctions de hash.

- **La sortie a une taille constante, indépendante de l'entrée.**

  La condensation peut porter sur tout fichier, quelle que soit sa taille : que le document en entrée soit une donnée technique de 20 octets, un document Word de 200 Ko ou une photo de 2 Mo, le résultat de sa condensation par la fonction SHA256 donnera pour résultat une chaîne de 256 bits, comme illustré par la figure 2-2.

Copyright © 2012 Eyrolles.

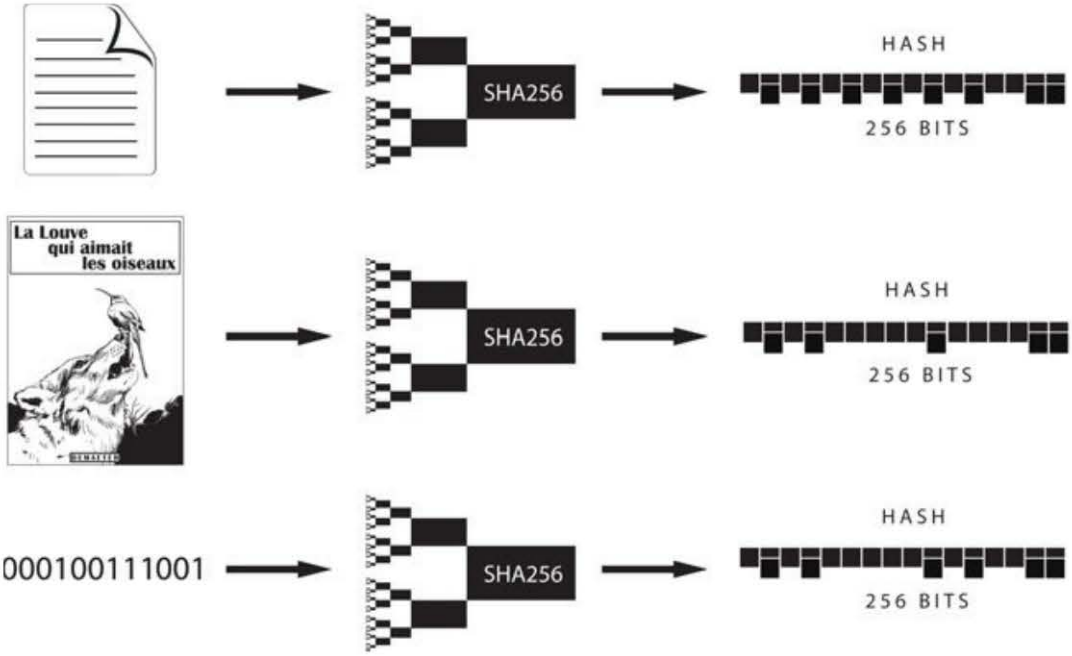


Figure 2-2 : La taille du hash est constante.

- **La sortie est pseudo-aléatoire, très dépendante de l'entrée.**

  La fonction de condensation donne un résultat dont chaque bit dépend de l'ensemble des données fournies en entrée. Ainsi, comme le montre la figure 2-3, si l'on calcule le hash de deux fichiers très proches, par exemple en modifiant un seul bit du fichier initial pour constituer le second, on obtiendra des résultats très différents, qui ne permettront en rien de déduire une ressemblance des fichiers fournis en entrée.



Figure 2-3 : La sortie du hash est très dépendante de l'entrée.

- **Le hash est une fonction « à sens unique ».**

  Attention à ne pas confondre les fonctions de condensation avec des fonctions de compression de données (comme le format ZIP, par exemple) : si SHA256 ramène tout fichier, quelle que soit sa taille, à une chaîne de 256 bits (figure 2-4), l'opération inverse est impossible… Et

Copyright © 2012 Eyrolles.

c'est là l'une des propriétés essentielles de la condensation : il s'agit de fonctions « à sens unique ». Connaître le condensé d'un fichier ne permet pas de déduire le contenu du fichier lui-même, ni de constituer un autre document qui aurait ce même condensé.

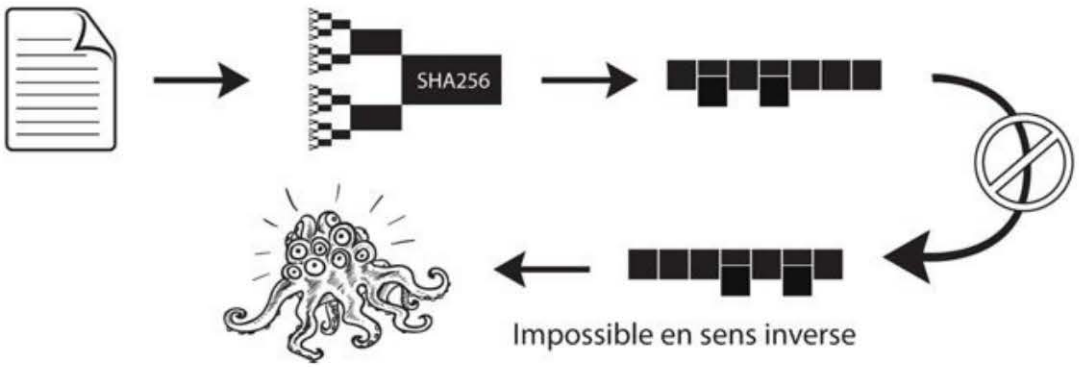


Figure 2-4 : Le hash est une fonction à sens unique.

À présent, évoquons rapidement quelques propriétés intéressantes des fonctions de hash, que nous détaillerons par la suite.

Le hash : un outil d'anonymisation

Il est parfois nécessaire de conserver la trace d'une donnée, sans pour autant conserver la donnée elle-même. Un exemple peut être l'exploitation à des fins statistiques de données médicales : il sera important de pouvoir lier entre elles deux données provenant du même patient, sans pour autant dévoiler le nom du patient. L'anonymisation consiste alors à remplacer le nom du patient par son hash : le nom étant toujours le même, le hash sera identique pour toutes les données provenant de ce dossier médical, ce qui permettra leur exploitation. Mais il sera impossible de remonter jusqu'au patient, le hash (fonction à sens unique) ne permettant pas de recalculer le nom.

Le hash : un outil de scellement

Comme nous le verrons dans le chapitre 11 sur la traçabilité, l'enregistrement de données à des fins de reconstitution de l'historique des actions peut nécessiter de garantir l'intégrité des traces ainsi constituées, afin de garantir qu'aucun enregistrement n'ait été ajouté, supprimé ou modifié. Une façon de réaliser ce scellement est d'inclure dans chaque enregistrement l'empreinte du précédent. De cette manière, la modification d'un seul enregistrement est détectée dans l'ensemble des enregistrements suivants.

Copyright © 2012 Eyrolles.

Le hash : une fonction de condensation

Nous verrons dans la section suivante sur la cryptographie asymétrique que les calculs réalisés avec les clés publique et privée ne peuvent porter que sur des données de taille limitée, inférieure à la taille de la clé RSA employée.

Pour la signature électronique en particulier, le document signé étant en général bien plus volumineux que la limite, on fera porter le calcul non sur le fichier, mais sur son hash, qui en représente une version condensée.

La cryptographie asymétrique

Clé privée et clé publique

L'utilité fonctionnelle de la cryptographie asymétrique, illustrée par la figure 2-5, est la suivante :

- un individu (le « porteur ») doit être capable de faire un calcul que lui seul est capable de réaliser : pour cela, il doit disposer d'un secret ;
- un autre individu (le correspondant) doit être capable de vérifier le calcul pour s'assurer que le porteur dispose de ce secret, mais sans en disposer lui-même.

Les algorithmes utilisables pour effectuer ces opérations sont regroupés sous le nom générique de « cryptographie à clé publique », ou « cryptographie asymétrique », parce qu'ils reposent sur deux données complémentaires, liées mathématiquement et générées conjointement, mais gérées de manière très différente :

- la « clé privée » constitue le secret que le porteur doit conserver confidentiel, et qu'il utilisera pour effectuer le calcul mentionné ci-dessus ;
- la « clé publique » est son pendant mathématique, qui permet d'effectuer le calcul inverse, et donc de vérifier que la personne qui a fait le calcul initial possédait bien la clé privée.

La clé publique peut être diffusée largement, et transmise librement à toute personne appelée à l'utiliser. Bien entendu, la connaissance de la clé publique ne permet pas de déduire la clé privée. La sécurité de la cryptographie asymétrique repose entièrement sur cette propriété mathématique.

L'algorithme de cryptographie asymétrique le plus employé s'appelle RSA, du nom de ses inventeurs : Rivest, Shamir et Adleman. Nous nous limiterons à aborder cet algorithme.

L'algorithme RSA a été inventé en 1976. Il demeure aujourd'hui le plus employé !

Nous ne développerons pas ici les bases mathématiques de la cryptographie asymétrique : il existe de nombreux ouvrages qui entrent dans le détail de l'implémentation de ces algorithmes, et la connaissance des arcanes de la cryptographie n'est absolument pas indispensable pour mettre en œuvre ces fonctionnalités dans des projets de dématérialisation.

Copyright © 2012 Eyrolles.

Il est en revanche extrêmement important de retenir les propriétés de base du couple clé publique/clé privée (aussi appelé la « bi-clé ») et des algorithmes asymétriques :

- deux clés complémentaires sont générées simultanément ;
- la clé « privée » reste secrète ;
- la clé « publique » est diffusée librement ;
- les deux clés effectuent des opérations inverses l'une de l'autre.

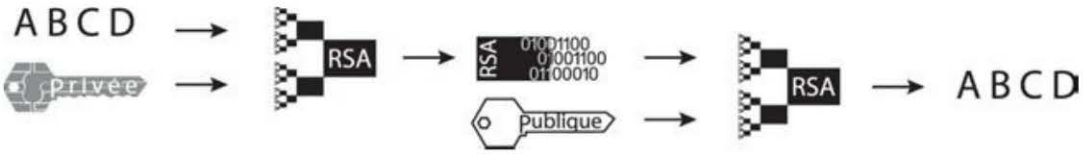


Figure 2-5 : La cryptographie asymétrique

La cryptographie asymétrique est utilisée pour l'authentification, la signature électronique et le chiffrement : voyons maintenant son usage dans chacun de ces cas.

Les fonctions de sécurité rendues par la cryptographie asymétrique

Sur la base de la figure 2-5, il est simple d'imaginer trois fonctions de sécurité qui seront rendues aisément à l'aide de la cryptographie asymétrique : l'authentification, le chiffrement et la signature électronique.

Ces grands mécanismes cités précédemment seront respectivement détaillés dans les chapitres 4, 6 et 7 mais nous pouvons d'ores et déjà les présenter schématiquement, du simple point de vue de l'usage des clés.

L'authentification

Le déroulement du mécanisme d'authentification est le suivant :

- le processus est initié par le correspondant, qui envoie au porteur un défi : le défi est une donnée volatile, utilisée une seule fois, générée aléatoirement par le correspondant ;
- la donnée utilisée en entrée de l'algorithme RSA est le hash du défi ;
- le porteur effectue le calcul RSA à l'aide de sa clé privée ;
- le correspondant vérifie ce calcul à l'aide de la clé publique ;
- le résultat du calcul RSA est détruit après vérification.

L'opération d'authentification est destinée à vérifier ponctuellement l'identité du porteur dans le but de lui donner accès à un service. La preuve de l'identité est apportée par la clé privée, la vérification par la clé publique.

Copyright © 2012 Eyrolles.

La signature électronique

La signature électronique consiste à utiliser sa clé privée sur une donnée (le contenu d'un document, par exemple) pour la lier à l'identité du porteur de manière durable, pour exprimer le consentement du porteur vis-à-vis du destinataire.

Le mécanisme mis en œuvre est le suivant :

- le processus est initié par le porteur ;
- la donnée utilisée en entrée de RSA est le hash de la donnée à signer (c'est-à-dire le hash du fichier contenant le texte sur lequel le porteur veut engager son consentement) : une donnée pérenne, destinée à être conservée ;
- le porteur réalise le calcul RSA à l'aide de sa clé privée ;
- le correspondant vérifie ce calcul à l'aide de la clé publique ;
- le résultat du calcul RSA est conservé ; le moment de la vérification dépend entièrement du processus métier mis en œuvre.

L'opération de signature est destinée à lier définitivement l'identité du porteur au document signé, dans le but de marquer son engagement. La signature électronique est obtenue à l'aide de la clé privée, sa vérification à l'aide de la clé publique.

Le chiffrement

Le chiffrement consiste à utiliser la clé publique sur une donnée confidentielle, de manière à garantir que seul le porteur, disposant de la clé privée correspondante, pourra faire l'opération inverse et donc accéder à la donnée en clair.

Le mécanisme mis en œuvre est le suivant :

- le processus est initié par le correspondant qui envoie des données confidentielles au porteur ;
- la donnée utilisée en entrée de RSA est la donnée confidentielle : une donnée pérenne, destinée à être conservée ;
- le correspondant effectue le calcul RSA à l'aide de la clé publique du porteur ;
- le porteur effectue le déchiffrement, toujours par l'algorithme RSA, à l'aide de sa clé privée ;
- le résultat du calcul RSA est conservé ; il s'agit de la donnée secrète rendue confidentielle.

L'opération est destinée à rendre la donnée secrète incompréhensible à tous, mis à part le porteur, puisqu'il est le seul à disposer de sa clé privée. Le chiffrement est effectué à l'aide de la clé publique, le déchiffrement à l'aide de la clé privée.

Copyright © 2012 Eyrolles.

Nota Bene : nous verrons dans le chapitre 6 consacré à la confidentialité que, dans la pratique, du fait des limitations de taille liées à l'algorithme RSA, le chiffrement est un mécanisme à deux étages impliquant également la cryptographie symétrique.

Sur quoi la sécurité de la cryptographie asymétrique repose-t-elle ?

Ce qui nous permet de nous appuyer sur la cryptographie asymétrique pour effectuer des opérations de sécurité, ce sont trois propriétés fondamentales : la robustesse de l'algorithme RSA, la « taille » de la clé privée et sa confidentialité.

Les propriétés mathématiques des clés et de l'algorithme

L'utilisation de la cryptographie asymétrique nous garantit que la connaissance de la clé privée est indispensable pour faire l'inverse des opérations réalisées avec la clé publique.

Nous avons, en outre, l'assurance que la connaissance de la clé publique ne permet pas de reconstruire la clé privée.

Enfin, nous avons la certitude qu'il n'existe pas d'attaque « à clair connu », c'est-à-dire qu'en connaissant une donnée et le résultat du calcul RSA effectué sur cette donnée avec la clé privée, on ne peut pas en déduire la clé privée.

Il n'est ainsi pas nécessaire de garder secret l'algorithme utilisé : la robustesse de RSA est suffisante pour garantir la sécurité contre les attaques. Un pirate qui saurait que les échanges sont sécurisés par RSA n'en serait pas plus avancé pour attaquer le système mis en œuvre.

La taille des clés

La robustesse de la sécurité offerte par RSA dépendra de la « taille » des clés utilisées. La taille d'une bi-clé RSA est le nombre de bits d'un élément, appelé le « module ». Pour attaquer une bi-clé RSA, il ne convient pas de tester toutes les valeurs possibles de la clé, mais de factoriser le module pour en déduire la clé privée.

La factorisation du module est facilement réalisable sur un ordinateur personnel pour une taille de clé de l'ordre de 256 bits. En revanche, dès 512 bits, ce n'est plus réalisable sans faire fonctionner en réseau plusieurs centaines d'ordinateurs, et on estime aujourd'hui qu'une taille de bi-clé de 2 048 bits offre une sécurité de très haut niveau.

L'Agence nationale de la sécurité des systèmes d'information (ANSSI) recommande une taille de clé minimale de 2 048 bits pour l'algorithme RSA pour des données devant être conservées jusqu'à 2020, et de 4 096 bits au-delà de cette période.

Copyright © 2012 Eyrolles.

La confidentialité de la clé privée

Bien entendu, utiliser un algorithme robuste et des clés de grande taille n'a aucun intérêt si l'on ne s'assure pas de conserver secrète la clé privée !

Il convient donc de s'assurer que la génération de la bi-clé soit réalisée sous le contrôle exclusif du porteur, ou dans le cadre d'un processus garantissant que nul n'ait pu en prendre connaissance.

Lorsque la clé privée est stockée, même temporairement, sur un support logiciel permettant de la dupliquer, il est important de mettre en œuvre toutes les mesures techniques et organisationnelles permettant de garantir qu'aucune duplication n'ait eu lieu. Toutefois, dans un tel cas, il demeure toujours un doute quant à l'unicité de la clé privée, et il n'est alors pas possible de prouver formellement qu'elle demeure sous le contrôle exclusif de son porteur.

La solution consiste à employer des supports physiques (cartes à puce, supports cryptographiques USB) offrant une fonctionnalité de génération « à bord », qui garantit que la clé privée ne sort jamais de la carte. Nous détaillerons ces mécanismes dans la section du chapitre 5 consacrée aux supports du certificat.

Quelles sont les limitations de la cryptographie asymétrique ?

La cryptographie asymétrique connaît deux limitations principales.

Tout d'abord, les données que l'algorithme RSA peut accepter en entrée sont limitées à la taille de la bi-clé.

Si l'on utilise une bi-clé de 2 048 bits, cela veut dire que l'on ne peut pas signer ou chiffrer avec l'algorithme RSA un fichier de plus de 256 caractères… Voilà qui risque de mettre fin rapidement à notre intérêt pour RSA… Sauf à trouver des solutions !

Ensuite, les performances de la cryptographie asymétrique sont assez mauvaises en termes de vitesse de réalisation. Générer des bi-clés est consommateur de ressources, et les utiliser pour effectuer des calculs RSA également. Il faut donc limiter l'usage de la cryptographie asymétrique à des opérations peu nombreuses.

La solution au premier inconvénient pourrait être d'augmenter considérablement la taille des clés… Mais le second inconvénient, le problème de performances, nous en empêche !

Nous verrons dans le chapitre 6 consacré à la confidentialité que la solution apportée aux limitations de RSA dans le domaine du chiffrement est l'utilisation conjointe de la cryptographie symétrique.

Pour la signature électronique, la solution apportée consiste à employer les fonctions de hash, présentées précédemment.

Copyright © 2012 Eyrolles.

Cryptographie asymétrique et certificat

Enfin, on ne peut parler de cryptographie asymétrique sans évoquer la notion de certificat.

Du point de vue technique, un certificat est un fichier scellé électroniquement par son émetteur (le prestataire de services de certification électronique), de manière à établir de manière inaltérable le lien entre l'identité du porteur et sa clé publique. Il sert donc à établir la confiance dans les échanges réalisés à l'aide de la bi-clé du porteur.

Nous en détaillerons la structure, le contenu et l'utilisation dans le chapitre 5 qui lui est consacré.

Abordons maintenant l'autre forme de cryptographie nécessaire à la sécurisation des échanges électroniques : la cryptographie symétrique.

La cryptographie symétrique

La cryptographie symétrique, ou cryptographie à « clé secrète », sert à garantir la confidentialité des données par le mécanisme appelé « chiffrement ».

Contrairement à ce que nous avons vu pour la cryptographie asymétrique, c'est ici la même clé qui sert à faire les calculs dans un sens et dans l'autre.

Cette clé secrète, ou clé symétrique, est simplement constituée d'une suite aléatoire d'octets.

L'algorithme actuellement recommandé pour le chiffrement symétrique s'appelle AES pour *Advanced Encryption Standard*.

Attention cependant : il existe plusieurs modes d'implémentation d'AES, qui n'offrent pas tous la même robustesse.

Ainsi, par exemple, le mode ECB (*Electronic CodeBook*) donne un chiffré identique pour deux clairs identiques. Son utilisation est déconseillée.

Au contraire, le mode CBC (*Cipher Block Chaining*), qui inclut un vecteur d'initialisation et un bouclage de l'algorithme sur les blocs successifs, offre une confidentialité optimale.

Le fonctionnement général de la cryptographie symétrique est illustré par la figure 2-6 :

- l'émetteur d'une donnée secrète génère une clé symétrique ;
- il l'utilise pour chiffrer la donnée secrète ;
- il transmet à son correspondant la donnée secrète chiffrée et la clé symétrique ;
- le correspondant se sert de la clé symétrique pour déchiffrer la donnée secrète et en prendre connaissance.

Copyright © 2012 Eyrolles.

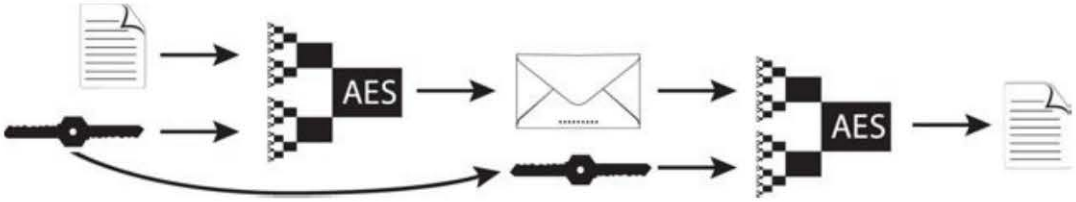


Figure 2-6 : La cryptographie symétrique

Ce mécanisme assure la confidentialité de la donnée chiffrée... Sous réserve que la clé secrète employée soit elle-même transmise de manière confidentielle !

Pour assurer le transfert de la clé secrète, deux mécanismes sont couramment utilisés.

- Envoyer la clé par un canal différent du canal d'envoi du document chiffré : par exemple, envoyer le document *via* un serveur et la clé par e-mail. La sécurité de cette façon de faire dépend de la sécurisation mise en œuvre sur le canal de transmission de la clé et de la capacité d'un éventuel indiscret à se procurer le document chiffré.
- Utiliser la cryptographie asymétrique pour rendre la clé secrète confidentielle à son tour. Nous détaillerons cela dans le chapitre 6 dédié à la confidentialité.

Les attaques que l'on peut mener contre la cryptographie symétrique sont des recherches exhaustives de la valeur de la clé, ce que l'on appelle des attaques « force brute ». Plus la clé est longue, plus la probabilité qu'un pirate parvienne à trouver la clé dans un temps raisonnable est faible.

C'est pourquoi l'ANSSI recommande l'utilisation de clés de chiffrement de 100 bits pour chiffrer les données devant rester confidentielles jusqu'à 2020 au plus, et de 128 bits au-delà de cette période.

Après avoir parcouru les mécanismes de sécurité disponibles au service de la dématérialisation, voyons comment leur mise en œuvre contribue à créer le contexte propice à leur adoption par les utilisateurs, au travers de la notion de confiance.

Copyright © 2012 Eyrolles.

Copyright © 2012 Eyrolles.

Chapitre 3

La notion de confiance

Une définition de la confiance

Un sentiment de sécurité indispensable

La confiance est un sentiment de sécurité, c'est-à-dire l'impression subjective que l'on peut se fier à notre environnement et à nos interlocuteurs sans courir de danger.

La sécurité, quant à elle, constitue l'ensemble de conditions garantissant l'absence de danger : elle est l'un des préalables à l'établissement de la confiance.

L'économie numérique a longtemps souffert de l'absence de confiance des utilisateurs. En effet, les questions suivantes sont récurrentes.

- Qui peut accéder à mes données ? Par exemple, les données bancaires lors d'un paiement en ligne, ou les données personnelles lors de l'inscription à un service.
- Comment être certain que mon message est bien parvenu à son destinataire ?
- Quelle valeur a le document que j'ai rédigé sur mon ordinateur et transmis *via* le service ?

L'établissement de la confiance entre les différents acteurs (fournisseurs de services, marchands, consommateurs, cocontractants, administrations…) a été rapidement perçu par le législateur comme un prérequis au développement de l'activité électronique en Europe et en France.

Copyright © 2012 Eyrolles.

À qui fait-on confiance ?

Au quotidien, nous faisons confiance, avec ou sans réticence, à de nombreux interlocuteurs. Citons quelques exemples qui trouveront leur pendant dans le monde dématérialisé.

- Nous faisons confiance à l'État, parce qu'il a été désigné par nous, *via* les élections, pour appliquer un programme politique qui nous avait été présenté, dans le respect de la Constitution.
- Nous faisons confiance au notaire ou à l'huissier de justice, parce qu'il exerce une profession réglementée qui lui impose de respecter un ensemble de règles qui sont garantes du bien commun.
- Nous faisons confiance au juge, parce qu'il est tenu d'appliquer la loi en toute neutralité.
- Nous faisons confiance au maître-nageur, parce qu'il est grand et fort, mais surtout parce qu'il a un diplôme qui garantit ses compétences en secourisme.
- Nous faisons confiance à notre banque ou à notre opérateur télécom, parce que nous avons avec eux un contrat, et parce qu'il s'agit de grandes entreprises ayant pignon sur rue.
- Nous faisons confiance à nos amis, parce que nous les connaissons *intuitu personae* et que nous avons une culture et une histoire communes.
- Nous faisons confiance à notre boucher, parce qu'il est soumis à des contrôles d'hygiène, parce que nous avons l'habitude qu'il nous vende de la bonne viande, et parce qu'il a tout intérêt à continuer pour conserver notre clientèle.
- Nous faisons confiance à l'inconnu à qui nous demandons notre chemin, parce qu'il n'a aucun avantage à nous fourvoyer.
- Nous faisons confiance à la rambarde qui nous empêche de tomber parce que nous pouvons constater de visu qu'elle est en bon état et robustement scellée.

Il serait bien évidemment possible de citer de nombreux autres exemples, mais ceux-ci suffisent à décrire de nombreux mécanismes d'établissement de la confiance.

Comment accorde-t-on sa confiance ?

Les exemples énumérés ci-dessus permettent d'établir plusieurs raisons d'accorder sa confiance.

- La capacité de vérifier par soi-même (exemple de la rambarde).

  Dans les relations dématérialisées, la capacité à vérifier par soi-même est très rarement applicable. On peut, à ce sujet, citer le cas du vote par Internet, même si la vérification est indirecte : la CNIL recommande

Copyright © 2012 Eyrolles.

aux organisateurs de scrutins, lors de chaque élection, de mandater un expert indépendant pour vérifier les conditions de mise en œuvre de l'élection et pour réaliser un audit du code informatique de la solution de vote. L'indépendance de l'expert permet de donner confiance non seulement à l'organisateur du scrutin, mais aussi aux candidats et aux électeurs, si le rapport d'expertise leur est communiqué.

- L'habitude ou la connaissance intime (commerçant, amis).

  Ce critère joue peu dans le domaine des e-services ou des téléservices, mais beaucoup pour les autres usages d'Internet comme le courrier électronique, le chat ou les réseaux sociaux. C'est également la base du modèle PGP d'échanges de certificats personnels, que nous développerons au chapitre 5.

- L'absence d'intérêt qu'a autrui à nous nuire.

  Ce critère détermine le fait que nous fassions confiance au contenu des sites web de partage de connaissances, comme les encyclopédies collaboratives. Il est pourtant reconnu que nombre d'informations, même basiques, y sont erronées !

- L'exemple de la confiance donnée par les autres (grandes enseignes).

  Ce critère joue pleinement dans l'économie numérique, exactement comme dans la vie réelle. Ainsi, le nombre de paiements en ligne était extrêmement faible jusqu'à l'instauration du modèle sécurisé, dans lequel le module technique de transmission des coordonnées bancaires est inclus dans la page du commerçant directement par la banque, et garantit une transmission confidentielle grâce au protocole SSL. L'acheteur, qui n'était pas prêt à faire confiance au commerçant en ligne, accepte en revanche de faire confiance à la banque.

- L'existence d'un contrôle par une entité supérieure (diplôme du maître-nageur), la confiance étant alors héritée de cette entité de contrôle.

  Il s'agit là du critère le plus mis en avant par le législateur, *via* les qualifications délivrées aux prestataires de services de confiance, comme nous avons pu le voir dans l'ordonnance du 8 décembre 2005 (voir le chapitre 2 et sa section sur le RGS). Un service dématérialisé qui s'appuie, pour sa sécurité, sur des produits et des prestataires qualifiés doit être digne de confiance. Nous ajouterons à cela un bémol : un mécanisme de sécurité robuste, mais mis en œuvre dans de mauvaises conditions ou à mauvais escient, ne garantit pas la sécurité. Citons l'exemple d'un service d'archivage électronique dans lequel les documents seraient conservés pendant 10 ans, mais où aucun système d'indexation ne permettrait de faire des recherches : ce service offrirait la certitude que les documents sont bien gardés… mais pour ainsi dire inaccessibles !

Copyright © 2012 Eyrolles.

- Le caractère bienveillant et neutre instauré de manière institutionnelle (profession réglementée, justice).

  Les professions réglementées ont mis en œuvre la dématérialisation des actes qu'elles produisent, dans des conditions de nature à en garantir la sécurité. Elles n'ont toutefois pas de rôle à proprement parler sur la confiance dans l'économie numérique. En revanche, ce rôle de « tiers de confiance », c'est-à-dire d'acteur de référence neutre, est l'une des grandes tendances actuelles du développement de l'économie numérique. Nous aborderons plus en détail cette notion à la section « Le tiers de confiance » de ce chapitre.

- La position absolument dominante et légitime (État démocratiquement élu).

  Ce critère fonctionne extrêmement bien, même lorsque le niveau de sécurité est dégradé. Ainsi, la Direction générale des finances publiques (DGFIP) avait instauré, pour la télédéclaration de l'impôt sur le revenu, l'obligation de signer électroniquement sa déclaration de revenus, selon le principe de l'équivalence du document électronique avec le document papier. En 2009, année où la signature électronique a été supprimée du téléservice, le nombre de télédéclarants (déjà en hausse régulière depuis de nombreuses années) a encore augmenté d'environ 25 %. Cet exemple illustre le fait que, lorsque la confiance dans le service est établie, la sécurité n'est pas un critère d'adhésion du grand public.

Dans la conception de services dématérialisés, le niveau requis de confiance réciproque entre le fournisseur et les usagers du service devra être étudié avec attention, à la lumière de l'ensemble de ces critères : il entre en compte de manière prépondérante dans la détermination du niveau de sécurité nécessaire et suffisant.

Voyons maintenant le point de vue du législateur sur la notion de confiance.

La confiance dans l'économie numérique du point de vue juridique

Le 8 octobre 1997, la Commission européenne a présenté au Parlement européen, au Conseil, au Comité économique et social, ainsi qu'au Comité des régions, une communication intitulée « Assurer la sécurité et la confiance dans la communication électronique – Vers un cadre européen pour les signatures numériques et le chiffrement » .

En aval de ce rapport, a été promulguée la directive 1999/93/CE du Parlement européen et du Conseil, du 13 décembre 1999, traitant de la définition d'un cadre communautaire pour les signatures électroniques.

Copyright © 2012 Eyrolles.

L'établissement de la confiance dans les e-services est marqué comme une priorité dans le considérant 4 de cette directive :

Directive 1999/93/CE – Considérant 4

[...] L'établissement d'un cadre communautaire clair concernant les conditions applicables aux signatures électroniques contribuera à renforcer la confiance dans les nouvelles technologies et à en favoriser l'acceptation générale [...].

La directive de 1999 a été transposée en droit français sous la forme de la loi du 13 mars 2000, dont nous avons vu des extraits dans le chapitre 1 traitant de la dématérialisation, et que nous verrons sur d'autres points dans les chapitres sur la signature électronique et la convention de preuve (chapitres 7 et 13), puis sous la forme du décret du 30 mars 2001, que nous verrons également dans le chapitre 7 sur la signature électronique.

La directive 2000/31/CE du Parlement européen et du Conseil du 8 juin 2000 relative à certains aspects juridiques des services de la société de l'information, et notamment du commerce électronique, dans le marché intérieur (« directive Commerce électronique ») cite encore l'établissement de la confiance du consommateur comme une condition du développement du commerce électronique :

Directive Commerce électronique – Considérant 7

Pour garantir la sécurité juridique et la confiance du consommateur, il y a lieu que la présente directive établisse un cadre général clair pour couvrir certains aspects juridiques du commerce électronique dans le marché intérieur.

Cette directive a été transposée en droit français en 2004 sous le nom de « Loi pour la confiance dans l'économie numérique » (LCEN), qui ne comporte le mot « confiance » que dans son titre.

La confiance ne se décrète pas !

La confiance ne se décrète pas : elle s'obtient, comme nous l'avons vu, soit par une légitimité acquise par ailleurs, soit par la mise en œuvre de mécanismes de sécurité garantis.

C'est pourquoi le principal apport du législateur, au travers de ces textes, ainsi que de ceux établissant le RGS, a été de définir des niveaux de sécurité pour les principales fonctions de sécurité applicative et, pour garantir au public le respect de ces niveaux, un cadre d'accréditation des prestataires de services de confiance et, parmi eux, des tiers de confiance.

Copyright © 2012 Eyrolles.

Le tiers de confiance

Pourquoi faire appel à un tiers de confiance ?

Établir la confiance...

L'expression « tiers de confiance » est trompeuse : il est en effet facile de l'interpréter comme « un tiers », c'est-à-dire une personne étrangère à l'échange en cours, « en qui l'on a confiance ».

Or, le sens de l'expression est tout autre : le tiers de confiance est en effet une personne neutre dans l'échange en cours, mais sur qui on s'appuie pour établir la confiance entre les protagonistes, comme le montre la figure 3-1.

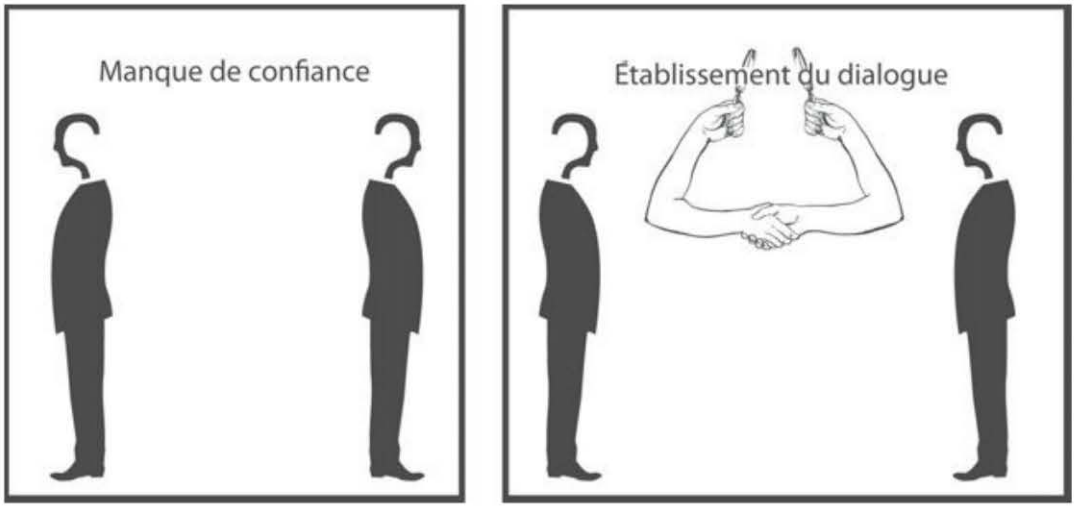


Figure 3-1 : Le rôle du tiers de confiance

Dans la vie « réelle », ce sont les autorités publiques et les professions réglementées qui jouent le rôle de tiers de confiance. Dans le domaine électronique, ce rôle a été confié à des entités souvent privées, que l'on appelle généralement des « autorités », par abus de langage et par une mauvaise traduction du terne anglais *authority* (qu'il aurait mieux valu traduire par « service ») : autorité d'horodatage, autorité de certification, etc., et qui sont regroupées sous le terme générique de tiers de confiance.

... sans faire confiance !

Un tiers de confiance, deux tiers de méfiance !

Le principe de base qui doit présider à l'emploi d'un tiers de confiance est, justement, de ne pas lui faire confiance aveuglément : le tiers de confiance doit publier les règles qu'il applique, et prouver leur bonne mise en œuvre au sein d'un service qui doit être irréprochable.

C'est tout le sens de l'arsenal de qualification mis en œuvre par le législateur, que nous verrons plus loin dans la section de ce chapitre dédiée à

Copyright © 2012 Eyrolles.

la qualification des produits de sécurité et des prestataires de services de confiance. Avant de faire appel aux services d'un tiers de confiance, il est donc indispensable de vérifier ses accréditations.

Nous verrons au chapitre 5, à travers l'exemple de la faillite de Diginotar, à quel point il peut être catastrophique de faire confiance à un tiers sans exiger qu'il fournisse les preuves de sa compétence et de ses bonnes pratiques !

Garantir l'équilibre de la preuve

L'emploi d'un tiers de confiance répond au grand principe de droit selon lequel « nul ne peut se constituer de preuve à soi-même ». Ainsi, en confiant à un tiers le soin de garantir l'intégrité des documents, la traçabilité des échanges, l'horodatage des événements, ou la conservation des fichiers dans des conditions de nature à en garantir la provenance et l'intégrité, le concepteur d'un service dématérialisé dispose d'éléments de preuve plus forts en cas de contentieux, car préservant l'équilibre de la relation.

Dans un service entre des acteurs de « poids » différents, par exemple entre une multinationale qui met à disposition une plate-forme et un utilisateur individuel, il existe un déséquilibre de fait dans la capacité des acteurs à accéder aux preuves et à s'en servir en cas de désaccord. Le fait de faire appel à un tiers de confiance et de donner accès aux preuves à l'ensemble des utilisateurs du service renforce la sécurité de la plate-forme en rendant impossible la mauvaise foi. La protection est ainsi bilatérale.

- Le « petit » dispose en toute transparence des éléments faisant foi, et peut en cas de besoin se défendre sur des bases objectives ;
- Le « gros » n'est pas susceptible de se voir reprocher des pratiques abusives voire mensongères, tous les éléments de preuve provenant d'un tiers neutre et objectif.

Ainsi, la volonté de transparence et d'objectivité qui est l'un des fondements de la profession de tiers de confiance gagne à être appliquée au sein même des services dématérialisés : nous développerons cette idée dans le chapitre 13 dédié à la convention de preuve.

Qui sont les tiers de confiance ?

Le point de vue de la Fédération nationale des tiers de confiance

La Fédération nationale des tiers de confiance (FNTC), fondée en 2001, est l'association des professionnels de la sécurité et de la confiance. Fondée sous l'égide des représentants historiques du domaine de la confiance (les professions réglementées : Ordre des experts comptables, Conseil national des greffiers de tribunaux de commerce, Chambre nationale des huissiers de justice), elle regroupe les opérateurs de services de confiance, les éditeurs de logiciels de sécurité, les experts du domaine (avocats,

Copyright © 2012 Eyrolles.

consultants…), ainsi que des « institutionnels », dans le but de promouvoir les bonnes pratiques en matière de sécurité et de confiance dans les échanges numériques.

La FNTC a donc décidé d'adopter une vision large de la notion de tiers de confiance, tous les maillons de la chaîne ayant un rôle à jouer dans l'établissement de la sécurité des systèmes d'information.

Le point de vue du législateur

Dans l'ordonnance 2005-1516 du 8 décembre 2005, le législateur a adopté un point de vue similaire à celui de la FNTC en définissant la notion de « prestataire de services de confiance » (PSCO) : tous les acteurs qui interviennent sur la chaîne de la confiance peuvent se reconnaître dans la définition ci-dessous.

Ordonnance 2005-1516 du 8 décembre 2005 – Article 1

[…] Sont considérés, au sens de la présente ordonnance : […] comme prestataire de services de confiance, toute personne offrant des services **tendant à** la mise en œuvre de fonctions qui contribuent à la sécurité des informations échangées par voie électronique […]

En revanche, le RGS a opté pour une définition très proche, mais où le mot « tendant à » a été remplacé par « consistant en » :

RGS – Glossaire

Prestataire de services de confiance (PSCO) – Toute personne ou entité offrant des services **consistant en** la mise en œuvre de fonctions qui contribuent à la sécurité des informations échangées par voie électronique.

Ainsi, du point de vue du RGS, seuls les opérateurs de services, c'est-à-dire les entités mettant en œuvre elles-mêmes les services de sécurité, sont des prestataires de services de confiance, à l'exclusion des éditeurs de logiciels ou des concepteurs d'applications sécurisées.

Le RGS définit les conditions de qualification des prestataires de services de confiance, et n'en retient que deux familles.

RGS – Chapitre 5.2 : Qualification des PSCO

Dans cette version du RGS, deux familles de PSCO peuvent faire qualifier leurs services :

- les prestataires de services de certification électronique pour les fonctions d'authentification, de signature (ou de cachet) et de confidentialité ;
- les prestataires de services d'horodatage électronique pour la fonction d'horodatage.

Copyright © 2012 Eyrolles.

Cela confirme la définition donnée par le RGS dans le glossaire, limitée aux seuls fournisseurs de services de sécurité.

Les prestataires de services de sécurité

Les fournisseurs de services de sécurité sont nombreux :

- les prestataires de services de certification électronique (PSCE), qui délivrent les certificats à des fins d'authentification, de signature électronique ou de confidentialité ;
- les prestataires de services d'horodatage électronique (PSHE), qui fournissent des « jetons d'horodatage » (ou « contremarques de temps ») faisant foi de l'existence d'une donnée à un moment précis ;
- les prestataires de services d'archivage électronique, qui garantissent la conservation sur le long terme des documents ;
- les prestataires de validation de certificats électroniques, qui vérifient pour leurs clients la validité des certificats ;
- les prestataires de services de signature électronique, qui réalisent des signatures électroniques ou des cachets à la demande de leurs clients ;
- les prestataires de services de gestion de preuve, qui conservent des traces sécurisées d'événements métier…

On fait appel à ces métiers pour obtenir des éléments faisant foi lors des échanges électroniques : il s'agit indubitablement de tiers de confiance !

Les fournisseurs de services métier incluant de la sécurité

Les plates-formes de services dématérialisés incluant des fonctions de sécurité peuvent adopter des positionnements différents relativement à la notion de tiers de confiance.

Certaines choisissent de jouer un rôle de tiers de confiance : ce sera le cas, par exemple, de la plate-forme de dématérialisation des marchés publics Achatpublic.com ou du service DICT.fr offert par Sogelink. D'autres, en revanche, préfèrent s'appuyer sur des tiers de confiance externes et ne pas adopter ce positionnement elles-mêmes, comme le service e-attestations.com. Détaillons ces exemples.

Achatpublic.com est une plate-forme de transfert d'informations et de documents entre deux familles d'acteurs : d'une part, les acheteurs publics et d'autre part, les fournisseurs. L'acheteur publie son marché (Avis d'appel public à la concurrence et Dossier de consultation des entreprises). Les entreprises déposent leur candidature et leur offre de manière strictement confidentielle. L'acheteur accède aux offres et peut en prendre connaissance de manière sécurisée. Dans ce schéma, la plate-forme offre de nombreux services de tiers de confiance :

Copyright © 2012 Eyrolles.

- la traçabilité de tous les échanges effectués grâce à la plate-forme, *via* l'établissement de preuves horodatées (prestataire de services d'horodatage électronique) ;
- la validation de certificats lors des signatures électroniques (autorité de validation) ;
- la garantie de confidentialité *via* le mécanisme de chiffrement, Achatpublic.com fournissant les certificats correspondants aux acheteurs (prestataire de services de certification électronique).

De même, la société Sogelink propose le service DICT.fr, qui est une plate-forme d'établissement et d'échange des documents préalables aux travaux entre, d'une part, les maîtres d'ouvrage et maîtres d'œuvre, et d'autre part, les exploitants de réseaux et canalisations. Sogelink a décidé de se positionner comme tiers de confiance sur les domaines suivants :

- la traçabilité de tous les échanges effectués grâce à la plate-forme, *via* l'établissement de preuves horodatées (prestataire de services d'horodatage électronique) ;
- la fourniture de certificats de signature électronique « à la volée » (prestataire de services de certification électronique, prestataire de services de signature électronique) ;
- la conservation des documents jusqu'à expiration des délais de recours contentieux (prestataire de services d'archivage électronique).

Dans les deux cas d'Achatpublic.com et de DICT.fr, le service métier rendu par la plate-forme est un service d'échange entre deux populations, vis-à-vis desquelles la plate-forme est entièrement neutre. Ainsi, le positionnement de tiers de confiance central, qui garantit la sécurité et fournit des preuves objectives en cas de contentieux, a sa logique. Pour pallier les cas où ce serait le service même rendu par la plate-forme centrale qui serait remis en cause par l'un des utilisateurs, Sogelink a publié une convention de preuve incluant les politiques correspondant à ces fonctionnalités, comme nous le verrons au chapitre 13, consacré à la convention de preuve. Tous les éléments faisant foi sont fournis aux utilisateurs dans un souci de transparence absolue.

Développons maintenant l'exemple d'une société qui a choisi un positionnement différent : e-attestations. Le rôle du service e-attestations.com est de faciliter les échanges de documents entre les donneurs d'ordre et les fournisseurs dans le cadre de l'obligation de vigilance pour la lutte contre le travail illégal. La société e-attestations a décidé de se positionner uniquement comme éditeur de logiciels en mode SaaS (*Software as a Service*), et le service proposé s'appuie sur des tiers de confiance entièrement externes pour les fonctions d'horodatage, d'archivage, d'émission de certificats et de signature électronique à la volée. La convention de preuve du service e-attestations.com mentionne le recours à ces services externalisés pour l'établissement de la sécurité et de la confiance.

Copyright © 2012 Eyrolles.

Parole d'expert

Emmanuel Poidevin, expert auprès de la Commission européenne, éditeur du service e-attestations.com

Le service e-attestations.com offre de nombreuses fonctions de sécurité à valeur probatoire (traçabilité certifiée, signature électronique...). Pourtant, e-attestations se positionne comme éditeur de logiciels en mode SaaS et non comme tiers de confiance. Pourquoi ?

À chacun son rôle ! Nous mettons tout notre savoir-faire dans des services en ligne qui ont pour but de simplifier les relations entre les donneurs d'ordre et leurs fournisseurs. C'est là notre domaine d'expertise et notre valeur ajoutée.

Les éléments techniques de certification, d'authentification forte, de traçabilité ou de conservation et d'intégrité des données, qui servent à renforcer la sécurité juridique des échanges, sont des services intégrés provenant d'experts du domaine de la sécurité, qui sont pour nous, mais surtout pour nos utilisateurs, des tiers de confiance.

Ce choix est essentiel car il définit nos engagements contractuels vis-à-vis de nos clients (disponibilité, réversibilité, hébergement de données...), et chacun de nos partenaires a son propre engagement concernant son cœur de métier (sécurité, traçabilité, intégrité et conservation des données). Les responsabilités de chacun sont ainsi clairement identifiées et définies.

Que vous apporte votre partenariat avec des tiers de confiance ?

Au-delà de la simple relation avec nos fournisseurs, nous avons établi des partenariats stratégiques avec des tiers de confiance dans les secteurs de la dématérialisation des échanges, domaines sensibles en constante évolution technologique et réglementaire. Il nous apparaît comme essentiel de nous appuyer sur des experts en capacité de maîtriser ces éléments, de s'engager sur leurs domaines d'expertise, et surtout de nous permettre non seulement d'anticiper sur les évolutions mais également de nous fournir les solutions conformes aux exigences présentes et à venir.

Ce sont eux qui sont les garants dans le temps de la pérennité des éléments clés d'identification, de signature, d'horodatage et de conservation des documents et informations de nos utilisateurs. Ainsi accompagnés, nous pouvons nous consacrer à notre cœur de métier : proposer la meilleure solution possible quels que soient les environnements dans lesquels nos utilisateurs évoluent.

Vous gérez, pour le compte de vos clients, des documents à forte valeur juridique, à conserver pendant plusieurs années. Comment garantissez-vous à vos clients la continuité de service en cas de rupture du contrat ?

Nous sommes, de par notre position unique sur le marché, confrontés à une double exigence qui va au-delà même de la durée d'engagement contractuel sur l'utilisation d'e-attestations : être capables de restituer dans l'avenir les documents, et garantir la réversibilité des informations dans le temps. Aussi avons-nous pris plusieurs garanties.

D'une part, toutes les pièces hébergées sur la plate-forme sont archivées électroniquement chez le tiers archiveur CDC Arkhinéo, qui en garantit l'archivage à

Copyright © 2012 Eyrolles.

valeur probante (haute disponibilité et intégrité des données, conservation dans des centres d'archivage hautement sécurisés), et qui permet à nos clients un accès direct en ligne aux archives. C'est ce tiers archiveur qui garantit, au-delà d'e-attestations, la restitution des données dans le temps.

D'autre part, nos logiciels sont déposés auprès de l'Agence pour la protection des programmes. Cet entiercement est une garantie supplémentaire pour nos clients.

Ces trois exemples concernent des services fournis en ligne aux utilisateurs. Voyons maintenant le cas des éditeurs de logiciels qui vendent uniquement des licences d'utilisation de leurs produits.

Les éditeurs de logiciels sont-ils des tiers de confiance ?

Les logiciels de sécurité…

Il est indubitable que les logiciels de sécurité jouent un rôle dans la chaîne de la sécurité et de la confiance : on ne peut pas faire de signature électronique sans un logiciel de signature, d'horodatage sans un logiciel d'horodatage, d'archivage électronique sans un coffre-fort électronique…

La confiance que pourra inspirer le système global découlera donc en partie de la qualité des composants logiciels sur lesquels il s'appuie.

Toutefois, l'engagement de l'éditeur de logiciels ne portera pas sur la façon dont son produit est mis en œuvre dans le service global, et l'éditeur ne sera ainsi pas en position de garantir la chaîne de sécurité.

Prenons le cas d'un logiciel de chiffrement de données à des fins de confidentialité : même si ce logiciel génère des clés robustes et les emploie conformément à l'état de l'art, son éditeur ne peut pas garantir que le service dans lequel il est inclus ne conserve pas une copie en clair des fichiers confidentiels. Ainsi, ce sera l'intégrateur du service global, *via* sa politique de confidentialité, qui pourra prendre un engagement sur la confidentialité globale.

Bien que chaque logiciel de sécurité indépendant ne soit qu'une brique, insuffisante à garantir la solidité de l'édifice global, la robustesse de chacune des briques est un prérequis indispensable.

C'est pourquoi, de même qu'il existe une qualification des prestataires de services de confiance, il en existe une pour les produits de sécurité, que nous détaillerons plus loin dans ce chapitre.

… mais aussi les autres !

Lors de la conception ou de l'audit d'un service sécurisé, ce serait une grave erreur d'ignorer les couches logicielles qui ne font pas directement partie du service, mais sur lesquelles celui-ci s'appuie.

Ainsi, le système d'exploitation, le serveur de base de données, le serveur web, voire d'autres briques métier comme la génération de fichiers `.pdf`

Copyright © 2012 Eyrolles.

ou `.xml` peuvent inclure des failles de sécurité importantes en termes d'intégrité ou de confidentialité des données.

Dans certains environnements très protégés, comme pour le vote par Internet, l'ensemble des briques logicielles sont intégrées dans un package global qui fait l'objet d'un audit de sécurité. Le système d'exploitation, en particulier, peut faire l'objet d'un « durcissement », c'est-à-dire un bridage des fonctionnalités empêchant toute fonction non directement nécessaire pour l'applicatif.

Les pièges de l'open source

Systèmes d'exploitation (Linux, BSD...), annuaires LDAP (OpenLDAP...), bases de données (PostgreSQL...), mais aussi briques de sécurité (OpenSSL, Bouncy Castle...) : l'usage de l'open source dans la conception de services dématérialisés est très répandu.

L'open source est souvent présenté comme un gage de sécurité dans la mesure où chacun peut contrôler l'implémentation effective du logiciel, et où une communauté large travaille à son élaboration. Toutefois, il s'agit là d'éléments qui inspirent confiance... et comme nous l'avons vu précédemment, rien n'est plus risqué que la confiance !

Illustrons ce propos par un exemple de produit de sécurité qualifié par l'ANSSI : Applatoo, de France Télécom R&D. Comme beaucoup de logiciels de sécurité, Applatoo s'appuie sur le logiciel open source de référence, Bouncy Castle. Lors de la qualification du produit, l'ANSSI a demandé à l'éditeur de modifier la fonction de génération de nombres aléatoires (à la base de la fabrication des clés de confidentialité), car l'implémentation du logiciel libre comportait des faiblesses. Ce module a été entièrement redéveloppé, ce qui a permis de garantir la sécurité de l'ensemble et d'obtenir la qualification, gage de qualité que l'open source seul ne saurait offrir en l'absence d'un audit de sécurité sérieux.

Ainsi, s'appuyer sur des produits open source est un gage de gain de temps... mais pas de sécurité ! Pour avoir la certitude de la qualité d'un produit de sécurité, il est recommandé de s'appuyer sur des logiciels et matériels disposant d'une qualification officielle.

La qualification des produits de sécurité et des prestataires de services de confiance en France

La qualification des produits de sécurité

Les produits de sécurité sont les matériels et les logiciels dont l'usage concourt à l'établissement de la sécurité des systèmes d'information. Les procédures mises en œuvre pour garantir la qualité des produits de sécurité sont définies par le décret n° 2002-535 du 18 avril 2002 relatif à

Copyright © 2012 Eyrolles.

l'évaluation et à la certification de la sécurité offerte par les produits et les systèmes des technologies de l'information.

Le fournisseur d'un produit de sécurité peut demander à l'Agence nationale de la sécurité des systèmes d'information (ANSSI) une qualification selon trois niveaux :

- niveau élémentaire (CSPN, Certification de sécurité de premier niveau) ;
- niveau standard (s'appuyant sur les critères communs, standard ISO 15408 pour la sécurité des systèmes d'information) ;
- niveau renforcé (s'appuyant sur les critères communs et comportant des vérifications supplémentaires).

Le décret RGS 2010-112 du 2 février 2010 définit dans son chapitre 3 les responsabilités pour l'octroi des qualifications des produits de sécurité. Les niveaux de sécurité sont publiés au sein du RGS.

La démarche de qualification est la suivante, reprise par la figure 3-2.

1. Le fournisseur du produit de sécurité définit sa cible de sécurité et fait sa demande de qualification.
2. L'ANSSI désigne un centre d'évaluation (CESTI) indépendant du fournisseur qui réalisera l'audit sur la base du RGS, des référentiels applicables et de la cible de sécurité définie.
3. Sur un rapport positif du CESTI, l'ANSSI délivre la qualification et publie les références du produit de sécurité sur la liste officielle.



Figure 3-2 : La qualification des produits de sécurité

La notion de « cible de sécurité » est fondamentale pour estimer la confiance que l'on peut apporter à un produit de sécurité, même qualifié : en effet, si un logiciel, qui réalise plusieurs fonctions de sécurité, n'a été qualifié que pour l'une de ces fonctions, l'utilisateur peut être induit en erreur et croire à une qualification « globale » du produit, le marketing ayant parfois tendance à faire un amalgame… Il convient donc de bien vérifier la cible de sécurité qualifiée avant de retenir un produit de sécurité sur la base de ce critère.

Copyright © 2012 Eyrolles.

La qualification des prestataires de services de confiance

Les prestataires de services de confiance (PSCO) sont les fournisseurs de services dont l'usage concourt à l'établissement de la sécurité des systèmes d'information. Les procédures mises en œuvre pour leur qualification sont définies par le décret n° 2002-535 du 18 avril 2002 relatif à l'évaluation et à la certification de la sécurité offerte par les produits et les systèmes des technologies de l'information et l'arrêté du 26 juillet 2004 relatif à la reconnaissance de la qualification des prestataires de services de certification électronique et à l'accréditation des organismes qui procèdent à leur évaluation.

La qualification se fait sur la base du RGS et, pour deux types de PSCO, selon des schémas de qualification spécifiques : les prestataires de services de certification électronique et les prestataires de services d'horodatage électronique.

La démarche de qualification, reprise dans la figure 3-3, est la suivante.

1. Le Cofrac (Comité français d'accréditation) accrédite des organismes à même de délivrer les qualifications aux PSCO (à noter qu'au moment de la rédaction de cet ouvrage, seule la société LSTI a obtenu l'accréditation du Cofrac).
2. Le PSCO demande la qualification à l'organisme accrédité de son choix.
3. L'organisme accrédité réalise l'audit du PSCO sur la base du RGS et des référentiels applicables.
4. Suite à un audit positif, l'organisme accrédité délivre la qualification et en informe l'ANSSI.
5. L'ANSSI publie les références du PSCO sur la liste officielle.

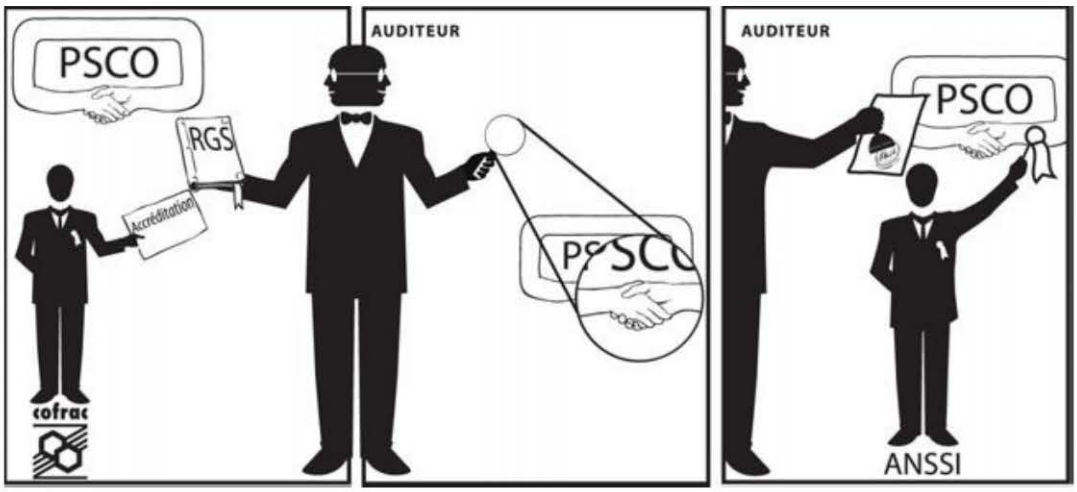


Figure 3-3 : La qualification des prestataires de services de confiance

Ainsi, la qualité des services rendus par le PSCO est garantie par le Premier ministre, sous contrôle de l'ANSSI, qui s'appuie sur l'expertise d'un auditeur accrédité. La qualité de l'auditeur est garantie par le Cofrac. La confiance

Copyright © 2012 Eyrolles.

que l'on met dans un PSCO découle donc d'un schéma entièrement sous le contrôle et la responsabilité de l'État.

La qualification des PSCE se fait sur la base de la norme européenne ETSI 101456. Un PSCE qualifié fait ensuite qualifier les autorités de certification qu'il exploite selon les différents niveaux du RGS.

Parole d'expert

Pascal Colin, directeur général de Keynectis

Keynectis est opérateur technique « prestataire de services de certification électronique » qualifié et opère des autorités de certification conformes au RGS. Qu'apportent ces qualifications à Keynectis et à ses clients ?

La qualification nous apporte tout d'abord l'opportunité de démontrer à nos clients nos bonnes pratiques, et ainsi de créer la confiance. Grâce au respect des normes, nous sommes en mesure de fournir nos services de certification au profit des administrations, en toute transparence et avec une reconnaissance officielle.

La récurrence des audits crée des points de passage réguliers et obligés pour se confronter aux meilleures pratiques, et ainsi regarder notre activité avec des yeux différents. L'interaction avec l'ANSSI nous permet en outre de solliciter des avis dans le cadre de notre processus d'amélioration continue.

Du point de vue commercial, nos clients bénéficient de la garantie de sécurité qu'offre le respect du RGS et bien sûr de l'interopérabilité avec les autres autorités de certification conformes au RGS.

Nos clients profitent aussi de notre capacité à mettre en œuvre des offres conformes en peu de temps.

Par ailleurs, le référencement permet de gagner en visibilité et d'accéder plus aisément aux clients, tout en structurant le marché au travers d'une certaine standardisation et du tri des prestataires sérieux.

Quels moyens mettez-vous en œuvre pour garantir la conformité de vos services aux exigences du RGS ?

Les offres de services sont étudiées pour assurer leur conformité dès le design. Elles sont ensuite construites avec un processus de contrôle de conformité qui permet de s'assurer qu'elles soient conformes dès leur déploiement.

Keynectis dispose d'un département dont la mission première est la veille réglementaire, qui réalise l'analyse du RGS, de ses évolutions, de son environnement et des aspects techniques associés. Il travaille en lien direct avec le marketing pour la définition des exigences applicables aux offres. Ce département a également pour mission l'audit interne afin d'assurer la conformité des offres et des pratiques de Keynectis, préalablement au lancement des offres, pendant le déploiement des projets clients et pendant les phases d'exploitation.

Selon vous, la qualification est-elle une contrainte ou une opportunité ?

La qualification est une opportunité, bien sûr !

Toutefois, si le processus de qualification français va dans le bon sens, il n'est pas suffisant. Il y a des vérifications qui ne sont pas rendues obligatoires par le RGS,

Copyright © 2012 Eyrolles.

ou encore trop peu abordées. Ainsi, nos clients bancaires nous demandent d'appliquer des règles plus contraignantes, en nous positionnant comme prestataires sensibles, ce qui impose au titre du règlement n° 97-02 de la Banque de France des tests nombreux : qualification de la sécurité des applications, tests d'intrusion préproduction, tests d'intrusion annuels, évaluation des vulnérabilités selon une fréquence plus élevée...

Voyons maintenant comment, sur la base de ces éléments, s'établit une « chaîne de la confiance » permettant aux utilisateurs finaux de se fier aux services dématérialisés.

La chaîne de la confiance

La confiance ne se décrète pas, elle s'établit sur la base de critères objectifs et subjectifs qui viennent se compléter les uns les autres. Deux critères permettent donc d'établir le lien de confiance :

- la réputation du tiers de confiance (il s'agit d'un expert incontournable de son domaine, il a de nombreux clients, il a pignon sur rue, on a une relation durable avec lui...) ;
- le fait que le tiers de confiance soit soumis à des contrôles, des audits, des accréditations par une autorité incontestable : organisme de normalisation, fédération professionnelle ou instance étatique.

Ainsi, la confiance que l'on accorde à une information découle de manière logique de la confiance que l'on a dans chacun des maillons ayant servi à produire cette information.

Prenons l'exemple d'un service dématérialisé fourni par une grande entreprise qui a de nombreux clients. La chaîne de la confiance s'établit selon la figure 3-4.



Figure 3-4 : Une chaîne de la confiance faible

Copyright © 2012 Eyrolles.

Prenons maintenant l'exemple d'un service dématérialisé qui s'appuie, pour sa sécurité, sur un tiers de confiance, qui a été qualifié conformément au RGS. La chaîne de la confiance s'établit selon la figure 3-5.

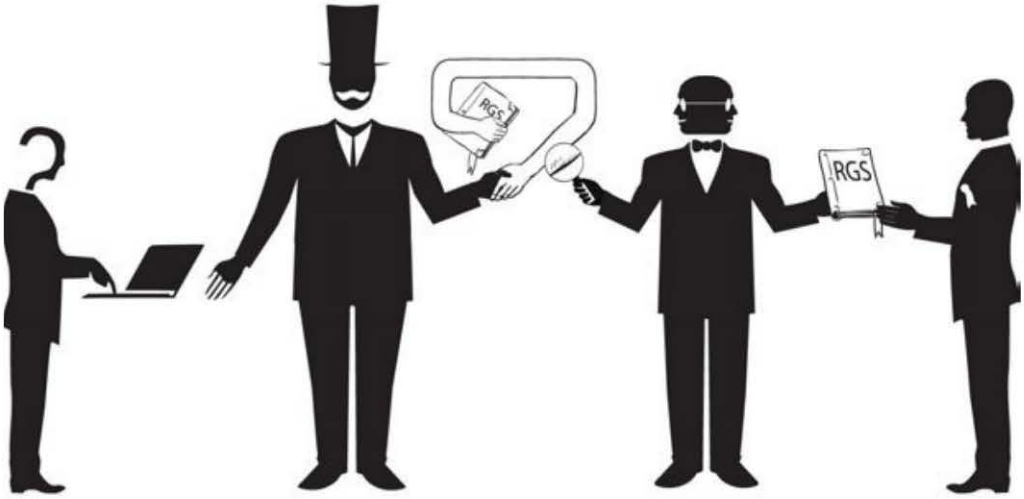


Figure 3-5 : Une chaîne de la confiance forte

Dans le premier cas, la confiance est accordée sans garantie, et le risque de voir cette confiance trahie est important. De plus, l'utilisateur qui décide d'accorder sa confiance du fait que de nombreux autres le font entre à son tour dans la liste des clients faisant confiance au service, et vient ainsi renforcer ce critère pour les autres utilisateurs : le système d'établissement de la confiance est auto-entretenu. C'est un cycle vertueux du point de vue marketing, mais pas du point de vue de la sécurité !

Dans le second cas, la confiance est établie par des vérifications, et s'appuie donc sur des bases plus objectives.

Nous verrons dans le chapitre 5 traitant des certificats comment s'établit techniquement la chaîne de la confiance pour l'utilisation de la cryptographie.

La première étape de l'établissement de la confiance étant de s'assurer de l'identité de son interlocuteur, nous allons maintenant tenter de définir l'identité numérique et de voir comment elle s'établit, se transmet et se vérifie.

Copyright © 2012 Eyrolles.

PARTIE 2

L'identité numérique



Copyright © 2012 Eyrolles.

Copyright © 2012 Eyrolles.

Chapitre 4

La gestion d'identités

La notion d'identité

Dans la vie « réelle », chacun d'entre nous dispose d'une identité « officielle » et, potentiellement, d'un grand nombre d'identités alternatives.

Prenons le cas imaginaire de M. Hégésippe Jean Pascal Dupont-Lenclos.

Depuis toujours, sa maman l'appelle Hégésippe, car il s'agit du prénom qu'elle lui a choisi. Très fière de son ascendance, elle ne comprend pas pourquoi, au travail, il a choisi pour nom d'usage son deuxième prénom, et une forme tronquée de son nom de famille…

Ainsi, professionnellement, notre personnage, cadre dans une grande entreprise, est connu sous le nom de Jean Dupont. C'est aussi sous ce nom que le connaissent la plupart de ses amis.

À son club de billard, ses camarades ne savent pas grand-chose de lui : il est simplement Jeannot, le spécialiste du triple-bande.

Le week-end, Hégésippe chante dans des bals et des concerts sous son nom de scène : John Bridges.

À la maison, ses enfants en bas âge l'appellent papa, et ne le connaissent pour l'instant que sous cette appellation.

Enfin, ce même individu souhaite légitimement être entièrement anonyme lorsqu'il descend dans la rue pour manifester contre la hausse du prix du pain.

Identité d'état civil, nom d'usage, pseudonyme, surnom, anonymat : une même personne peut avoir de nombreuses identités, et l'usage libre de l'une ou de l'autre de ces identités est le garant, tant des grandes fonctions sociales (prouver qui l'on est pour voter, par exemple), que du respect de notre vie privée. Ainsi, Jean serait sans doute très déstabilisé que l'un de ses collègues, ayant assisté un jour par hasard à l'un de ses concerts,

Copyright © 2012 Eyrolles.

se mette à l'appeler John Bridges au cours d'une réunion de négociation stratégique.

Voyons maintenant comment ces notions se déclinent dans l'univers numérique.

L'identité numérique

Sur Internet, média universellement accessible, d'usage quasiment gratuit et indispensable à un grand nombre de services de la vie quotidienne moderne, le sujet de l'identité prend encore une nouvelle dimension. Il existe bien entendu de nombreux contextes dans lesquels l'internaute préfère garder l'anonymat ou employer un pseudonyme plutôt que de révéler son identité.

Mais le problème est plutôt l'inverse : dans un monde où l'anonymat ou l'usage d'un pseudonyme est quasiment la règle, comment peut-on prouver qui l'on est, et inversement, comment vérifier à qui l'on a affaire ?

En effet, le nombre d'utilisateurs de services dématérialisés se compte aujourd'hui en milliards, et pourtant Internet ne s'est pas structuré à la manière d'un pays, dans lequel un registre d'état civil et des titres officiels d'identité permettent à chaque citoyen de prouver son identité, et à chaque service (banque, douane, etc.) de la vérifier.

La fonction d'identification des utilisateurs est donc entièrement laissée à la charge de chaque service dématérialisé. En fonction de la nature et des enjeux du service, les choix pourront être extrêmement différents.

Prenons quelques exemples pour illustrer des cas de figure emblématiques, en commençant par un cas où la sécurité passe avant tout : la banque en ligne.

Accéder à son compte bancaire

L'accès par le titulaire d'un compte en banque à ses fonctions de gestion en ligne a pour préalable la création d'une identité numérique dans le système d'information de la banque. Le contrôle d'accès s'appuie soit sur un couple identifiant/mot de passe, soit sur un certificat, usage qui tend à se répandre du fait des nouvelles obligations prudentielles des banques.

L'utilisation du service en ligne n'est possible que suite à la création du compte bancaire qui donne lieu, en général, à la rencontre physique entre le banquier et le client, le banquier ayant l'obligation de vérifier l'identité du client sur la base de ses papiers.

On peut donc parler d'*identité enregistrée* (la banque vérifie qui vous êtes et vous crée un compte d'accès avec un identifiant qui vous est propre) ou d'*identité certifiée* (dans le cas de l'usage d'un certificat).

Copyright © 2012 Eyrolles.

L'exemple suivant, la réponse aux marchés publics, illustre le fait qu'au sein d'un même service, des fonctions distinctes peuvent entraîner des exigences différentes en termes de gestion des identités.

Répondre à un marché public

La personne qui dépose un pli de réponse à un appel d'offres n'est pas nécessairement le signataire de l'offre : il peut s'agir de tout membre de l'entreprise candidate, d'un coursier externe à la société, voire du facteur si le pli a été envoyé par voie postale.

Il faut donc distinguer deux niveaux d'identité dans la réponse aux marchés publics.

Le dépôt du pli, qui ne nécessite aucun contrôle d'identité, peut être réalisé sur une base *déclarative* voire *anonyme*. Il serait coûteux et contre-productif de forcer chaque secrétaire de service commercial à disposer d'un certificat pour pouvoir déposer les offres !

En revanche, le Code des marchés publics impose que l'acte d'engagement soit signé par une personne habilitée à engager sa société, et le pouvoir adjudicateur a le devoir de vérifier cette signature. L'identité du signataire de l'offre doit donc être *certifiée* avec un niveau de confiance important.

Enfin, ce troisième exemple portant sur le dépôt d'une marque auprès de l'INPI permet de réaliser que même lorsque l'identité est au cœur du service offert, elle n'est pas nécessairement l'objet d'une forte sécurisation.

Déposer une marque à l'INPI

L'Institut national de la propriété industrielle (INPI) est chargé d'enregistrer les dépôts de marques, et a ouvert dans ce but un service sur Internet. On conçoit l'importance que peut revêtir la bonne identification du titulaire d'une marque. Pour autant, le choix a été fait de s'appuyer uniquement sur une *identité déclarative*, le futur titulaire du dépôt de marque remplissant simplement un formulaire dans lequel il saisit ses nom et prénom ou sa dénomination sociale.

Paradoxal ? En fait, non.

En effet, le dépôt de la marque est précédé par une étape de paiement en ligne, et il ne confère à son titulaire que des droits, et aucun devoir susceptible de donner lieu à des sanctions. Dans cette mesure, quel avantage pourrait-il y avoir à déposer une marque au nom d'un tiers ou sous un pseudonyme ?

Ainsi, en l'absence de risque de fraude, une identité déclarative est bien suffisante pour garantir la propriété des marques !

Sur la base de ce dernier exemple, un parallèle avec les réseaux sociaux est intéressant. En effet, on peut très facilement créer un compte sur un réseau social au nom d'un tiers et y enregistrer des informations, véridiques ou non. L'inscription est purement déclarative, aucune vérification d'identité n'est en général effectuée, et les fonctions de base (remplir le profil, par exemple) sont souvent gratuites.

Copyright © 2012 Eyrolles.

Dans les réseaux sociaux, comme pour le dépôt de marque, l'identité du titulaire du compte est le cœur du service – mais il y a deux différences fondamentales entre les deux services.

Tout d'abord, la gratuité de la création de compte enlève à la fois la barrière financière à l'usurpation d'identité, et la traçabilité *via* les informations bancaires.

Ensuite, contrairement à la propriété d'une marque, le fait de diffuser des informations personnelles sur un réseau social peut avoir des conséquences très lourdes pour la personne concernée, notamment en termes d'image. Un individu malintentionné peut ainsi avoir avantage à ternir la réputation d'un tiers en employant un compte usurpé sur un réseau social.

Les services « grand public » se donnent très rarement les moyens de gérer les identités au-delà de la création d'un compte déclaratif et de la gestion de couples identifiant/mot de passe. Cela vient du fait que leur modèle économique n'est pas fondé majoritairement sur la pertinence des informations transmises, mais sur le nombre de visiteurs, le financement étant assuré en grande partie par la publicité.

Pour un service dématérialisé « professionnel », il est impératif d'estimer les risques et les contraintes liés à chacun des rôles présents dans le système afin de définir le mode de création, d'attribution et de gestion des identités numériques, dans les buts d'identification et d'authentification.

Identification et authentification : quelle différence ?

La gestion d'identités et le contrôle d'accès sont fréquemment réunis sous le sigle IAM pour *Identity and Access Management*. Cet acronyme qui reproduit la phrase « I am » (« Je suis » en anglais) nous renvoie à deux notions très proches mais différentes : l'identification et l'authentification, illustrées par la figure 4-1.

S'identifier, c'est dire qui l'on est.

S'authentifier, c'est le prouver.

Par exemple, lorsque l'on décline son nom au téléphone, il s'agit d'une identification. Si le correspondant nous connaît, il nous authentifiera grâce à notre voix.

De manière plus formelle, lors d'une visite chez le médecin, on s'identifie en lui donnant nom, prénom, date de naissance, etc., informations qu'il accepte sans vérification. En revanche, pour bénéficier du remboursement des soins par la Sécurité sociale, il faut s'authentifier en présentant une carte Vitale valide, dont l'un des assurés correspond au nom que l'on a donné au médecin.

Copyright © 2012 Eyrolles.



Figure 4-1 : Identification et authentification

Dans la suite de ce chapitre, nous détaillerons les différents mécanismes de gestion d'identités disponibles pour les concepteurs de services dématérialisés avec, pour chacun, ses qualités, ses limitations et ses cas d'usage les plus courants.

Les différents modes d'identification et d'authentification

Sur Internet, il existe de nombreux cas où une identification et une authentification sont nécessaires. Nous illustrerons les différents modes d'authentification et l'identification sous-jacente au travers de plusieurs mécanismes : mot de passe statique ou dynamique, certificat et question secrète.

Copyright © 2012 Eyrolles.

Nous définirons ensuite les notions d'authentification faible et d'authentification forte, puis nous verrons différentes attaques qui existent contre les modes d'authentification faible.

L'authentification d'un utilisateur par mot de passe

Lorsqu'un internaute crée un compte sur un service dématérialisé, il doit s'identifier en remplissant le formulaire comportant son prénom, son nom, etc. Lors de cette première étape de création de compte, il choisit ou reçoit un « identifiant » (ou *login*) et un « authentifiant » (ou mot de passe, *password* en anglais) qui lui sont personnels.

Une fois le compte créé, pour y accéder de nouveau, il devra présenter l'identifiant et le mot de passe, afin de garantir qu'il est le titulaire légitime du compte.

L'identifiant sert à faire le lien entre son identité et son compte (s'identifier, se présenter) : il est souvent lié au nom du titulaire du compte. Il sera utilisé tout au long de la navigation sur le site pour maintenir une « session ».

Le mot de passe, en revanche, n'est demandé qu'une fois, en début de session. Il s'agit d'un secret que le titulaire du compte est le seul à connaître : le fait de le présenter lui permet de prouver qui il est, donc de s'authentifier, comme illustré sur la figure 4-2.

Ce premier exemple montre que l'identification et l'authentification peuvent reposer sur deux éléments complètement distincts. Le mot de passe peut être modifié sans changer d'identifiant. Toutefois, il doit exister un lien entre les deux qui permet de vérifier que tel mot de passe est bien relié à tel identifiant : c'est le rôle de l'annuaire, ou de la base de données, que de faire ce lien.

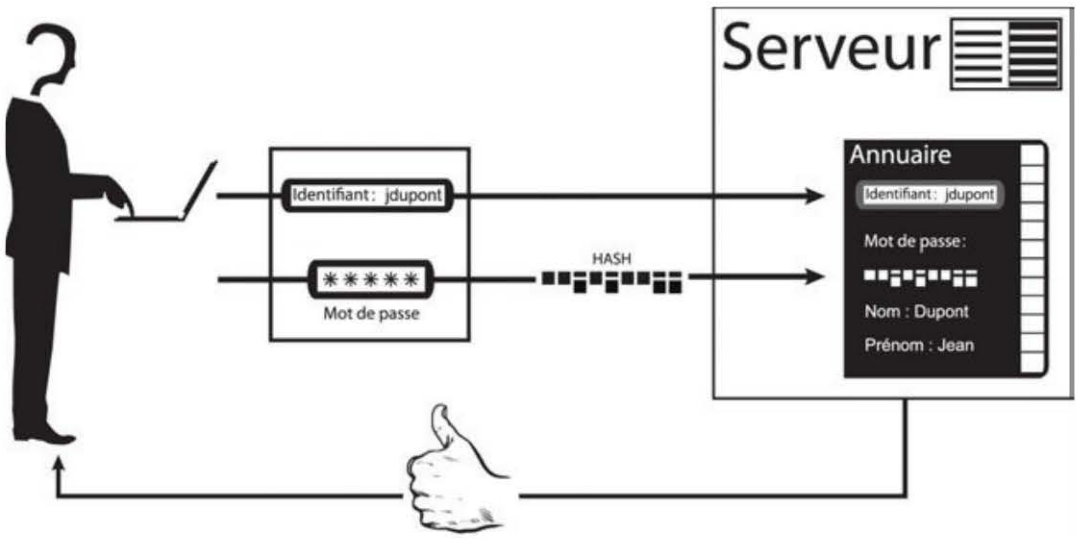


Figure 4-2 : Authentification par mot de passe

Copyright © 2012 Eyrolles.

L'authentification d'un utilisateur par mot de passe à usage unique (OTP)

L'authentification d'un utilisateur par mot de passe à usage unique (OTP, *One-Time Password*) repose sur le même fonctionnement que l'authentification par mot de passe simple (« statique »), sauf que le mot de passe change à chaque authentification. On parle aussi de mot de passe « dynamique ».

Pour pouvoir changer de mot de passe à chaque accès, il est nécessaire de partager un secret entre l'utilisateur et le serveur, le mot de passe étant calculé à partir de ce secret. Il existe de nombreuses façons de faire, et nous allons en décrire quelques-unes.

On notera que l'utilisation d'un OTP nécessite toujours une identification préalable à l'authentification : le serveur saura retrouver le secret de l'utilisateur à partir de son identité, puis se servira de ce secret pour vérifier cette identité.

OTP par dispositif synchronisé

De nombreux systèmes de mot de passe à usage unique reposent sur la possession d'un petit terminal avec affichage, permettant à l'utilisateur de lire le mot de passe, différent à chaque fois, et de le saisir dans l'interface web d'authentification.

La capacité à s'authentifier repose sur la synchronisation entre le terminal de l'utilisateur et le serveur d'authentification : soit les deux dispositifs doivent être à la même date et heure, le mot de passe généré n'ayant qu'une validité limitée dans le temps, soit le nouveau mot de passe est calculé à partir du précédent, soit il est calculé à partir d'un compteur qui est partagé entre le dispositif et le serveur, comme illustré sur la figure 4-3.

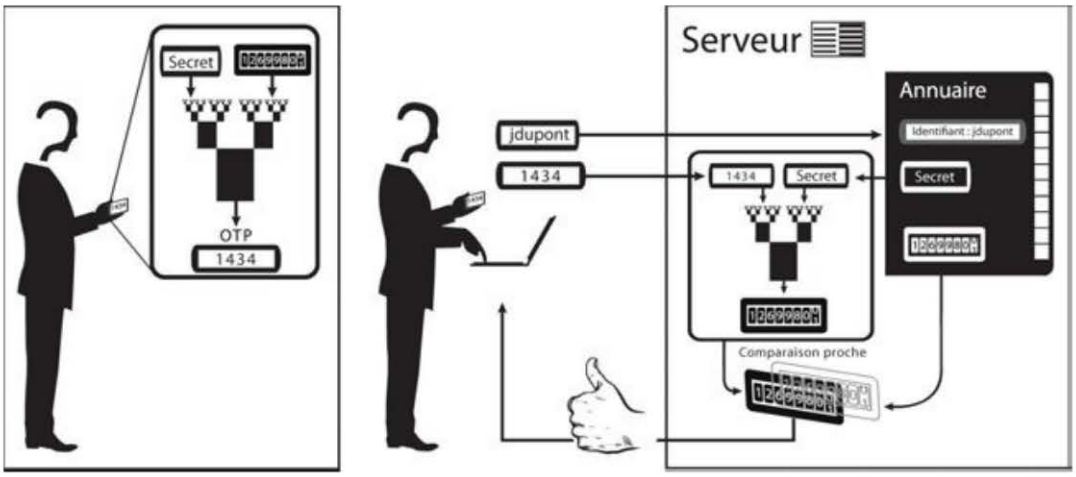


Figure 4-3 : Authentification par mot de passe à usage unique

Copyright © 2012 Eyrolles.

Le mot de passe est le résultat d'un calcul portant, d'une part, sur un secret partagé entre le terminal et le serveur, et d'autre part, sur le compteur. Lors de la vérification, le serveur contrôle que le secret partagé a bien été employé pour faire le calcul, et que le compteur est bien cohérent.

L'identification est nécessairement préalable à l'authentification, puisque le serveur doit d'abord savoir qui est l'utilisateur, aller chercher son secret et son élément synchronisé, pour pouvoir vérifier si l'authentifiant (le mot de passe à usage unique) provient bien de lui.

La faiblesse du dispositif réside dans le risque de désynchronisation : si l'utilisateur demande à son dispositif plusieurs mots de passe successifs sans les présenter au serveur, le compteur du dispositif va avancer indépendamment de celui du serveur, et la prochaine tentative d'authentification échouera. Il faudra alors resynchroniser le dispositif et le serveur, ce qui nécessite l'intervention d'un administrateur.

OTP par utilisation d'un second canal de communication

Le secret partagé entre l'utilisateur et le serveur est ici le second canal de communication, par exemple une adresse e-mail ou un numéro de téléphone mobile.

Lorsque l'utilisateur, préalablement enregistré, souhaite accéder au service, il s'identifie comme représenté sur la figure 4-4. Le serveur lui fait alors parvenir un mot de passe généré aléatoirement (aussi appelé « code d'accès ») sur le second canal de communication, et lui présente un champ de saisie pour le code d'accès.

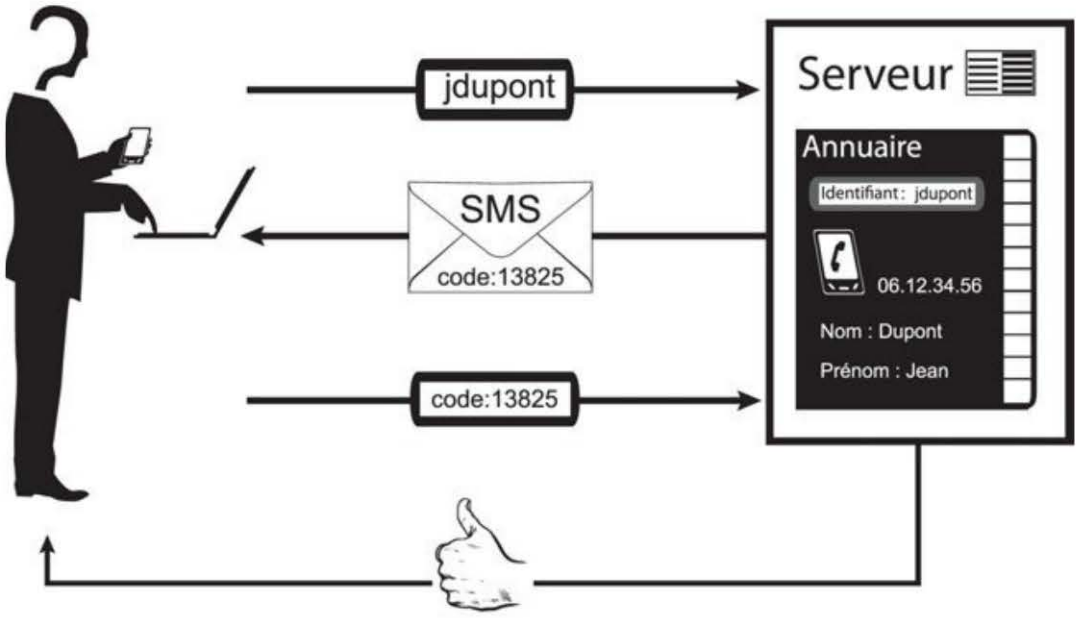


Figure 4-4 : Authentification par second canal

Copyright © 2012 Eyrolles.

L'utilisateur reçoit le SMS ou l'e-mail contenant le code d'accès, le renseigne, et le serveur peut ainsi vérifier que la personne avec qui il communique a bien un accès au second canal de communication.

Ce type de dispositif fait reposer la sécurité de l'authentification sur celle du second canal d'authentification. Ainsi, en volant le téléphone mobile d'un utilisateur, ou en usurpant un accès à sa boîte e-mail, il est possible de se faire passer pour lui. Ce type de mécanisme est couramment utilisé en renfort d'une authentification par mot de passe classique, pour disposer d'un mode d'authentification à deux facteurs.

OTP par papier

Il est possible de générer des mots de passe à usage unique en remettant à un utilisateur une grille imprimée comprenant des chaînes de caractères aléatoires.

Lorsque l'utilisateur souhaite accéder au service, il s'identifie, ce qui permet au serveur de connaître la grille unique attribuée à cet utilisateur. Il lui demande alors de saisir le contenu d'une ou plusieurs cases de cette grille, par exemple les cases A2, C8 et E3.

Si l'utilisateur est capable de donner les valeurs contenues dans ces cases, c'est qu'il est en possession de la bonne grille.

Bien entendu, le risque est le vol de la grille papier, qui permet l'usurpation d'identité. Pour en faire un mode d'authentification à deux facteurs, on peut coupler la remise de la grille avec celle d'un secret, par exemple un ordre de parcours de la grille. Dans ce cas, l'utilisateur sait qu'il doit parcourir sa grille, par exemple vers le haut puis vers la gauche. Le serveur lui donne la case de départ : B3. L'utilisateur devra renseigner les valeurs comprises dans les cases A3 (au-dessus de B3) et A2 (à gauche de A3). Ainsi, la seule possession de la grille papier ne suffit pas à usurper l'identité du porteur légitime.

L'authentification d'un serveur et d'un utilisateur par certificat : le protocole SSL (TLS)

Le protocole TLS (*Transport Layer Security*), toujours couramment désigné par son ancien nom, SSL (*Secure Socket Layer*), sert de base à la sécurité des échanges sur le réseau public Internet.

Lorsque l'internaute se connecte à un serveur sécurisé par ce protocole, l'URL (l'adresse Internet à laquelle le serveur est localisé) est modifiée, le préfixe « http:// » étant remplacé par « http**s**:// ». Graphiquement, un cadenas ou une clé apparaît, et dans certains navigateurs, la couleur d'affichage de l'URL est modifiée. Ces changements d'affichage sont toutefois subtils pour le grand public.

Copyright © 2012 Eyrolles.

Un « défi » est un test transmis par celui qui veut vérifier une identité, la « réponse » est le retour du candidat à l'authentification. Ces éléments peuvent prendre des formes différentes mais sont le fondement de toute authentification.

Nous allons ici décrire deux modes d'établissement d'une session sécurisée SSL : l'authentification du serveur seul, puis l'authentification réciproque, le serveur et l'utilisateur se reconnaissant mutuellement à l'aide de leurs certificats respectifs.

L'authentification d'un serveur par certificat

Lorsque l'internaute se connecte à l'URL du serveur (par exemple, *https://www.leserveur.com*), comme illustré dans la figure 4-5, son navigateur envoie au serveur un défi, constitué d'une chaîne d'octets aléatoires.

Le serveur réalise sur ce défi un calcul mathématique appelé « réponse », en employant sa clé privée. Il renvoie alors au navigateur la réponse, ainsi que son certificat d'authentification.

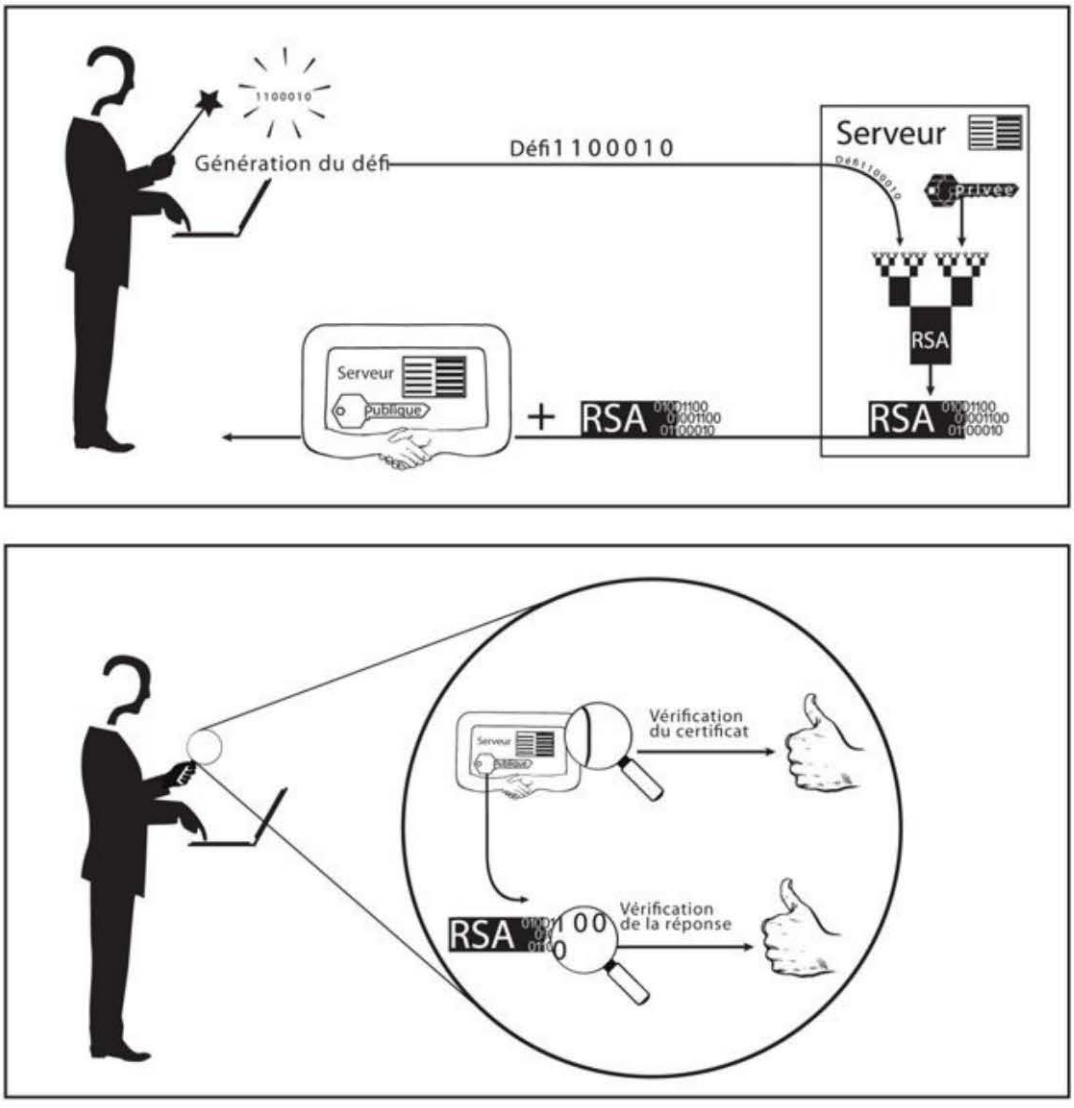


Figure 4-5 : Authentification SSL d'un serveur

Copyright © 2012 Eyrolles.

Grâce au certificat, le navigateur peut vérifier si la réponse correspond bien au défi, et ainsi acquérir la certitude que le serveur avec lequel il communique est bien le titulaire du certificat. La première étape réalisée est donc l'authentification.

Le navigateur vérifie ensuite que l'URL du serveur est bien celle qui est inscrite dans le certificat : c'est l'étape d'identification. Si la vérification est correcte, le navigateur donnera accès au site et indiquera à l'internaute par un pictogramme (cadenas fermé ou clé) qu'il est sur un site sécurisé dont l'authenticité a été vérifiée. Dans le cas contraire, un avertissement lui sera présenté.

Dans cet exemple, l'identification est réalisée grâce au certificat, et l'authentification grâce au couple défi/réponse.

Nota Bene : nous verrons plus loin que le moyen d'authentification du serveur est sa clé privée, et le lien qui existe entre clé privée et certificat.

Cet exemple montre que l'identification et l'authentification peuvent être réalisées sans une base d'identités prédéfinie : le navigateur de l'internaute ne dispose pas d'un annuaire ou d'une base de données pour vérifier la légitimité du site web, et l'internaute peut accéder au serveur dès sa première visite, sans effectuer une étape préalable de vérification ou de déclaration. La vérification reposera toutefois sur une base d'« autorités de certification de confiance » préenregistrées, permettant de vérifier la validité du certificat du serveur. Nous détaillerons cette notion dans le chapitre sur la chaîne de la confiance.

Il est à noter qu'à l'issue de la phase d'authentification du serveur, le serveur et le navigateur établissent un canal sécurisé garantissant la confidentialité des échanges ultérieurs. Pour cela, le navigateur génère aléatoirement une « clé de session » qui servira à chiffrer l'ensemble des échanges, la rend confidentielle à l'aide de la clé publique du serveur, et la lui envoie. Le serveur prend connaissance de la clé de session à l'aide de sa clé privée, comme illustré dans la figure 4-6.

Ainsi, ce canal sécurisé permettra ensuite à l'internaute de s'authentifier par identifiant et mot de passe sans qu'un tiers puisse prendre connaissance de son mot de passe. Mais la sécurité de l'authentification de l'utilisateur est plus grande si l'on procède à l'aide d'un certificat, comme décrit ci-dessous.

Copyright © 2012 Eyrolles.

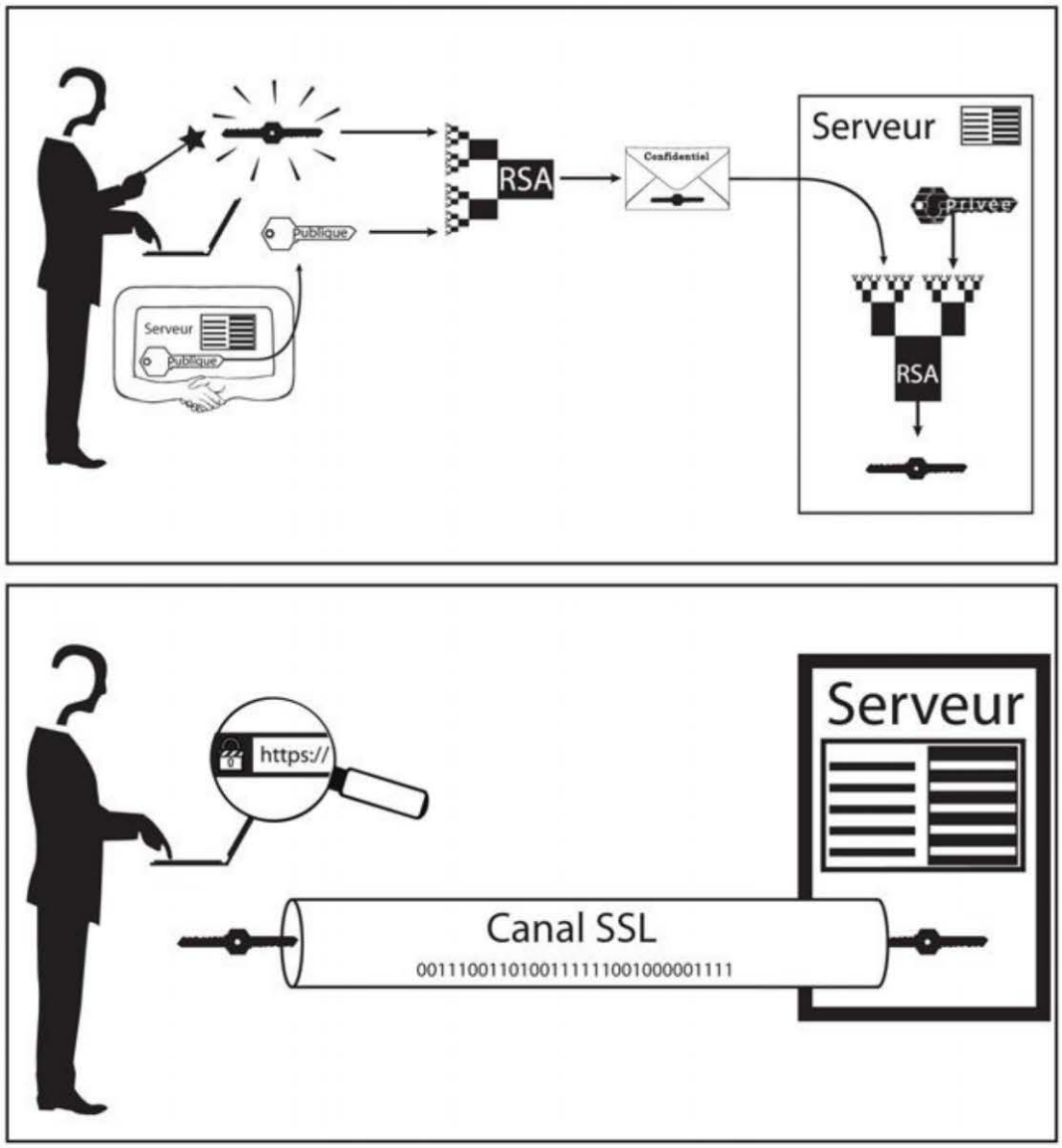


Figure 4-6 : Établissement du canal sécurisé SSL

L'authentification d'un utilisateur par certificat

Lorsque l'on souhaite authentifier un utilisateur par certificat, l'étape de création de compte est identique à celle de l'authentification par mot de passe, à une exception près : au lieu de recevoir un identifiant et de choisir un mot de passe, l'utilisateur devra présenter son certificat.

Lors des accès ultérieurs, le serveur contrôle l'identité de l'utilisateur afin de lui donner accès au service. Ce mode d'authentification est appelé « défi/réponse » et est illustré par la figure 4-7.

Quand l'utilisateur demande l'accès au service, il procède tout d'abord à l'établissement d'une session SSL avec authentification forte du serveur

Copyright © 2012 Eyrolles.

comme décrit ci-dessus. Le même mécanisme d'authentification est alors réalisé dans l'autre sens par le serveur ; ce dernier envoie au navigateur de l'internaute un « défi », constitué d'une chaîne d'octets aléatoires.

Le navigateur demande à l'utilisateur l'autorisation d'utiliser sa clé privée pour réaliser, sur ce défi, un calcul mathématique appelé « réponse ». Il renvoie alors au serveur la réponse, ainsi que le certificat d'authentification correspondant à la clé privée employée.

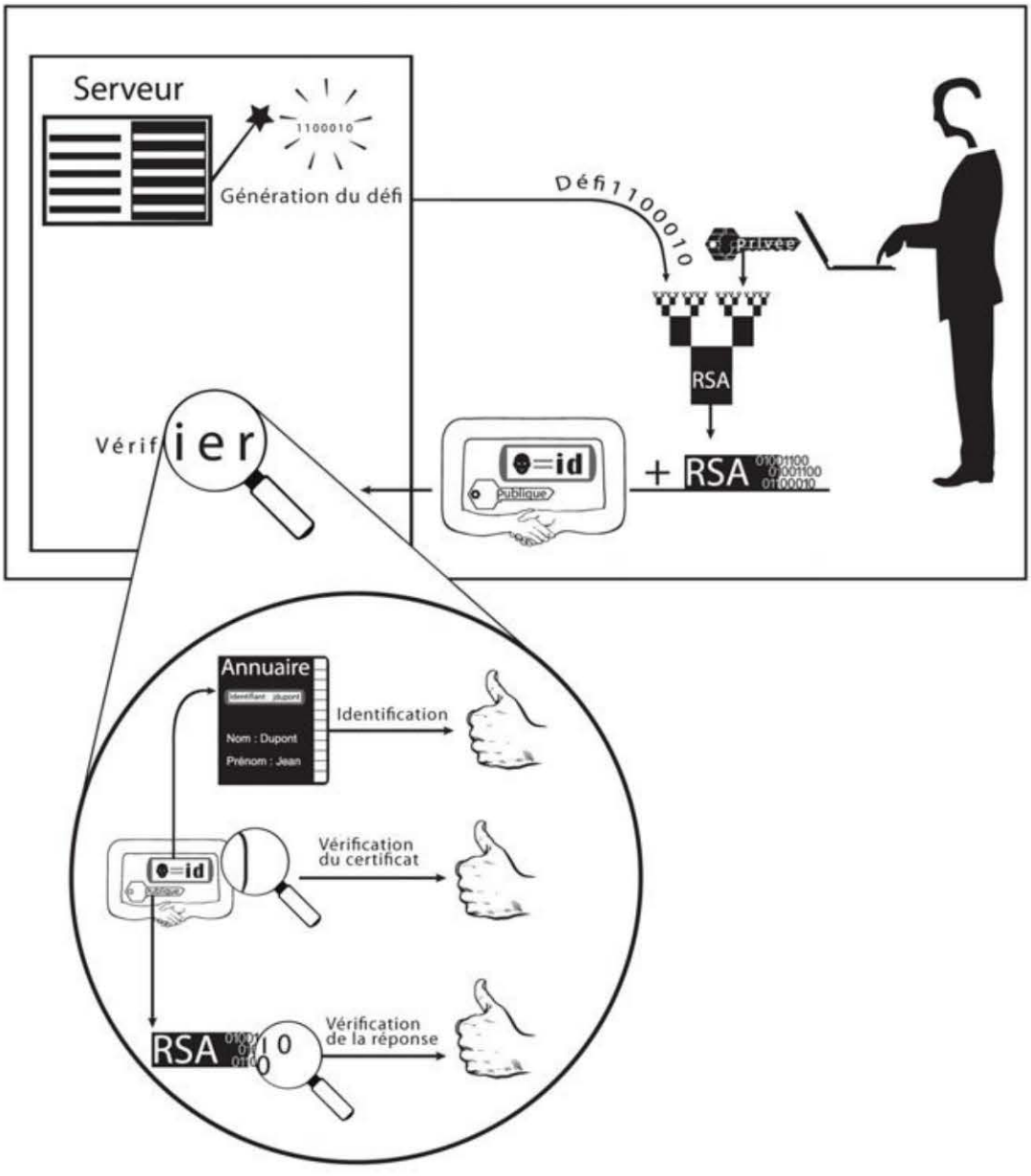


Figure 4-7 : Authentification SSL réciproque

Copyright © 2012 Eyrolles.

Grâce au certificat, le serveur vérifie si la réponse correspond bien au défi, et acquiert ainsi la certitude que l'utilisateur avec lequel il communique est bien le titulaire du certificat. La première étape réalisée est donc l'authentification.

Le serveur s'assure ensuite que le certificat correspond à un compte enregistré pour le service : c'est l'étape d'identification. Si la vérification est correcte, le serveur autorise l'accès de l'utilisateur au site.

Dans cet exemple, l'identification est réalisée grâce au certificat, et l'authentification grâce au couple défi/réponse.

Nota Bene : dans le cas d'une authentification réciproque par certificat, le canal sécurisé permettant les échanges confidentiels est établi à l'issue de la double authentification. La clé de session est toujours choisie par le navigateur de l'internaute, jamais par le serveur.

L'authentification par question secrète

Lorsqu'un service dématérialisé impose à ses utilisateurs l'emploi de certificats pour s'authentifier, il peut arriver qu'un utilisateur ne soit plus en possession de ce certificat (par exemple, en cas de perte) ou qu'il ne soit plus en mesure de l'utiliser (par exemple, en cas d'expiration).

Pour accéder au service, l'utilisateur doit alors acquérir un nouveau certificat, et le déclarer auprès du service pour qu'il soit associé à son compte (lien identification/authentification).

Mais comment permettre à l'utilisateur de déclarer un nouveau certificat dans ce cas ? En effet, pour effectuer cette nouvelle déclaration, l'utilisateur doit préalablement prouver qu'il est bien le titulaire légitime du compte. Or, il doit pour cela s'authentifier avec son certificat… dont il ne dispose plus !

Si l'on permet le changement de certificat sans vérification préalable, on ouvre la porte à l'usurpation d'identité, puisqu'un tiers pourrait déclarer son propre certificat et ainsi s'attribuer le compte de manière illégitime.

Contrairement à ce que l'on a vu dans l'exemple précédent pour les serveurs (vérification de l'URL contenue dans le certificat), on ne peut pas s'appuyer sur l'identité de la personne contenue dans le certificat. D'une part, il existe des homonymes (Jean Dupont est-il bien *le* Jean Dupont qui a ouvert le compte ?), et d'autre part, l'orthographe du nom n'est pas certaine, le champ *Common Name* utilisable à cette fin comportant une concaténation du prénom et du nom sans ordre défini, sans règle systématique sur les accents, sur les éventuels traits d'union et apostrophes contenus dans le nom, sans garantie sur l'éventuel second prénom, etc.

Une façon de résoudre le problème est de demander à l'utilisateur, au moment de la création de son compte, de choisir une question parmi une liste, et de saisir la réponse à cette question. Les questions choisies seront

Copyright © 2012 Eyrolles.

suffisamment intimes pour qu'il soit vraisemblable que l'utilisateur soit le seul à connaître la réponse : héros préféré de son enfance, nom de jeune fille de sa mère, nom de son premier animal domestique… Mais il arrive aussi que l'on utilise tout simplement la date de naissance.

Ainsi, le serveur autorisera le changement du certificat sous réserve que l'utilisateur présente sa réponse secrète à la question prédéfinie. On pourra coupler ce contrôle avec, par exemple, la vérification que le certificat remplacé est bien révoqué ou expiré (on sait ainsi qu'il est légitime de le remplacer, ce qui réduit le risque d'usurpation), ou avec l'emploi d'un mot de passe à usage unique ou d'un lien d'activation envoyé par e-mail à une adresse définie lors de la création du compte.

La question secrète sera également utilisée lors de l'accès de l'utilisateur au support téléphonique : autant il est malaisé de présenter un mot de passe par téléphone, autant répondre à une question est simple, et il y a peu de risque d'oublier une donnée intime, contrairement à un mot de passe que l'on utiliserait rarement.

Cet exemple est fondamental pour appréhender l'ensemble des cas d'usage de l'authentification dans la dématérialisation : il ne suffit pas de distribuer des moyens d'authentification, il faut également se doter des moyens sécurisés de les changer périodiquement, de les révoquer, de les retrouver en cas d'oubli. L'interlocuteur, dans ces cas d'usage, ne sera pas toujours la machine mais parfois un service support, comme le service de révocation de certificat opéré par un prestataire de services de certification électronique.

Voyons maintenant sur quels critères choisir le mode d'authentification à un service dématérialisé.

Choisir un mode d'authentification

Authentification forte et authentification faible

Nous venons de voir qu'il existe plusieurs paradigmes d'identification et d'authentification, qui entraînent des contraintes différentes et offrent des niveaux de sécurité différents. On parlera d'authentification « faible » ou d'authentification « forte » selon la robustesse du mécanisme, l'objectif *in fine* étant de pouvoir accorder sa confiance à l'identification.

On parlera d'authentification faible lorsque l'une des conditions suivantes est remplie :

- l'authentification repose sur un seul secret : elle est alors sensible aux attaques par *phishing* ou par *key logger* (voir plus loin) ;
- l'authentification est rejouable, ce qui signifie que c'est toujours la même information qui circule à chaque demande d'accès. Elle est alors sensible aux attaques par écoute et rejeu.

Copyright © 2012 Eyrolles.

Le mot de passe ou la question secrète constituent des modes d'authentification faible.

On parlera en revanche d'authentification forte lorsqu'elle repose sur deux secrets ou deux canaux distincts de communication, et lorsqu'elle n'est pas rejouable.

L'usage d'un certificat présent sur un support cryptographique physique (carte à puce ou clé USB) constitue un mode d'authentification forte, puisqu'il faut disposer de la carte et de son code secret (deux éléments) pour s'authentifier, et que le couple défi/réponse change à chaque authentification.

On peut également constituer une authentification forte en combinant deux modes d'authentification faible, par exemple un mot de passe et un code à usage unique envoyé par SMS.

Mettre en œuvre un niveau de sécurité adapté

Le fait qu'il existe des niveaux de sécurité différents pour l'authentification ne signifie pas qu'il faille rejeter d'emblée la plus faible et n'employer systématiquement que l'authentification forte.

Il convient d'adapter les moyens mis en œuvre à la fois aux risques encourus et aux contraintes rencontrées lors de la mise en place du service.

Ainsi, déployer des certificats pour contrôler l'accès du grand public à un téléservice purement déclaratif serait une erreur, les contraintes liées au coût d'acquisition du certificat et à la complexité de l'installation n'étant justifiées ni par l'enjeu ni par la fréquence d'utilisation. Le risque encouru est alors de voir le service peu voire pas utilisé.

Illustrons ce propos par quelques exemples concrets.

Planet Limousin : la gestion des demandes d'aide auprès de la région Limousin

La région Limousin a mis en œuvre au sein de la plate-forme « Planet Limousin » la gestion des demandes d'aide adressées à la région pour la création ou le développement des entreprises. Il semble difficile de demander à un futur créateur d'entreprise d'acheter un certificat juste pour pouvoir demander une aide, qu'il n'est pas certain d'obtenir. Il a donc été décidé de procéder à une authentification par identifiant et mot de passe, qui permet non seulement de déposer sa demande et de la suivre, mais également de procéder à une signature électronique selon le processus « à la volée » que nous décrivons dans le chapitre 7 consacré à ce sujet.

Voyons maintenant le cas de l'Ineris, qui met en œuvre le téléservice « Réseaux et canalisations », destiné à recenser les réseaux terrestres, aériens et subaquatiques pour les formalités préalables aux travaux.

Copyright © 2012 Eyrolles.

Parole d'expert

Michel Treins, DSI de l'Ineris

Au sein du téléservice « Réseaux et canalisations », vous avez mis en œuvre des modes d'authentification différents pour les diverses catégories d'utilisateurs : mot de passe, certificat RGS (**), certificat RGS (***). Comment avez-vous fait ce choix ?

Dès la phase d'étude de faisabilité et avant même le lancement officiel du projet, des cas d'usage différenciés par profils d'utilisateurs ont été envisagés.

Une étude risques/bénéfices montre que le niveau de sécurité maximal n'est pas toujours souhaitable dans les services dématérialisés. Nous avons mis en balance les menaces potentielles liées aux différents types d'acteurs avec les enjeux, et notamment le risque de non-adhésion des utilisateurs au service proposé si celui-ci est trop contraignant. L'étude de sécurité EBIOS a ensuite confirmé notre intuition initiale et nous a amenés à définir des politiques différenciées selon les profils d'utilisateurs, dans une démarche avant tout pragmatique. Notre choix a été déterminé pour chaque population par le rapport qualité/prix global, la qualité comprenant la valeur ajoutée en termes de sécurité et le prix global incluant le poids du changement et le risque de contournement ou de rejet.

Ainsi, pour la population des déclarants qui viennent chercher sur le téléservice la liste des exploitants de réseaux concernés par le chantier qu'ils prévoient, la marche à gravir pour mettre en œuvre l'authentification forte est trop haute : le risque de non-déclaration des chantiers est bien supérieur au risque d'usurpation d'identité. Les informations gérées sur le téléservice étant publiques, la fiabilité des informations remises et la traçabilité de cette remise sont plus importantes que la certitude de l'identité du demandeur. Nous avons donc permis une authentification par mot de passe.

Pour les exploitants de réseaux qui viennent enregistrer leurs ouvrages pour alimenter le référentiel du téléservice, la manifestation du consentement lors de la déclaration est essentielle, ce qui nous a amenés à mettre en œuvre la signature électronique. Le coût marginal pour amener cette catégorie d'acteurs à l'authentification forte est très faible, puisque le même certificat peut servir à s'authentifier et à signer. Nous avons donc fait le choix de certificats RGS (**).

Les administrateurs techniques du service, enfin, disposent de très forts privilèges en termes d'accès aux données et d'actions sur le logiciel. S'agissant d'une population réduite en nombre et bien connue, pour laquelle le circuit de délivrance de certificats est maîtrisé, nous avons opté pour des certificats d'authentification RGS (***), qui ne présentent pas de surcoût par rapport aux certificats (**).

Le téléservice permet également des échanges papier avec certains acteurs du processus. Selon vous, les échanges papier offrent-ils une sécurité meilleure ou dégradée par rapport aux échanges dématérialisés ?

Les échanges papier offrent une sécurité bien moindre que les échanges électroniques ! La chaîne globale de la sécurité est donc plus faible à chacun de ses maillons dans un processus papier.

La signature manuscrite n'est pas apposée à l'issue d'un processus formalisé et sécurisé d'enregistrement du signataire, elle ne permet pas de contrôle de validité

Copyright © 2012 Eyrolles.

et ne comprend pas d'horodatage fiable et précis. On est donc obligé d'appliquer la théorie juridique du mandat apparent.

L'intégrité des documents papier n'est pas garantie, les possibilités de compromission et de falsification sont bien plus fortes qu'en électronique. De plus, les procédures d'archivage papier sont bien moins exigeantes, même réglementairement, que pour l'archivage électronique.

Enfin, les manipulations humaines font naître un risque d'erreur et de perte qui est également une source de compromission. L'audit des documents et la traçabilité des informations sont bien moindres en papier que par voie dématérialisée.

Mais alors, pourquoi avoir néanmoins mis en œuvre un processus papier ?

Toujours par souci de pragmatisme !

Le téléservice « Réseaux et canalisations » s'adresse à des populations diverses, et certaines sont peu au fait ou ont peu le goût des technologies de la dématérialisation. Les utilisateurs ont besoin de temps pour s'adapter. La conduite du changement ne peut faire abstraction de cette période de découverte.

Nous envisageons dès 2013 d'aller vers des moyens intermédiaires, avec notamment la signature électronique à la volée employant le téléphone mobile comme canal d'authentification. En effet, pour déployer à très grande échelle des procédés de confiance, avec des niveaux de sécurité plus ou moins élevés, il faut s'appuyer sur des outils déjà déployés à très grande échelle et proches de la personne. Le téléphone mobile remplit ces critères et sera un soutien incontournable au déploiement de la dématérialisation dans les années à venir.

Le choix d'un mode d'authentification doit résulter d'une véritable étude de sécurité, comme nous le verrons dans le chapitre 14 dédié à ce sujet. Il faut prendre en compte la sensibilité des données, les risques encourus, la population concernée, les impacts financiers et organisationnels, mais aussi les moyens alternatifs de parade des risques : responsabilisation des utilisateurs par l'usage d'une politique de sécurité mettant leurs moyens d'authentification sous leur contrôle exclusif, ou assurance par rapport aux dommages éventuels.

Pour les cas où l'étude de sécurité nous amène à faire le choix d'un contrôle d'accès par identifiant et mot de passe, abordons maintenant les bonnes pratiques à mettre en œuvre pour la gestion de ces deux éléments.

Du bon usage des identifiants et des mots de passe

Comment constituer un identifiant

La première caractéristique d'un identifiant est d'être unique au sein du référentiel (de l'annuaire) : deux utilisateurs ne peuvent pas avoir le même identifiant.

Copyright © 2012 Eyrolles.

La seconde caractéristique d'un identifiant est de « représenter » l'utilisateur. Il fera le lien entre l'utilisateur et ses données ou ses droits au sein du service.

Pour le concepteur d'un service dématérialisé, le choix du mode de constitution des identifiants doit être fait avec un soin tout particulier. En effet, il existe plusieurs pièges qu'il convient d'éviter.

Les services web ont facilement trouvé la parade à l'oubli de mot de passe en mettant en œuvre le renvoi du mot de passe par e-mail, ou la possibilité de le réinitialiser en cas de perte. En revanche, pour les services auxquels on accède rarement, il peut arriver que l'on oublie son identifiant. Il n'y a alors souvent pas moyen de l'obtenir à nouveau, ce qui peut entraîner une paralysie du service.

La fabrication automatique de l'identifiant est possible : nom de famille, concaténation du prénom et du nom, avec ou sans majuscule, séparés ou non par un point ou un tiret, concaténation de l'initiale et du nom, du nom et d'un chiffre s'il y a des homonymes… Le nombre d'identifiants « probables » pour un même utilisateur est très grand et le risque d'oubli ou de mélange entre les identifiants correspondant à différents services dématérialisés est donc élevé, ainsi que l'inconfort qui en résulte.

L'usage de l'adresse e-mail comme identifiant tend à se répandre, pour deux raisons simples : l'utilisateur ne risque pas de l'oublier, et elle le désigne en général de manière unique. Toutefois, il existe des cas où ce choix n'est pas pertinent, par exemple s'il existe une seule adresse e-mail pour la famille, à laquelle tout le monde accède (cas d'usage très répandu) : le risque est fort de donner accès aux enfants à un service destiné aux parents. Dans certaines entreprises, il existe également des adresses e-mail « génériques », attribuées à un ensemble de personnels (la comptabilité, le secrétariat…). Si le service dématérialisé nécessite la traçabilité précise de l'individu, l'usage d'une telle adresse e-mail comme identifiant sera problématique.

Une alternative est le libre choix de l'identifiant par l'utilisateur : il a alors de fortes chances de mieux s'en souvenir, mais il rencontrera des difficultés si ses identifiants « habituels » sont déjà utilisés par un autre abonné au service lorsqu'il vient s'y inscrire. Si « jean.dupont », « jdupont » et « jean-dupont » ne sont plus disponibles, le système proposera en général un identifiant de la forme « jdupont75 », pas nécessairement évident à retenir.

L'existence d'homonymes rend délicat le choix d'une règle de constitution d'identifiants.

Enfin, pour certains types de services, il peut être utile d'employer des identifiants « anonymes », c'est-à-dire sans aucun rapport avec l'identité de l'utilisateur, par exemple une suite de lettres ou de chiffres aléatoires : « 59863569 » ou « VGFYUIVG ». Parmi les cas d'usage, citons le vote électronique, pour lequel il peut être important de savoir qu'un utilisateur dispose d'un droit de vote, sans pouvoir faire le lien avec son identité.

Copyright © 2012 Eyrolles.

La constitution des identifiants prendra donc en compte :

- la population concernée (grand public ou professionnel, individualisée ou groupée en services…) ;
- la probabilité d'homonymie (en fonction du nombre de personnes utilisant le service) ;
- la finalité de l'identifiant (usage rare, risque d'oubli important poussant à l'usage de l'adresse e-mail, usage fréquent garantissant la mémorisation, anonymat requis ou exclus) ;
- l'existence ou non d'un référentiel préexistant (annuaire d'entreprise, par exemple), qui plaide pour la réutilisation d'identifiants déjà connus des utilisateurs ;
- la probabilité de fusionner à terme avec un autre référentiel : il sera alors nécessaire de choisir des modes de constitution d'identifiants qui garantissent leur unicité entre les deux référentiels.

Comment choisir et gérer les mots de passe

La question du choix du mot de passe s'adresse à la fois au concepteur du système de gestion d'identités et aux utilisateurs des services.

En effet, le concepteur du service peut imposer une politique de constitution des mots de passe contraignant les utilisateurs à choisir un mot de passe « fort ». Sa force peut se calculer, par exemple, en fonction du temps qu'il faut pour le trouver à l'aide d'une attaque « force brute » ou d'une attaque par dictionnaire.

Une attaque « force brute » consiste à essayer toutes les combinaisons possibles jusqu'à trouver la bonne. Elle peut être réalisée sur des mots de passe, mais aussi sur des clés cryptographiques.

Les contraintes les plus fréquemment imposées sont :

- une taille minimale du mot de passe (l'ANSSI recommande ainsi des mots de passe d'au moins 10 caractères, et de préférence de 16 caractères) ;
- l'utilisation conjointe de majuscules et de minuscules ;
- l'utilisation conjointe de lettres et de chiffres ;
- l'utilisation de caractères non alphanumériques (parenthèse, apostrophe, point d'exclamation…).

La limite à l'application de telles politiques est la capacité de l'utilisateur à retenir un mot de passe complexe… Ou plutôt un grand nombre de mots de passe complexes, puisque de nombreux services reposent sur ce mode d'authentification. Il est bien entendu déconseillé d'utiliser le même mot de passe pour tous les services, afin d'éviter qu'une « fuite » de l'un des services ne soit préjudiciable aux autres.

Ainsi, en imposant des mots de passe trop complexes et trop longs, on court le risque que les utilisateurs notent leur mot de passe sur un Post-it

Copyright © 2012 Eyrolles

ou dans un fichier conservé sur leur ordinateur, ce qui réduit à néant la sécurité du dispositif.

Sécurité contre capacité de mémorisation : un équilibre difficile.

Pour constituer un mot de passe « fort » que l'on puisse tout de même mémoriser, les moyens sont assez nombreux.

- On pourra, par exemple, traduire une phrase phonétiquement : g3k7viDo pour « j'ai trois cassettes vidéo ».
- On pourra prendre les premières lettres d'une phrase : Djvpl'aà3 pour « Demain je vais prendre l'air à Troyes ».
- On pourra remplacer certaines lettres d'un mot par des caractères qui leur ressemblent : CItr0u1!!e pour « Citrouille »…

La politique de sécurité pourra également imposer un changement périodique des mots de passe, par exemple tous les deux mois, en vérifiant que l'utilisateur ne réemploie pas le même mot de passe trop fréquemment.

Enfin, la gestion de la fonction « mot de passe oublié » doit être étudiée avec soin. Il existe trois modes principaux de réalisation de cette fonctionnalité.

- Le mot de passe est renvoyé à l'utilisateur par e-mail. Pour ce faire, le service conserve une base de données des mots de passe en clair. Il devient alors difficile de considérer que le mot de passe est sous le contrôle exclusif de son titulaire, les exploitants système ayant accès à la plate-forme. Il est préférable de ne pas disposer dans l'annuaire du mot de passe entier, mais seulement de son hash (voir le chapitre 2), de manière à pouvoir le vérifier sans en disposer.
- Le mot de passe est réinitialisé avec une valeur aléatoire. Ce nouveau mot de passe est transmis à l'utilisateur par e-mail, avec la possibilité ou l'obligation de le changer au premier usage.
- L'utilisateur reçoit par e-mail un lien de réinitialisation, d'une durée de validité limitée : ce lien le dirige vers une page sur laquelle il saisit son nouveau mot de passe, dans le respect des contraintes imposées par la politique de sécurité.

Les attaques contre les mots de passe… et leurs réponses

L'attaque par dictionnaire

L'attaque par dictionnaire est une forme d'attaque « force brute » qui consiste à tenter un grand nombre de fois consécutif de s'authentifier à la place de l'utilisateur, en présentant des mots de passe probables, et en espérant trouver le bon.

Cette attaque repose sur le fait que les mots de passe employés en pratique sont très souvent, pour des raisons mnémotechniques, des mots existants, des noms propres ou des dates.

Copyright © 2012 Eyrolles.

Les mots de passe probables sont ainsi constitués d'un ensemble de mots, de leurs combinaisons et de leurs différentes orthographes en changeant la casse, ou *via* des modifications d'ordre phonétique.

Sa variante exhaustive, la force brute, consiste à tester toutes les valeurs possibles d'un mot de passe par combinaisons successives des caractères du clavier. Elle ne fonctionne que sur des mots de passe courts.

On se protège contre ces attaques de quatre manières.

- Du côté de l'utilisateur, on réduit le risque en employant des mots de passe « forts », comme nous l'avons vu précédemment.
- Du côté du serveur, il est possible de limiter le nombre de tentatives d'authentification successives avec le même identifiant, et de bloquer le compte, par exemple, après trois tentatives erronées. Il suffit de mettre en œuvre un blocage pour une durée limitée (10 minutes, par exemple) pour que l'attaque devienne impossible, la probabilité de trouver le mot de passe en essayant trois fois toutes les 10 minutes étant très faible.
- Le serveur peut également ajouter la nécessité de saisir un *captcha*, c'est-à-dire présenter à l'utilisateur une image déformée de lettres et de chiffres, que l'utilisateur doit saisir. Le but est de vérifier que c'est bien un humain qui accède au service, et non un robot, et ainsi d'éviter les attaques par présentation systématique de mots de passe. C'est ce que l'on appelle un test de Turing.[1]

L'acronyme captcha signifie *Completely Automated Public Turing test to tell Computers and Humans Apart.*

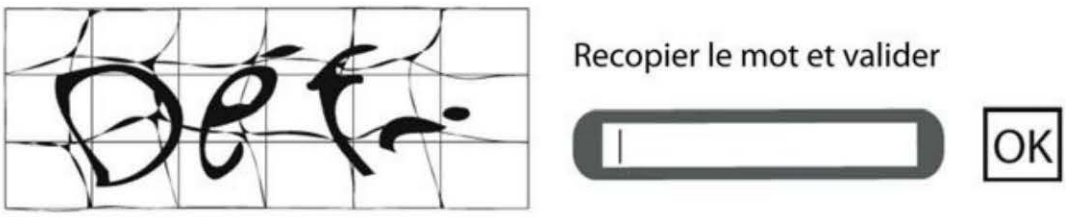


Figure 4-8 : Le captcha

- Enfin, toujours côté serveur, il est possible de détecter les « comportements déviants » afin de bloquer les comptes attaqués. Ce mode de protection entre dans le domaine de la détection d'intrusion.

Le key logger

Un key logger est un programme informatique placé sur l'ordinateur d'un utilisateur dans le but d'enregistrer les saisies réalisées au clavier. Le programme conserve toutes ces informations et les met à disposition du pirate qui l'a placé, soit en les lui envoyant par e-mail ou *via* le Web, soit en sauvegardant l'ensemble de ces données dans un fichier qu'il viendra chercher directement sur la machine.

Copyright © 2012 Eyrolles.

Il suffit alors de parcourir les traces et de trouver celle qui correspond au mot de passe pour pouvoir se faire passer pour l'utilisateur.

Mettre en place un key logger nécessite d'accéder à la machine, soit par un accès direct (par exemple, par un collègue qui disposerait de la machine laissée sans surveillance et non verrouillée, ou par un administrateur système), soit par une *backdoor*, c'est-à-dire un accès à distance créé *via* un programme malveillant appelé « cheval de Troie », qui se diffuse comme tous les virus informatiques lors de l'exécution d'un programme non contrôlé, d'une macro ou encore *via* un e-mail.

On s'en protège en employant un bon antivirus, mais il est très difficile de détecter la présence d'un key logger « artisanal ».

L'écoute et le rejeu

Contrairement au key logger, qui permet de prendre connaissance du mot de passe directement sur le poste de l'utilisateur, l'écoute consiste à s'en emparer lors de sa transmission sur le réseau.

L'écoute nécessite des moyens techniques relativement importants, mais est à la portée de tout administrateur système d'une entreprise, ou de tout exploitant d'un cybercafé, par exemple.

Afin d'éviter l'écoute des mots de passe, nous disposons de deux mécanismes de sécurité.

Tout d'abord, il est possible de ne jamais faire circuler le mot de passe lui-même, mais seulement son hash (voir le chapitre 2) : lors de la saisie du mot de passe par l'utilisateur, le navigateur calcule le hash de ce dernier et c'est cette donnée qui est transmise au serveur. Le serveur lui-même ne dispose pas du mot de passe dans son intégralité mais seulement du hash. Ainsi, l'utilisateur est le seul à disposer du mot de passe, qui ne circule jamais. Il est néanmoins possible d'écouter le hash et de le rejouer en contournant la page d'accueil par un envoi direct des informations de connexion au serveur.

On rendra l'écoute véritablement impossible en procédant à l'authentification de l'utilisateur au sein d'une session sécurisée par le protocole SSL/TLS. L'établissement préalable d'un canal chiffré entre l'utilisateur et le serveur garantit que nul ne puisse surprendre les données qui circulent. Pour plus de détails sur ce mode de sécurisation, on se reportera, dans ce chapitre, à la section SSL/TLS.

Le phishing

Le terme « phishing » est composé de deux mots *phone fishing*, c'est-à-dire « pêche par téléphone ». Il s'agit du mode le moins technique et le plus facile de piratage des mots de passe, puisqu'il repose sur les concepts d'ingénierie sociale.

Copyright © 2012 Eyrolles.

Le principe en est simple : il consiste à contacter un utilisateur et de lui inspirer confiance pour l'amener à donner son mot de passe.

« Allô, ici Untel, de la DSI. Il y a un problème sur votre compte, apparemment certains e-mails ne vous parviennent pas… Pourriez-vous me donner votre mot de passe afin que nous puissions procéder à des tests ? »… Et le tour est joué !

Une alternative très employée est l'envoi d'e-mails d'apparence officielle demandant la transmission en retour d'informations confidentielles, ou contenant un lien qui dirige vers un faux site ressemblant à celui du service, où l'utilisateur renseignera son mot de passe sans méfiance.

La grande force de l'authentification forte, notamment par certificat sur support physique, est qu'elle ne permet pas la mise en œuvre du phishing : même si l'utilisateur imprudent donnait son code PIN, il faudrait disposer de sa carte à puce pour pouvoir l'utiliser.

La principale parade face au phishing est la sensibilisation, la formation, le rappel fréquent des règles de confidentialité. La probabilité qu'un utilisateur non averti se laisse dépouiller de son secret est très élevée. Elle baisse sensiblement dans les populations correctement informées.

Rappelons au passage que le principal maillon faible de la chaîne de sécurité est l'humain, et que 80 % des attaques de systèmes d'information viennent « de l'intérieur ». Il est infiniment plus facile d'obtenir de manière frauduleuse un vrai moyen d'accès que de forcer les barrières techniques très robustes mises en œuvre dans les systèmes d'information modernes !

Quelques exemples emblématiques de projets de gestion d'identités

Constituer un référentiel d'entreprise

La constitution d'un annuaire d'entreprise représente un projet en soi, dont la complexité est multiple.

- L'annuaire ainsi constitué formera la base incontournable sur laquelle toutes les applications du système d'information s'appuieront, ce qui en fait un élément clé pour le succès des autres projets de dématérialisation de l'entreprise.
- L'existant est en général conséquent : dans toute grande structure, on trouve de nombreux annuaires, gérant des ensembles d'utilisateurs différents pour des applications différentes (ressources humaines, applications métier, annuaire téléphonique…).
- L'existant n'est en général pas fiable : on constate généralement que 20 % des entrées d'un annuaire d'entreprise sont totalement ou

Copyright © 2012 Eyrolles.

partiellement erronées (employés ayant changé de poste, numéros de téléphone ou adresse e-mail non tenus à jour, situation hiérarchique obsolète, voire noms ou dates de naissance incorrects, et surtout droits d'accès non actualisés).

- La matière traitée dans l'annuaire est par nature évolutive, et le projet ne consiste pas simplement à regrouper des informations existantes, mais à concevoir et mettre en œuvre les procédures et outils permettant leur maintien en cohérence dans l'avenir, en prenant en compte les évolutions structurelles de l'entreprise, mais aussi les nouvelles applications qui y seront déployées.

C'est pourquoi, paradoxalement, alors que les employés sont l'essence même de l'entreprise, la constitution d'un annuaire fiable n'est pas une tâche aisée.

Sans entrer dans le détail technique des formats X.500, du protocole LDAP et de la synchronisation des annuaires, nous allons aborder deux notions essentielles pour le déploiement de la gestion d'identités dans les entreprises : le méta-annuaire et le *Single Sign-On* (SSO).

Annuaire et méta-annuaire

Comme nous l'avons vu précédemment, du fait de la multiplicité des applications qui composent un système d'information d'entreprise, les référentiels d'utilisateurs y sont systématiquement nombreux.

Le projet d'optimisation de l'annuaire se trouve alors face à un choix structurant : créer un annuaire unique, sur lequel s'appuieront l'ensemble des services du SI, ou interconnecter les annuaires existants de manière à garantir leur cohérence et leur homogénéité.

La première option nécessite de tels travaux d'adaptation des applications existantes que son coût et sa complexité sont en général prohibitifs.

La seconde solution constitue ce que l'on appelle un « méta-annuaire », c'est-à-dire un référentiel centralisé regroupant les informations de tous les annuaires et bases de données de l'entreprise, dans le but de les fédérer et de les synchroniser.

Le méta-annuaire regroupe donc trois fonctions :

- le stockage des données, en général au sein d'un annuaire LDAP ;
- des connecteurs avec les autres annuaires et bases de données du système d'information ;
- un ensemble de règles de synchronisation, de vérification, d'actualisation, gérées par un moteur de règles, pour diffuser les mises à jour entre le référentiel central et les référentiels annexes *via* les connecteurs.

La dimension technique du projet de méta-annuaire met donc en œuvre le LDAP et les connecteurs, tandis que la dimension organisationnelle et

Copyright © 2012 Eyrolles.

métier définit les règles de tenue à jour à partir de et vers les annuaires secondaires « opérationnels ».

Le SSO

Le *Single Sign-On*, ou SSO, est le mécanisme par lequel un utilisateur pourra, après s'être authentifié une seule fois sur le système d'information, accéder à différents services.

Ainsi, par exemple, l'ouverture de session sur l'ordinateur permettra de se connecter à la messagerie, à la gestion des ordres de mission, aux logiciels métier, etc.

Le principal apport du SSO consiste à réduire le nombre de saisies de mots de passe nécessaires, allégeant ainsi la charge de l'utilisateur en termes de mémorisation d'une part, et de temps passé à la saisie d'autre part. Il évite ainsi le recours trop fréquent à la fonction « mot de passe oublié ». Par ailleurs, la multiplication des mots de passe n'est que la partie la plus simple du problème : c'est souvent le nombre important d'identifiants qui pose un problème de mémoire.

Le SSO permet en outre de mutualiser entre plusieurs applications une politique de sécurité commune, par exemple sur la sécurité du mot de passe : robustesse, fréquence des changements obligatoires…

Techniquement, le SSO repose en général sur un service d'authentification centralisé s'appuyant sur un méta-annuaire. Lorsqu'un utilisateur tente d'accéder à un service, ce dernier vérifie d'abord si l'utilisateur dispose d'un jeton d'authentification en cours de validité. Si tel est le cas, il laisse accéder l'utilisateur en fonction de ses droits. Dans le cas contraire, l'utilisateur est redirigé vers le service d'authentification, qui vérifiera son identité avant de lui délivrer le fameux jeton et de le ramener vers le service demandé.

Le jeton d'authentification est un petit fichier structuré, souvent un cookie géré par le navigateur, comportant l'identité (l'identifiant) de l'utilisateur, une date d'expiration et éventuellement un ensemble de droits. Le jeton peut être scellé cryptographiquement de manière à en garantir l'intégrité et la provenance, et chiffré de pour en préserver la confidentialité.

Le renouvellement du jeton après expiration se fait de manière transparente pour l'utilisateur et ne requiert pas, en général, une nouvelle saisie du mot de passe.

Il existe des modèles dans lesquels l'authentification n'est pas centralisée, plusieurs systèmes d'authentification séparés partageant seulement une politique de sécurité commune. Le SSO tendra alors vers la fédération d'identités, que nous aborderons plus loin dans ce chapitre, dans la section consacrée aux utilisateurs externes au SI.

Copyright © 2012 Eyrolles.

Le risque principal du SSO se situe dans les conséquences d'une usurpation d'identité : si un utilisateur malveillant se procure un identifiant et un mot de passe valides, il a accès d'un seul coup à l'ensemble des applicatifs auxquels l'utilisateur légitime a droit. Pour réduire ce risque, il est recommandé de mettre en place le SSO sur la base d'une authentification forte, par exemple par certificat ou par mot de passe à usage unique.

Parole d'expert

Jean Denuzière, directeur commercial d'Ilex, éditeur des solutions de gestion d'identités Meibo et Sign and Go

Quelles sont les principales difficultés que l'utilisation d'un méta-annuaire et d'un SSO permettent de solutionner au sein d'un système d'information ?

Sans référentiel central d'authentification, il est impossible de mettre en œuvre une politique de sécurité fiable dans une grande entreprise.

La mise en place d'un annuaire de sécurité permet de recenser la population concernée, la qualifier et définir les habilitations. C'est sur ce référentiel tenu à jour selon des procédures rigoureuses que s'appuie le contrôle d'accès : lors de toute demande d'accès, le SSO vérifie si l'utilisateur existe, et s'il a le droit de consulter l'information ou le service demandé.

Un référentiel d'identités centralisé évite l'existence pour le même utilisateur de profils divers et parfois contradictoires. Les contrôles d'accès mieux effectués améliorent l'efficacité du système d'authentification, ce qui induit un gain important de sécurité.

Du point de vue de l'utilisateur, la mutualisation de l'authentification évite les pertes de mots de passe et des échecs de connexion à répétition, qui engorgent les helpdesks et engendrent au sein de l'entreprise des coûts et du mécontentement.

Les coûts d'administration induits par un méta-annuaire centralisé et un SSO sont bien moindres que ceux qui découlent d'une architecture répartie : le retour sur investissement est quasiment immédiat. Chacun conserve la maîtrise et l'attribution des rôles sur ses applications, sans avoir à supporter le poids de l'exploitation technique.

Enfin, la traçabilité et l'audit sont facilités, avec une faculté native d'anonymisation vis-à-vis des partenaires auditeurs.

Selon vous, la fédération d'identités permettra-t-elle à terme aux internautes de disposer d'une identité numérique unifiée ?

C'est la lettre au Père Noël ! Mais le rêve est déjà réalité dans certaines communautés d'internautes et certains sites, qui ont un grand besoin de fluidité dans la navigation.

La fédération d'identités permet de partager l'identité en créant un « cercle de confiance » *via* un contrat de fédération. Grâce au jeton de sécurité fourni par le « fournisseur d'identités » au moyen de standards d'échanges sécurisés, les fournisseurs de services permettent aux utilisateurs de passer d'un site à l'autre sans devoir s'authentifier à nouveau.

Copyright © 2012 Eyrolles.

Nous mettons couramment en œuvre ces technologies : on peut, par exemple, citer un grand groupe de média et un groupe bancaire de dimension internationale, pour lesquels des liens fédérant l'identité sont même inclus automatiquement dans les principaux réseaux sociaux. Même si l'authentification unifiée sur l'ensemble d'Internet n'est pas encore d'actualité, elle est indubitablement en marche grâce aux grands acteurs, qui en sont le moteur. La fédération d'identités devrait se généraliser à un rythme accéléré dans les années à venir : les solutions techniques sont prêtes... et les utilisateurs sont demandeurs !

Permettre l'enregistrement d'utilisateurs externes

Les services dématérialisés sont en général destinés à permettre à des utilisateurs d'y accéder ! Dans certains services, les utilisateurs sont identifiés à l'avance : par exemple, une banque pourra proposer à ses clients de souscrire en ligne de nouveaux produits ou services. La base des utilisateurs potentiels est alors connue puisqu'il s'agit des clients de la banque.

En revanche, dans une majorité de services, les utilisateurs ne sont pas connus *a priori*, et doivent pouvoir s'inscrire pour utiliser le service. Nous allons aborder trois manières de procéder à cette inscription, puis nous évoquerons un facilitateur : la fédération d'identités.

L'inscription en ligne

La création d'un compte d'utilisateur est souvent déclarative : l'internaute remplit un formulaire dans lequel il renseigne son identité, ses coordonnées, ainsi que les autres informations utiles au service auquel il s'inscrit. Un contrôle élémentaire est souvent réalisé sur la base de l'adresse e-mail déclarée, *via* l'envoi d'un lien d'activation du compte ou l'envoi du mot de passe.

L'intérêt de l'inscription déclarative réside dans son extrême simplicité et son immédiateté. Son inconvénient principal est qu'il est très facile d'usurper l'identité d'un tiers en s'inscrivant à sa place. On ne compte plus, par exemple, les cas de faux comptes créés sur les réseaux sociaux.

Dans certains cas, la création de compte peut être renforcée par un contrôle : l'utilisateur peut être invité à fournir *via* Internet un scan de papiers d'identité, à renvoyer par courrier un contrat signé, voire à se déplacer pour valider la création de son compte dans une agence. Si une procédure de ce type ajoute beaucoup de fiabilité au compte créé, elle a également un coût important en termes de délais et de temps de traitement pour la vérification des pièces justificatives.

Il existe une troisième option, qui consiste à authentifier les utilisateurs à l'aide d'un certificat électronique émis par un prestataire de services de certification électronique (PSCE).

Copyright © 2012 Eyrolles.

Si le niveau de sécurité exigé pour les certificats est suffisamment élevé (par exemple, RGS (**), ou à l'avenir les certificats labellisés Idénum), le fournisseur du service dématérialisé a la certitude que le porteur de certificat a bien présenté des pièces justificatives de son identité lors de la procédure d'enregistrement qui a donné lieu à la délivrance de son certificat. Il est ainsi possible de « déléguer » les contrôles d'identité nécessaires à la création du compte au PSCE qui a délivré le certificat. Le coût lié à la vérification des pièces justificatives est couvert par le prix payé pour l'obtention du certificat, et repose alors sur l'utilisateur.

En cas de contentieux relatif à l'identité de l'utilisateur, il peut être envisagé de se retourner vers le PSCE pour lui demander les justificatifs de l'enregistrement. Il convient toutefois de vérifier que la politique de certification du PSCE autorise l'utilisation de ses certificats pour le service dématérialisé concerné.

La fédération d'identités

Nous avons vu dans le cadre de la constitution d'un référentiel d'entreprise qu'il était possible, à l'aide du SSO, de centraliser l'authentification d'un utilisateur pour lui donner accès à plusieurs services. Le rôle de la fédération d'identités est de réaliser la même fonctionnalité à une échelle plus large, au-delà d'un système d'information contrôlé par une seule entreprise.

Le principe consiste à créer un « cercle de confiance » dans lequel un ou plusieurs « fournisseurs d'identités » rendent un service d'authentification à des fournisseurs de services dématérialisés.

Ainsi, comme dans le cas du SSO, l'utilisateur qui souhaite accéder à un service est orienté vers le fournisseur d'identités, auprès duquel il a préalablement ouvert un compte, et qui l'authentifie. Il est alors redirigé vers le fournisseur de services avec un jeton d'authentification, et l'identifiant correspondant au service.

Lorsqu'il accède à un deuxième service du même cercle de confiance, le fournisseur d'identités procédera à la redirection avec l'identifiant correspondant au deuxième service.

Ainsi, en s'authentifiant une seule fois, l'utilisateur accède à des services sans aucun rapport les uns avec les autres, si ce n'est d'appartenir à un même cercle de confiance.

L'un des intérêts principaux de la fédération d'identités est la centralisation de l'authentification. En effet, si le mode d'authentification choisi est le certificat, il est complexe pour un utilisateur, lors du renouvellement de son certificat, de déclarer son nouveau certificat sur tous les services auxquels il est inscrit. Grâce à la fédération d'identités, il n'aura à faire cette

Copyright © 2012 Eyrolles.

opération qu'auprès d'un seul fournisseur d'identités, ce qui constitue une simplification majeure de la procédure.

Nous allons consacrer le chapitre suivant à l'étude de cet outil indispensable à la dématérialisation : le certificat.

Copyright © 2012 Eyrolles.

Chapitre 5

Le certificat, une carte d'identité numérique

Qu'est-ce qu'un certificat ?

Parallèle avec les titres d'identité

Dans la vie courante, lorsqu'un individu doit s'authentifier, on lui demande fréquemment de présenter « ses papiers ». Selon le cas, il pourra s'agir d'une carte d'identité (par exemple, pour justifier de sa signature sur un chèque à la caisse du supermarché), d'un passeport (pour franchir une frontière), d'un permis de conduire (pour prouver son droit de conduire un véhicule motorisé), d'un badge professionnel (pour justifier d'un droit d'accès à un bâtiment), d'une carte d'étudiant (pour accéder à la bibliothèque ou bénéficier d'une réduction au cinéma), etc.

Propriétés des titres d'identité

Tous les titres d'identité sont destinés à identifier ou authentifier leur porteur. À cette fin, ils comportent des informations sur la personne : prénom, nom, date et lieu de naissance, photographie, signature, adresse, etc.

Certains d'entre eux sont officiels, délivrés par les pouvoirs publics ; d'autres, non. Les différents papiers sont identifiables au premier regard, leur nature et leur provenance sont clairement lisibles. Ils comportent souvent un numéro unique permettant de les identifier et de faire le lien avec le porteur.

En fonction de leur nature et de leur origine, ils n'auront pas la même force probante vis-à-vis de l'interlocuteur à qui on le présente. Ainsi, la caissière du supermarché n'acceptera pas une carte d'étudiant comme justificatif d'identité pour un chèque, et une carte d'identité ne suffira pas à un citoyen français pour se rendre aux États-Unis (alors qu'elle suffit pour se rendre en Tunisie). A *contrario*, une carte d'identité ne donnera pas accès à un local professionnel sécurisé car elle n'atteste pas de l'appartenance de la personne à l'entreprise.

Copyright © 2012 Eyrolles.

Contenu d'un certificat

Pour afficher le contenu d'un certificat installé sur un PC, on peut, par exemple, lancer Internet Explorer et se rendre dans le menu Outils/Options Internet, puis sur l'onglet Contenu et enfin cliquer sur le bouton Certificats (figure 5-1).

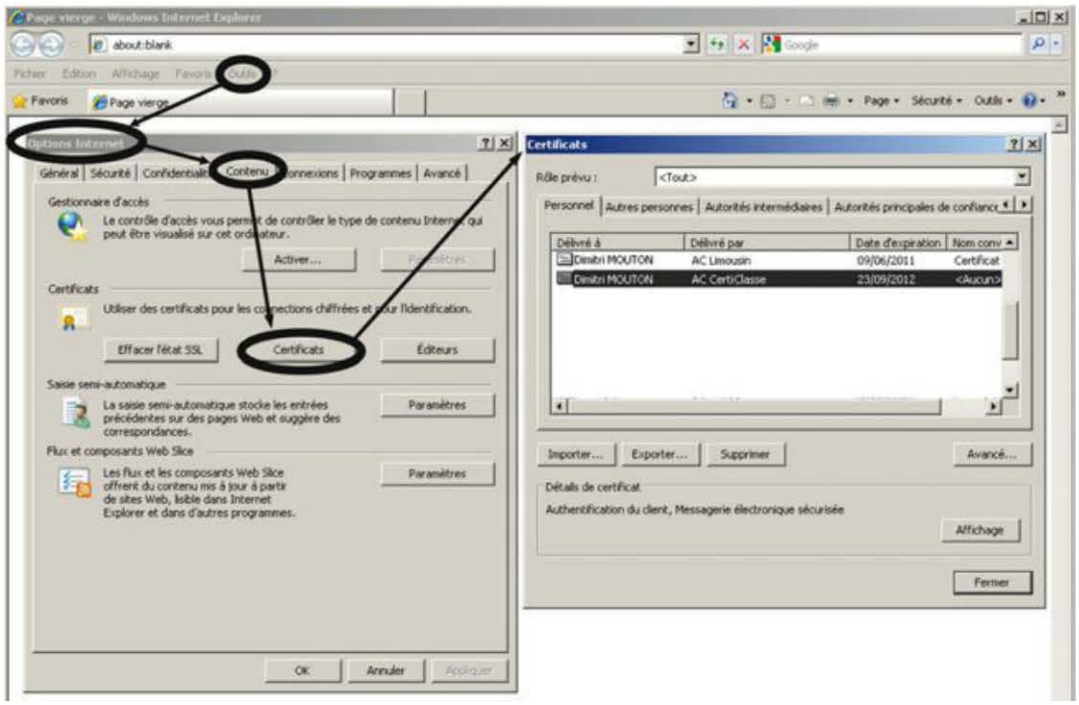


Figure 5-1 : Accès au contenu d'un certificat

Une fenêtre s'affiche alors pour présenter la liste des certificats disponibles sur le poste de travail. En double-cliquant sur la ligne d'un certificat, on en affiche le contenu. La figure 5-2 illustre le parallèle entre le contenu du certificat et celui d'une carte d'identité. Au dos de la carte, on trouve :

- la date d'émission et la date limite de validité, qui correspondent aux dates de validité du certificat ;
- la désignation, le tampon et la signature de l'entité qui a procédé à l'émission du titre, à mettre en parallèle avec le prestataire de services de certification électronique (PSCE) qui a délivré le certificat, présent dans le champ Émetteur.

Au recto de la carte, trois informations sont intéressantes :

- le nom et le prénom du porteur, qui figurent dans le certificat dans le champ Objet ;
- le numéro de carte d'identité renvoie au numéro de série du certificat, qui est unique au sein de la « famille de certificats » délivrée par le PSCE ;

Copyright © 2012 Eyrolles.

- la signature manuscrite figurant sur la carte d'identité constitue un équivalent fonctionnel de la « clé publique » du porteur, comme nous allons l'illustrer dans le paragraphe suivant.

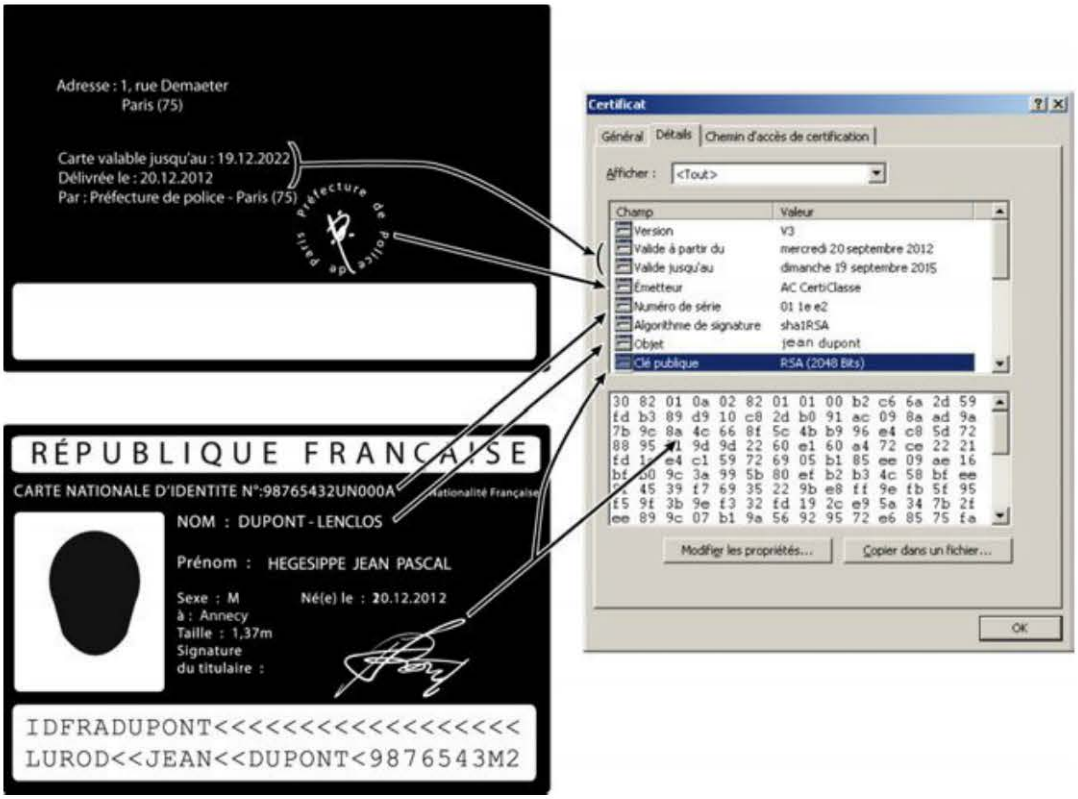


Figure 5-2 : Le certificat : une carte d'identité électronique

Pour ce qui est des différences, notons que la photographie, qui figure de manière indispensable sur la carte d'identité, n'est qu'une option dans le certificat. Cela se justifie pleinement par le fait que l'on soit rarement en présence physique du signataire d'un document électronique, ce qui ne donne que peu de valeur ajoutée à la présence de sa photographie.

Vérifier une identité avec une carte d'identité et avec un certificat

Dans le monde matériel, vérifier l'identité d'une personne à l'aide de sa carte d'identité se fait de la manière suivante : on compare les éléments présents sur la carte avec des éléments objectifs ou subjectifs physiquement disponibles.

Par exemple, pour vérifier une signature sur un chèque, la caissière vérifie que la photo correspond bien au signataire, que le nom sur la carte est bien le même que sur le chèque, et que la signature ressemble à celle qui a été faite sur le chèque. Elle note ensuite au dos du chèque le type de titre vérifié et son numéro.

Copyright © 2012 Eyrolles.

Ainsi, on s'appuie sur la présence physique du titulaire de la carte pour faire des comparaisons qui démontrent la vraisemblance de l'identité de la personne.

Dans le monde électronique, la personne dont on souhaite vérifier l'identité se trouve à distance. La vérification d'identité est réalisée le plus souvent par une machine, sur des critères purement objectifs. La comparaison de la photo avec le visage du porteur est ainsi fort difficile à mettre en œuvre, et il en va de même pour un signe graphique comme la signature manuscrite.

La vérification d'identité sur la base d'un certificat doit donc passer par d'autres critères, de nature mathématique. L'authentification d'une personne (ou d'un serveur) s'appuie sur trois éléments :

- la nature du certificat : s'il a été émis par un prestataire de services de certification électronique (PSCE) auquel on a attribué sa confiance (voir le chapitre 3 sur la notion de confiance), alors les informations qu'il contient sont fiables ;
- les dates de validité du certificat, ainsi que son statut de révocation (voir la section suivante de ce chapitre sur le cycle de vie du certificat), afin de s'assurer que le titre est toujours fiable ;
- les fonctions cryptographiques offertes par le certificat : la clé publique incluse dans le certificat doit permettre de vérifier un calcul effectué par le porteur sur la base de sa clé privée. Si cette vérification est correcte, l'interlocuteur dispose bien de la clé privée et il est donc bien le porteur légitime du certificat. Dans le cas contraire, on doit rejeter l'utilisateur.

Pour la vérification de l'identité, le parallèle entre papiers d'identité et certificat peut donc se résumer au tableau suivant.

Tableau 5-1 : Parallèle entre papiers d'identité et certificat

	Papiers d'identité	Certificat
Émetteur	L'émetteur du titre d'identité est légitime : le tampon qui figure sur la carte et la nature de la carte permet de le vérifier.	L'émetteur est légitime : il s'agit d'un PSCE auquel le vérificateur a accordé sa confiance.
Titre	La carte est en cours de validité.	Le certificat est en cours de validité. Le certificat n'est pas révoqué.
Porteur	Le porteur correspond au titre : il ressemble à la photo ou il est capable de reproduire la signature manuscrite.	Le porteur dispose de la clé privée correspondante, ce qu'il a prouvé en faisant un calcul que l'on a pu vérifier à l'aide de la clé publique.

Copyright © 2012 Eyrolles.

Attention : nous verrons dans la section « La chaîne de la certification » de ce chapitre, plus particulièrement le paragraphe dédié aux différents niveaux de sécurité des certificats que, selon le niveau choisi, le certificat peut être comparé à une carte d'identité… ou à une simple carte de visite !

La notion de confiance accordée à un PSCE est détaillée dans le présent chapitre à la section « La chaîne de la certification ». Les notions de clé privée et clé publique, ont été abordées au chapitre 2 dans la section dédiée à la cryptographie, et la notion de révocation sera étudiée dans la section de ce chapitre dédiée au cycle de vie du certificat.

Le certificat en tant qu'objet technique

Le format du certificat

Un certificat est un fichier contenant des informations sur les usages qui peuvent en être faits et sur son porteur. Il est structuré selon le modèle de la famille X.500 de l'UIT (qui sert de base également à la conception des annuaires LDAP). Il est scellé par son émetteur, communément appelé « autorité de certification ».

Le format des certificats est décrit par la norme X.509v3, reprise dans la norme RFC 5280. Il n'y a aucune différence fondamentale entre un certificat de personne physique, de serveur ou d'autorité de certification.

Les principales parties du certificat, que nous allons détailler ici, sont les suivantes :

- les informations sur le porteur du certificat ;
- les informations techniques sur le certificat et la clé publique certifiée ;
- les informations sur les usages qui peuvent être faits du certificat ;
- les informations sur l'émetteur du certificat ;
- le scellement du certificat par son émetteur.

L'ensemble des informations contenues dans les certificats d'une même famille forment ce que l'on appelle le « profil » du certificat.

Les détails donnés dans le présent chapitre ne sont pas exhaustifs, mais reprennent l'essentiel de l'esprit de la norme, à laquelle on se référera pour de plus amples informations. Nous n'aborderons pas, en particulier, la notion d'extensions « critiques ».

Les informations sur le porteur du certificat : le Distinguished Name

Le *Distinguished Name* (DN ou nom distinctif en français) est la partie du certificat qui décrit le porteur de ce certificat, aussi parfois appelé de manière un peu cavalière l'« objet ».

Pour un serveur, le champ DN comportera principalement le nom de domaine du serveur (sous-partie de l'URL).

Copyright © 2012 Eyrolles.

Pour une personne physique, le DN comporte en général les attributs suivants :

- *Common Name* (CN) : le nom du porteur, composé par la concaténation de son prénom et de son nom ;
- *Email* (E) : l'adresse e-mail du porteur ;
- *Country* (C) : le pays de l'autorité de certification émettrice du certificat ;
- *Organization* (O) : l'entreprise (ou équivalent) d'appartenance du porteur ;
- *Organizational Unit* (OU, champ multivalué) : l'entité d'appartenance du porteur, ou le numéro SIRET de l'entreprise référencée dans le champ O.

D'autres champs peuvent être ajoutés dans le DN : localité, titre, prénom, nom, initiales, pseudonyme, adresse postale, et même des données biométriques, telles que la photo du porteur ou l'image de sa signature manuscrite… Toutefois, il n'existe aucune obligation.

L'usage fait des champs O et OU peut varier d'un émetteur de certificat à l'autre ou selon les pratiques en vigueur dans différents pays, ce qui limite parfois l'interopérabilité des certificats puisqu'une application ne saura pas nécessairement quelle information précise s'y trouvera.

Le principal inconvénient de cette norme est l'utilisation de l'attribut *Common Name* pour identifier une personne. Ce champ présente en effet deux défauts.

D'une part, il fait reposer l'identification d'une personne sur son prénom et son nom, qui ne sont pas uniques, car il existe des homonymes. Cela rend le principal champ d'identification inopérant pour les systèmes automatisés, et force à se replier sur une autre donnée, telle que le numéro de série. Or, lorsqu'un utilisateur change de certificat, il change aussi de numéro de série, et le serpent se mord ainsi la queue. On garde la possibilité de saisir un identifiant unique d'utilisateur dans l'attribut de pseudonyme, par exemple, mais cela restreint l'usage du certificat au seul service pour lequel cet identifiant a été créé : si le porteur utilise son certificat pour accéder à son compte bancaire et à son intranet, il y a peu de chances que son identifiant soit le même sur les deux services.

D'autre part, l'ordre dans lequel sont concaténés le prénom et le nom n'est pas normalisé. L'usage des champs prénom et nom séparés étant très rare, il n'est pas possible de déduire automatiquement du certificat les éléments d'identification de son porteur, par exemple pour préremplir un formulaire.

Les informations techniques sur le certificat

Les informations techniques sur le certificat sont de plusieurs natures :

- des éléments purement techniques :
  - la version du certificat identifie la version de la norme X.509 à laquelle il est conforme. Dans la pratique, on y trouvera toujours la valeur 2 désignant la version V3 ;

Copyright © 2012 Eyrolles.

  - le numéro de série du certificat, qui est un numéro unique parmi les certificats du même émetteur ;
- la clé publique sur laquelle porte le certificat :
  - le type de clé (le plus souvent RSA) ;
  - la clé publique elle-même, sous la forme d'une suite d'octets, qui sera utilisée pour faire les calculs RSA, par exemple lors des vérifications de signatures électroniques ;
- des éléments servant à la vérification de la validité du certificat :
  - les dates de validité du certificat, sous la forme de deux champs, début de validité et fin de validité ;
  - le point de distribution de la liste de certificats révoqués (CRLDP), qui sera utilisé pour vérifier la validité du certificat (voir la section de ce chapitre sur le cycle de vie du certificat) ;
  - un identificateur de la clé du sujet (SKI), qui est un hash de la clé publique du porteur du certificat, et un identificateur de la clé de l'émetteur (AKI) : ces champs sont utilisés pour reconstituer la chaîne de la confiance (voir la section sur la chaîne de la certification dans le présent chapitre).

Les usages possibles du certificat

Plusieurs extensions complémentaires du certificat sont employées pour présenter les usages qui peuvent en être faits.

L'extension Utilisation de la clé (*Key usage*) décrit les opérations élémentaires qui peuvent être réalisées avec le certificat. Les choix possibles sont :

- signature électronique ;
- non-répudiation ou « engagement sur le contenu » (en grande partie redondant avec le précédent) ;
- chiffrement de clés (voir le détail dans le chapitre sur la confidentialité) ;
- chiffrement de données (usage rare) ;
- échange de clés (voir le chapitre sur le protocole SSL/TLS), et deux compléments permettant de restreindre l'usage en complément :
  - chiffrement seulement ;
  - déchiffrement seulement.
- scellement de certificat : si le porteur du certificat est une autorité de certification uniquement ;
- scellement de liste de certificats révoqués : en général, la liste de certificats révoqués est scellée par l'autorité de certification.

L'extension Utilisation avancée de la clé (*Extended key usage*) donne des détails supplémentaires sur les usages permis, à un niveau protocolaire

Copyright © 2012 Eyrolles.

plus élevé que l'extension Utilisation de la clé. On peut citer, par exemple, l'authentification de serveur ou de client (voir la description du protocole SSL/TLS au chapitre 4), la signature de code, la protection des e-mails (voir le chapitre 9 sur les usages de la signature électronique), l'horodatage (voir le chapitre 11 sur la traçabilité) et les réponses OCSP (voir la section de ce même chapitre sur le cycle de vie du certificat).

L'extension Contraintes de base (B*asic constraints*) permet de déterminer si le certificat est un certificat d'autorité de certification et, dans ce cas, combien de sous-niveaux d'autorités de certification peuvent être créés en-dessous. Ce point est développé dans le présent chapitre, dans la section sur la chaîne de la certification.

En complément, une extension particulière des certificats mérite d'être mentionnée ici, celle de Certificat qualifié.

Chaque pays a la possibilité de définir un profil et des règles particuliers garantissant un niveau de sécurité reconnu comme élevé pour les certificats, qui seront alors appelés « certificats qualifiés ». C'est le cas de l'Union européenne, qui a ainsi créé une norme pour garantir l'interopérabilité des certificats dans l'ensemble des pays membres. La présence de cette extension implique le respect d'un certain nombre de contraintes, décrites dans la norme RFC 3039.

L'émetteur du certificat

Un émetteur de certificats est ce que l'on appelle également un prestataire de services de certification électronique (PSCE). Le PSCE est une personne morale qui délivre des certificats pouvant être classés en « familles », chaque famille étant délivrée par une autorité de certification (AC), chaque AC étant une déclinaison marketing et technique des activités du PSCE.

L'émetteur indiqué dans le certificat est l'autorité de certification responsable de la famille à laquelle appartient le certificat.

Il est décrit dans un champ de type DN, qui a la même structure que le DN du porteur décrit plus haut. Le champ Common Name, au lieu de comporter le prénom et le nom d'une personne physique, désignera le nom de l'autorité de certification, aussi appelé la « famille de certificats ».

La « stratégie de certificat »» ou « politique de certification » est le document publié par le PSCE décrivant ses engagements pour la délivrance des certificats par une des autorités de certification qu'il exploite, et les obligations des porteurs de certificats émis par cette AC. Ce document sera décrit plus en détails dans le chapitre 13 sur la convention de preuve. L'extension correspondante contient un lien permettant de prendre connaissance du document.

Copyright © 2012 Eyrolles.

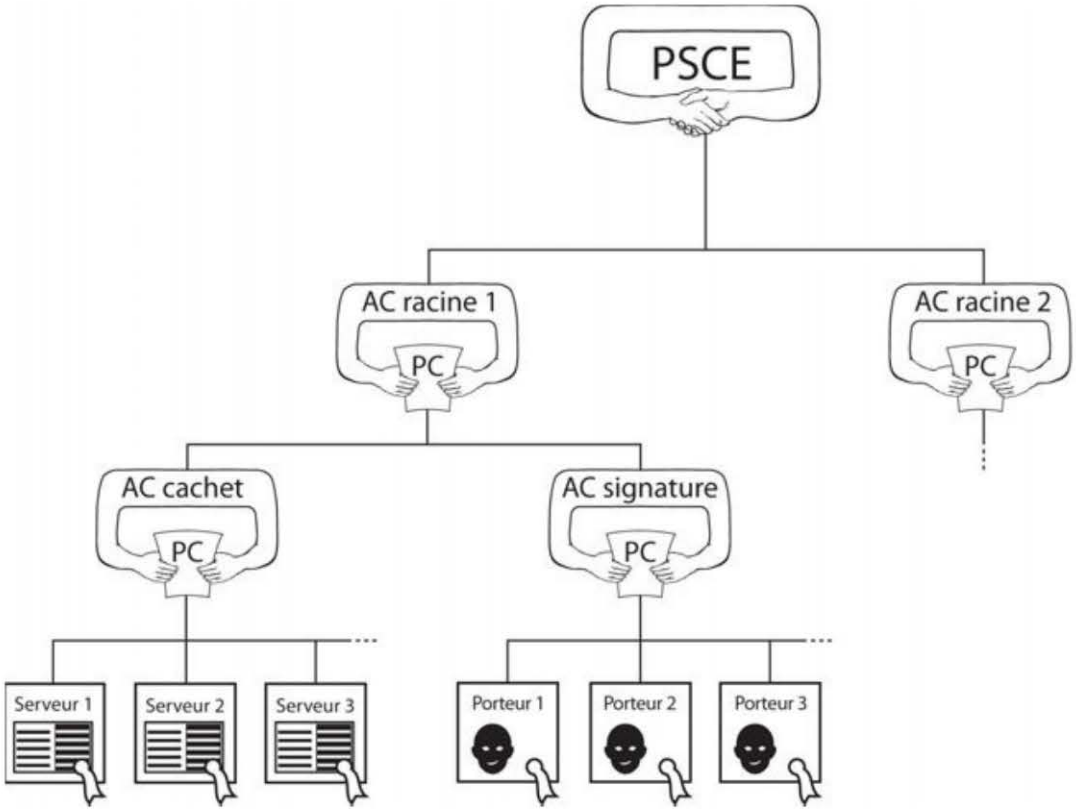


Figure 5-3 : La chaîne de la certification

Le scellement du certificat

Le scellement du certificat est l'élément technique qui permet d'en garantir l'intégrité, et de s'assurer qu'il a bien été émis par l'autorité de certification qui y est indiquée.

Nous verrons dans le chapitre 9 sur les usages de la signature électronique que ce scellement est l'équivalent technique d'une signature, terme qui est le plus souvent employé pour le désigner. Toutefois, pour des raisons de clarification du vocabulaire, nous préférons employer ici la notion de scellement, puisqu'il ne s'agit pas d'une signature de personne physique au sens de la loi du 13 mars 2000 (voir le chapitre 7 sur la signature électronique), mais bien d'un élément technique apposé par le serveur de l'autorité de certification.

Au titre du scellement, le certificat comporte :

1. l'empreinte de l'ensemble des informations contenues dans le certificat ;
2. l'algorithme employé pour le scellement ;
3. le scellement lui-même, c'est-à-dire le résultat du calcul mathématique effectué avec la clé privée de l'autorité de certification sur l'empreinte mentionnée au point 1 avec l'algorithme mentionné au point 2.

Copyright © 2012 Eyrolles.

Le contrôle de la provenance du certificat nécessitera donc d'utiliser le certificat de l'autorité de certification émettrice pour vérifier le scellement du certificat.

Les supports du certificat

Certificat et clé privée : protéger les données secrètes et rendre publiques les données de vérification

Du point de vue informatique, un certificat est un fichier structuré comportant des informations sur :

- son émetteur ;
- son porteur ;
- les usages qui peuvent en être faits.

Ce fichier est rendu inviolable, et son origine est garantie à l'aide d'un scellement apposé par le prestataire de services de certification électronique (PSCE) qui l'a émis. Ce scellement fait partie intégrante du certificat, et l'usage de ce dernier, par exemple pour authentifier une personne, passe nécessairement par la vérification préalable de ce scellement.

Le certificat est l'élément public qui peut être transmis à tout destinataire pour permettre de vérifier une identité. Il ne contient aucun secret (outre les données à caractère personnel) et peut être diffusé très largement sans aucun risque de sécurité. Ainsi, le certificat sera systématiquement joint à toute authentification et à toute signature électronique, et pourra être publié dans un annuaire.

Ce certificat ne peut pas être utilisé sans son pendant indispensable : la clé privée. Cette clé privée est, comme la clé publique, une suite d'octets, d'usage technique, qui n'a pas de sens immédiat pour un être humain, mais qui sera utilisée par les machines pour effectuer des calculs mathématiques. La clé privée est conservée secrète par son titulaire, elle ne doit jamais être diffusée ou rendue publique.

À l'achat d'un certificat, le mot « certificat » est entendu dans un sens plus large, ce seul terme désignant alors non seulement le certificat lui-même, mais également la clé privée correspondante, et le support (physique ou logiciel) qui contient cette clé.

Les supports de certificats ont trois fonctions principales :

- contenir le certificat lui-même et le mettre à disposition des applications afin qu'elles puissent librement le transmettre aux destinataires à des fins de vérification ;
- conserver secrète la clé privée, de manière à garantir qu'elle reste sous le contrôle exclusif du porteur légitime ;

Copyright © 2012 Eyrolles.

- permettre aux applications de faire appel à la clé privée, c'est-à-dire de lui faire faire un calcul sans pour autant la révéler publiquement, comme dans la figure 5-4.

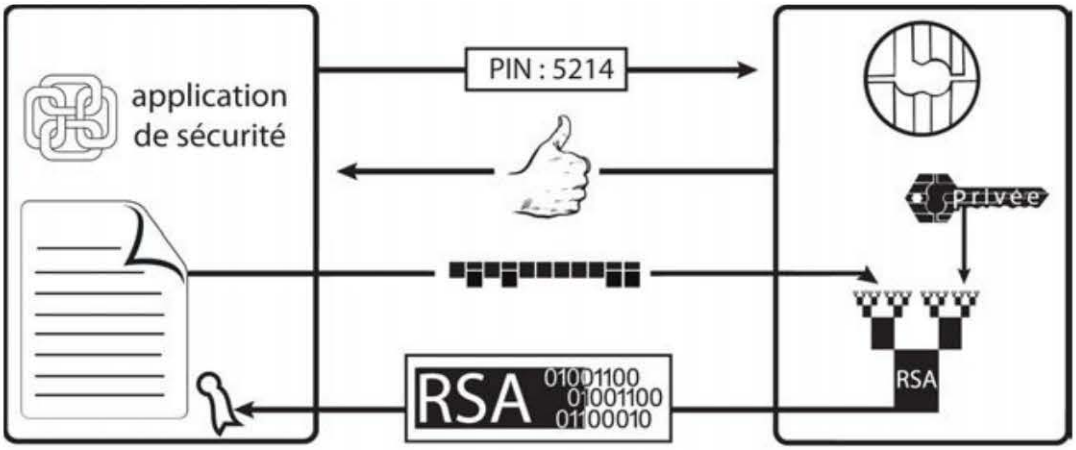


Figure 5-4 : Support cryptographique : contenu et appels

Ainsi, lorsqu'on parle du « support d'un certificat », il s'agit d'un abus de langage, puisque la partie sensible est plutôt la clé privée. La carte à puce, la clé cryptographique USB, etc., seront ainsi plutôt les supports sécurisés de la clé privée que du certificat, qui peut être, quant à lui, diffusé librement.

Deux grandes familles de supports sont disponibles :

- les supports logiciels ;
- les supports physiques.

On ajoutera à ces deux familles classiques un troisième mode de gestion des clés : les supports dynamiques externalisés.

Il est à noter que ce qui va être décrit dans ce chapitre est valable quels que soient les usages qui seront faits des bi-clés et des certificats : authentification, signature électronique ou chiffrement. Le mode de conservation et d'utilisation des clés ne change pas fondamentalement et les mêmes supports sont utilisés pour tous les usages.

Les supports logiciels

Il existe deux types de supports logiciels pour les certificats :

- les magasins de certificats ;
- les enveloppes autonomes.

Les magasins de certificats

Un magasin de certificats est une base de données dédiée à l'utilisation d'éléments cryptographiques, dans laquelle la partie publique est

Copyright © 2012 Eyrolles.

généralement en accès libre, et la clé privée est protégée par un chiffrement à l'aide d'un mot de passe.

Ainsi, les systèmes d'exploitation (Windows, Mac OS) incluent des magasins de certificats. Ces derniers sont à la disposition des applications, qui pourront s'en servir pour effectuer des opérations cryptographiques. Par exemple, les navigateurs Internet Explorer ou Chrome s'appuient sur le magasin de certificats de Windows, *via* l'interface programmatique CAPI.

Le navigateur Firefox contient également un magasin de certificats, qui accédera à des ressources externes *via* l'interface programmatique PKCS#11.

Pour des raisons de compatibilité multi-plates-formes, la machine virtuelle Java inclut un magasin de certificats propre, mais elle offre aussi la possibilité d'accéder à des magasins extérieurs, comme celui de Windows ou celui de Firefox.

Le serveur web Apache inclut un magasin de certificats pour l'établissement de sessions sécurisées SSL.

Par nature, les supports logiciels sont duplicables. Il est possible d'en faire une copie, et donc de disposer de plusieurs instances d'une même clé privée, ce qui rend plus difficile de garantir qu'elle demeure sous le contrôle exclusif de son titulaire légitime.

A *contrario*, les supports logiciels présentent deux avantages :

- leur coût nul, puisque les magasins de certificats sont nativement inclus dans les logiciels ;
- la capacité d'effectuer une copie de sauvegarde de son certificat et de la clé privée correspondante.

Lorsque l'on utilise un magasin de certificats, deux problématiques se présentent donc.

- Comment protéger efficacement les clés privées contenues dans le magasin ?
- Comment importer et exporter de manière sécurisée les certificats et les clés privées ?

La protection des clés privées s'appuie en général sur un double mécanisme de chiffrement et de gestion de droits.

Afin de garantir la confidentialité de la clé privée, celle-ci est chiffrée lors de son stockage dans le magasin de certificats, c'est-à-dire qu'elle est rendue incompréhensible à quiconque ne dispose pas du mot de passe permettant de la déchiffrer. Ainsi, à chaque accès à la clé privée, il faut présenter le mot de passe pour déchiffrer la clé privée. Selon les types de magasins de certificats, ce mot de passe est présenté par l'utilisateur ou géré directement par l'application.

Copyright © 2012 Eyrolles.

Prenons l'exemple du magasin de certificats de Windows : si l'on règle le niveau de sécurité de ce magasin sur « fort », un mot de passe de protection doit être défini par l'utilisateur, et il devra le saisir pour utiliser une clé privée, par exemple lors d'une authentification ou d'une signature électronique.

Par ailleurs, la sécurité est parfois renforcée par un contrôle d'accès : une application ou un utilisateur non autorisé ne pourra pas faire appel à la clé privée, ou, s'il y a une tentative d'accès à cette clé, l'utilisateur légitime en sera informé par une fenêtre d'avertissement.

Poursuivons l'exemple du magasin de certificats de Windows : si le niveau de sécurité est réglé sur « moyen », une fenêtre pop-up sera présentée à l'utilisateur à chaque tentative d'accès à la clé privée, et celui-ci devra autoriser cet accès (sans avoir à saisir de mot de passe). Ainsi, si un logiciel malveillant essaie de réaliser une signature électronique sans que l'utilisateur l'ait demandé, le magasin l'en avertira, et il pourra empêcher l'opération.

Pour achever cet exemple, notons qu'il existe aussi un niveau de sécurité « faible », dans lequel aucun avertissement n'est présenté à l'utilisateur : tout appel à une clé privée sera accepté automatiquement. Ce réglage est extrêmement dangereux, car le logiciel malveillant cité ci-dessus pourrait alors faire signer par l'utilisateur à son insu n'importe quel document, ou exporter une copie de la clé privée et la transmettre à un tiers.

L'utilisation des magasins de certificats doit donc être envisagée avec une grande prudence, car la protection de la clé privée correspond au niveau de sécurité qui lui est rattaché : au mieux, la force d'un mot de passe, au pire, celle du simple accès au poste de travail.

L'importation et l'exportation des certificats dans les magasins de certificats sont en général réalisées *via* l'utilisation d'enveloppes autonomes, dont nous allons maintenant détailler la nature et l'usage.

Les enveloppes autonomes

Il est parfois nécessaire de faire une copie d'une paire clé privée/certificat : par exemple si la génération de ces éléments est faite par un tiers qui doit ensuite les transmettre au porteur, ou pour en faire une copie de sauvegarde.

Il ne suffit pas, bien entendu, de copier ces éléments dans un fichier et de les envoyer par e-mail. Les contraintes de confidentialité qui pèsent sur la clé privée rendent nécessaire la création d'une enveloppe dont le contenu soit sécurisé. De plus, les contraintes d'interopérabilité impliquent une normalisation du format de l'enveloppe, afin de garantir que les éléments exportés puissent toujours être réimportés dans le contexte cible.

La société RSA Security a défini un format qui s'est imposé comme un standard, et n'a jamais fait l'objet d'une normalisation internationale en

Copyright © 2012 Eyrolles.

dehors de la définition qu'en a donné son inventeur. Au sein de la série de standards PKCS (*Public Key Cryptographic Standards*), ce format d'enveloppe « syntaxe d'échange d'information personnelle » porte le numéro 12.

Une enveloppe PKCS#12 porte en général une extension `.p12` ou `.pfx`. Elle contient la clé privée, chiffrée à partir d'un mot de passe choisi lors de la composition de l'enveloppe, et le certificat correspondant.

Afin de garantir la sécurité du transport, il convient de transmettre l'enveloppe par un canal (par exemple, par e-mail), et le mot de passe par un canal différent (par exemple, par téléphone ou SMS).

Les supports dynamiques externalisés

L'acquisition et l'installation d'un certificat sur le poste de travail de l'internaute pouvant être considérées comme des opérations complexes de nature à limiter l'utilisabilité de certains services (en particulier vis-à-vis du grand public), il peut être envisagé de sous-traiter la gestion des éléments secrets à un serveur distant.

Dans ce cas, le couple clé privée/clé publique sera généré au moment où l'utilisateur en a besoin, sur sa demande, utilisé une seule fois, puis détruit.

Il existe plusieurs façons de faire, qui font reposer une responsabilité plus ou moins grande sur le serveur. Nous allons présenter deux exemples de modes de réalisation de signature électronique « à la volée ».

Exemple 1 : réalisation de la signature sur le serveur

Lorsque l'utilisateur souhaite réaliser une signature électronique, le serveur recueille la demande de signature en contrôlant son mot de passe ou un autre défi tel qu'un code envoyé par SMS. Le serveur génère alors une clé privée et un certificat au nom de l'utilisateur, effectue la signature électronique, puis détruit de manière sécurisée et tracée la clé privée.

On voit bien que dans ce cas d'utilisation, la traçabilité de la demande de signature et de la destruction de la clé est fondamentale, car virtuellement, le serveur aurait la possibilité de générer des signatures électroniques au nom du signataire. Le serveur joue là un rôle de tiers de confiance qui va au-delà de celui de prestataire de services de certification électronique, puisque non seulement il génère le certificat de l'utilisateur, mais l'utilisateur lui délègue aussi l'usage de sa clé privée.

Aucune installation de certificat n'est nécessaire sur le poste de l'utilisateur, un simple navigateur lui suffit pour réaliser une signature électronique. Cela permet une utilisation du service depuis un environnement public, sans crainte de laisser des éléments confidentiels sur l'ordinateur utilisé.

Exemple 2 : réalisation de la signature sur le poste du signataire

Lorsque l'utilisateur souhaite réaliser une signature électronique, une applet est téléchargée sur son poste de travail, et s'exécute dans le

Copyright © 2012 Eyrolles.

cadre du navigateur. Cette applet génère alors en local une clé privée, et transmet au serveur la clé publique correspondante. Le serveur fabrique le certificat au nom de l'utilisateur et le retransmet à l'applet. La signature électronique est alors effectuée dans l'applet, qui détruit immédiatement la clé privée.

Ce schéma permet au serveur de ne jouer que le rôle de prestataire de services de certification électronique, la clé privée restant dans l'environnement du signataire et n'étant jamais connue par le serveur.

Là encore, la clé privée n'ayant qu'une existence volatile, aucune installation de certificat n'est nécessaire sur le poste de l'utilisateur. En revanche, le poste du signataire doit disposer d'un environnement d'exécution d'applets Java.

Ces deux exemples ne sont pas à proprement parler des « supports de certificats », mais plutôt des procédés dynamiques permettant de se passer de support, en ne laissant à la clé privée qu'une existence fugitive. La sécurité d'un tel dispositif est équivalente à celle du moyen d'authentification qui permet à l'utilisateur de faire sa demande de signature, c'est-à-dire en général un mot de passe ou la transmission d'un code par SMS.

Les supports matériels

Pour garantir la confidentialité des clés privées, le plus sûr est de les conserver au sein d'un support physique : transportable, inviolable, simple d'utilisation, le support matériel du certificat combine de nombreuses qualités.

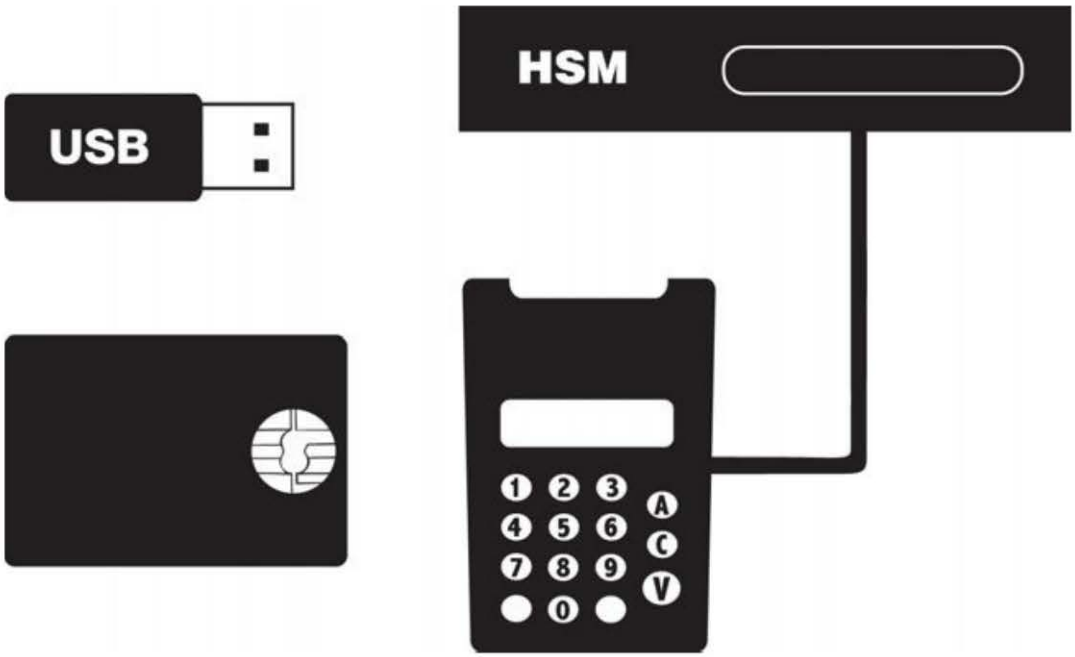


Figure 5-5 : Les différents types de supports cryptographiques matériels

Copyright © 2012 Eyrolles.

Pour le grand public : carte à puce et clé USB

Pour le grand public et les usages professionnels, deux formes de supports matériels sont disponibles et largement répandus : la carte à puce et la clé cryptographique USB.

La carte à puce : un format sécurisant

De par sa ressemblance avec la carte bancaire, la carte à puce est le support le plus « sécurisant » : le porteur aura naturellement tendance à lui appliquer les mêmes règles de sécurité qu'à son moyen de paiement, surtout si l'on couple sur le même support d'autres fonctions telles que la puce sans contact de contrôle d'accès aux locaux, le paiement à la machine à café ou la personnalisation graphique pour en faire un badge d'entreprise.

L'inconvénient de la carte à puce est qu'elle nécessite la présence d'un lecteur sur le poste où l'on souhaite l'utiliser. Même s'ils sont aujourd'hui très bon marché et parfois intégrés au clavier des ordinateurs, les lecteurs de cartes à puce ne sont pas un périphérique standard dans la plupart des environnements informatiques.

Parmi les projets utilisant une carte à puce, on peut citer la carte de professionnels de santé, ou encore les cartes d'agents de la fonction publique déployés par l'Agence nationale des titres sécurisés.

La clé USB : un format pratique

Pour des raisons de simplicité, la clé cryptographique USB est aujourd'hui plus répandue en tant que support des certificats. Elle présente en effet l'avantage de combiner la carte et le lecteur, avec un format de connectique universel.

Du point de vue de la perception par les utilisateurs, la clé USB présente l'inconvénient de s'assimiler aux supports de mémoire employés quotidiennement pour transporter et échanger des fichiers (d'ailleurs souvent au mépris des risques de contamination par des virus informatiques !).

Pourtant, les fonctionnalités des clés cryptographiques USB ne sont pas comparables à celles des simples supports de mémoire : ce qui fait leur intérêt est leur capacité à stocker des clés privées de manière sécurisée, et à les utiliser pour effectuer des calculs mathématiques.

La plupart des prestataires de services de certification électronique référencés pour les téléprocédures ou la réponse aux marchés publics délivrent les certificats sur ce type de support.

La sécurité des clés privées

Lorsqu'une clé privée doit circuler entre deux systèmes, par exemple celui qui l'a générée et celui qui doit l'utiliser, il existe toujours un risque de compromission.

Copyright © 2012 Eyrolles.

Dans le but d'éviter ce risque, le bon usage consiste à générer la clé privée directement dans l'environnement où elle sera ensuite utilisée, donc sous le contrôle de son porteur, et à ne faire circuler que la clé publique à des fins de génération du certificat par le PSCE.

Les supports cryptographiques offrent donc des fonctionnalités de génération de bi-clés directement à bord de la puce : la clé privée ainsi construite à l'aide d'un générateur aléatoire dans l'enceinte sécurisée est immédiatement stockée dans un « coffre-fort » miniature, qui est un espace mémoire particulier, extrêmement sécurisé, d'où la clé privée ne peut jamais sortir.

Les standards de sécurité des supports cryptographiques imposent que l'espace de stockage des clés soit inviolable : en cas de tentative d'attaque par quelque moyen que ce soit (électrique, laser, microscope électronique…), le secret sera immédiatement détruit sans avoir pu être lu.

Bien entendu, la clé privée doit pouvoir être utilisée pour faire les opérations mathématiques auxquelles elle est destinée. Mais cette utilisation ne nécessitera pas d'extraire la clé privée de la puce où elle est confinée : c'est le coprocesseur arithmétique de la carte à puce (ou de la clé cryptographique USB) qui fera les calculs, à la demande des applications appelantes. En aucun cas une application ne peut obtenir de la puce qu'elle lui transmette une copie de la clé privée.

Une utilisation des clés privées sous le contrôle du porteur

De même que pour la carte bancaire, l'utilisation de la puce cryptographique nécessite la présentation du code secret de l'utilisateur, aussi appelé code PIN (*Personal Identification Number*) .

Le code PIN comporte 4 ou 6 chiffres, et la puce se bloque après trois mauvaises présentations. Certaines puces peuvent être débloquées en utilisant le PUK (PIN U*nlocking Key*), un code de niveau supérieur qui ne permet que le déblocage ou la réinitialisation de la puce (c'est-à-dire l'effacement de l'ensemble des données), mais pas l'utilisation des secrets.

Le support peut être configuré pour demander la présentation du code PIN pour chaque utilisation de la clé privée, ou pour conserver la session active après une première présentation du code PIN, de manière à alléger l'acte de signature, par exemple pour un utilisateur qui aurait de nombreux documents à signer.

Qu'est-ce qu'un dispositif sécurisé de création de signature électronique ?

Dans le cas particulier de la signature électronique « présumée fiable » définie par le décret n° 2001-272 du 30 mars 2001, il est imposé que le support de la clé privée soit « un dispositif sécurisé de création de signature électronique ». Un tel dispositif doit respecter les exigences suivantes.

Copyright © 2012 Eyrolles.

- Les données de création de signature électronique (c'est-à-dire la clé privée) ne peuvent être établies plus d'une fois, et leur confidentialité doit être assurée par la génération des clés à bord du support grâce à un générateur aléatoire, et par le stockage des clés dans la zone sécurisée de la puce.
- La clé privée ne peut être trouvée par déduction et la signature électronique est protégée contre toute falsification : cela découle de la qualité du générateur aléatoire employé, et des propriétés intrinsèques aux bi-clés RSA.
- Le signataire peut protéger sa clé privée de manière satisfaisante contre toute utilisation par des tiers : cela est garanti par la nécessité de présenter son code PIN pour pouvoir utiliser la clé privée dans le but de faire une signature électronique.
- L'utilisation du dispositif ne doit entraîner aucune altération du contenu de l'acte à signer, et ne doit pas faire obstacle à ce que le signataire en ait une connaissance exacte avant de signer : le processus de signature électronique n'est jamais contrôlé directement par le dispositif de signature, mais par l'application qui y fait appel, comme nous le verrons plus loin. Le support ne faisant que réaliser des opérations mathématiques dont le résultat est remis à l'application appelante, il n'y a aucun risque de voir de telles altérations se produire du seul fait du support.

Les dispositifs logiciels (magasins de certificats ou systèmes de génération de certificats temporaires) ne correspondent pas à ces exigences : dans un projet de signature électronique, si la conformité aux impératifs de la signature « présumée fiable » est nécessaire, il faudra sélectionner un support physique (clé cryptographique USB ou carte à puce) certifié conforme à ces conditions.

La signature électronique « présumée fiable » sera abordée plus en détail au chapitre 7 consacré à la signature électronique.

Côté serveur : les HSM (*Hardware Security Module*)

Nous avons vu que les clés cryptographiques USB et les cartes à puce sont de petits coffres-forts destinés à la génération, la conservation et l'utilisation des bi-clés cryptographiques. Ces dispositifs présentent l'intérêt d'être transportables, mais ont deux inconvénients majeurs : ils ont une capacité assez faible, et des performances médiocres en termes de temps de traitement. Or, ce qui n'est pas handicapant pour un utilisateur humain, soumis de toute façon aux lenteurs de son logiciel, du débit réseau et de sa propre lenteur à introduire le support et à taper le code PIN, devient inacceptable pour une utilisation intensive de la cryptographie, par exemple par un PSCE.

Copyright © 2012 Eyrolles.

Ainsi, pour un usage industriel, commandé par un serveur, les bi-clés sont gérées par des modules physiques plus puissants, plus volumineux, et encore plus sécurisés, que l'on appelle des « modules de sécurité matériels », *Hardware Security Modules* (HSM) en anglais.

Outre leur rapidité d'exécution et leur capacité à gérer plusieurs dizaines voire centaines de bi-clés, ces modules de sécurité offrent des fonctionnalités d'administration importantes : nécessité de la présence de plusieurs opérateurs pour les initialiser, générer des clés ou les redémarrer après une coupure de courant, possibilité de les sauvegarder de manière sécurisée…

De plus, les HSM offrent une résistance aux intrusions et aux tentatives d'attaques plus forte que celle des supports individuels. Ainsi, chaque élément de la chaîne de la sécurité apporte une réponse graduée par rapport aux enjeux qui découlent de lui.

Dans l'intimité des opérations cryptographiques : les procédés d'échanges et de communication

Lorsque l'utilisateur réalise une opération cryptographique qui nécessite de faire appel à sa clé privée, par exemple pour s'authentifier, faire une signature électronique ou déchiffrer un message confidentiel, les composants techniques mis en jeu sont très nombreux. Nous allons ici identifier ces modules et illustrer les principales interactions qui ont lieu. Ces éléments sont présentés sur la figure 5-6.

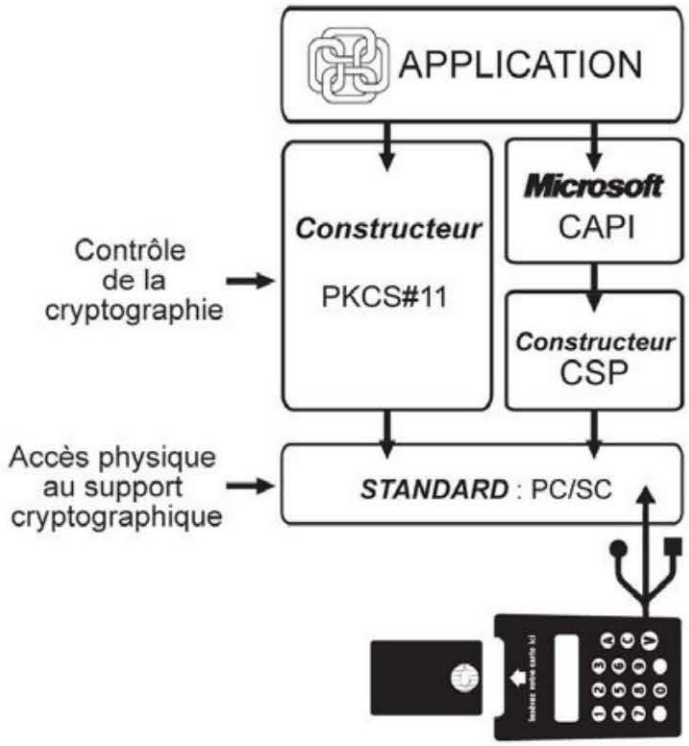


Figure 5-6 : La chaîne des modules cryptographiques

Copyright © 2012 Eyrolles.

Au sommet se trouve l'application métier, par exemple le logiciel de signature électronique ou le navigateur Internet par lequel l'utilisateur se connecte à un site web qui lui demande une authentification par certificat.

Au plus bas se trouvent les couches techniques de communication entre l'ordinateur et le lecteur de carte à puce (ce lecteur étant éventuellement intégré à la clé cryptographique USB) : cette communication est standardisée dans une librairie informatique appelée « PC/SC » pour *Personal Computer/Smart Card*. En règle générale, la communication au travers de PC/SC se fait par *secure messaging*, c'est-à-dire que toutes les informations qui circulent à ce niveau, par exemple le code PIN, sont chiffrées pour éviter tout risque de piratage.

Nota Bene : le schéma reste le même dans le cas de l'utilisation d'un magasin logiciel, les clés privées stockées dans ce dernier pouvant être utilisées *via* PKCS#11 ou CAPI. Dans la figure 5-8, on remplacerait alors le bloc « accès physique au support cryptographique » par un bloc « magasin logiciel ».

Pour faire le lien entre les deux, il existe deux canaux, illustrés par la colonne de gauche (PKCS#11) et celle de droite (CAPI/CSP).

Le standard PKCS#11 (*Public Key Cryptographic Standard* numéro 11, aussi appelé « Cryptoki ») est une interface programmatique développée par RSA Laboratories. Elle est principalement utilisée dans les environnements autres que Windows ou, sous Windows, par les applications qui ne souhaitent pas s'appuyer sur les couches de sécurité fournies par Microsoft, comme le navigateur Internet Firefox. Dans ce schéma, l'application fait directement appel au module PKCS#11, qui est une bibliothèque dynamique (DLL) fournie par le constructeur de la carte à puce. Cette DLL implémente les fonctions de sécurité (présentation du code PIN, signature électronique, déchiffrement d'une clé…) et gère les appels à PC/SC pour les faire réaliser par la puce.

Le standard CAPI/CSP (*Crypto* API/*Cryptographic Service Provider*) est une interface programmatique fournie nativement dans Windows. L'application fait appel aux fonctions de sécurité offerte par le module CAPI, fourni par Microsoft, qui s'appuie à son tour sur le module CSP fourni par le par le constructeur de la carte à puce.

Le standard PKCS#11 présente un inconvénient important : la DLL implémentant les fonctions de sécurité n'est pas elle-même sécurisée. Il est ainsi possible, si l'on a accès à un poste de travail, de remplacer le module PKCS#11 par un autre, qui rendrait apparemment les mêmes fonctions, mais pourrait réaliser des opérations supplémentaires à l'insu de l'utilisateur : tracer le code PIN ou faire des signatures électroniques, par exemple. C'est une attaque de type *man in the middle* comme illustré dans la figure 5-7, où le module PKCS#11 frauduleux fait réaliser à l'utilisateur, à son insu, la signature électronique d'un document compromettant.

Copyright © 2012 Eyrolles.

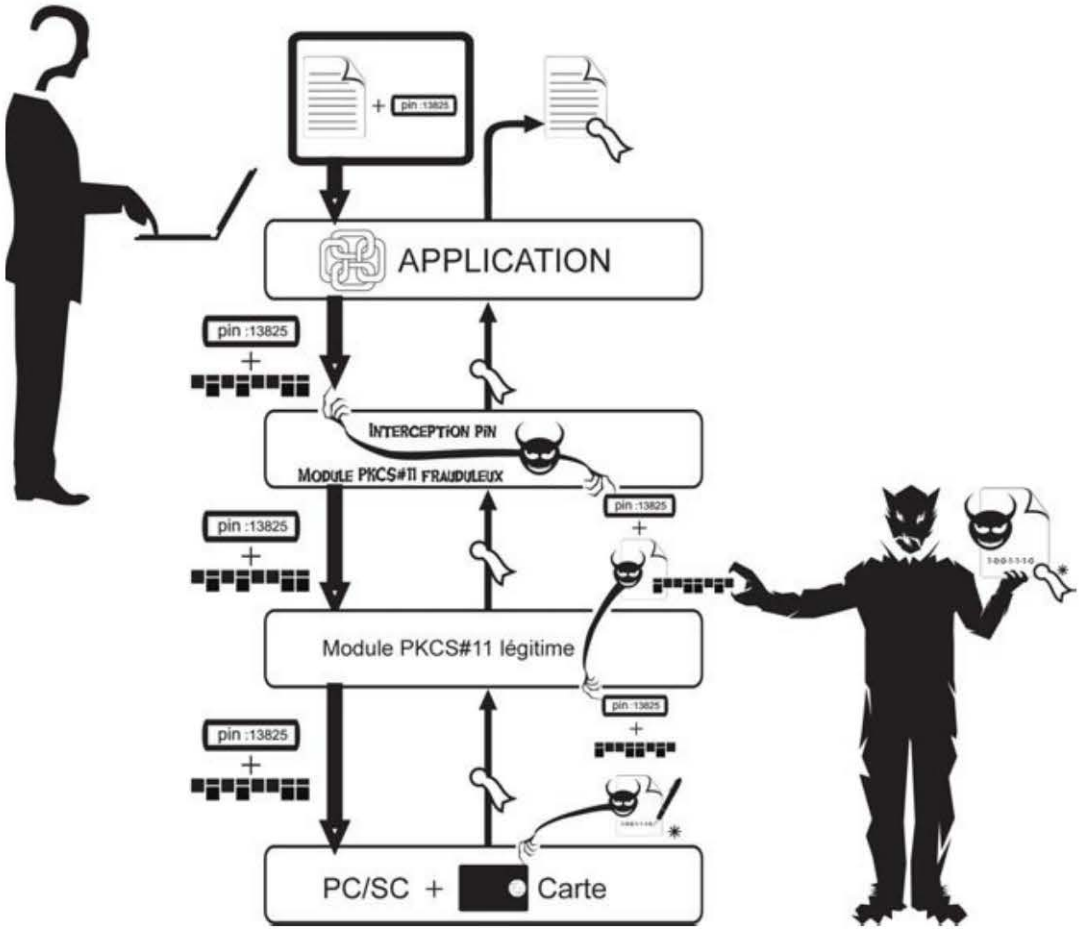


Figure 5-7 : PKCS#11 : attaque man in the middle

En revanche, tout module CSP sera refusé par CAPI s'il n'a pas été préalablement validé par Microsoft et scellé logiquement (voir le chapitre 9 sur le scellement de code exécutable pour plus de détails). Ainsi, le type d'attaque envisageable pour PKCS#11 n'est pas possible avec CAPI, et l'utilisateur a la certitude que la chaîne de la communication entre son application et la puce qui réalise les opérations cryptographiques est bien intègre.

La façon de stocker les clés et les certificats sur la puce, même s'il existe une norme appelée PKCS#15, reste de la responsabilité du fournisseur de la puce. C'est pourquoi, pour utiliser un support de certificat matériel, il est nécessaire, dans tous les cas, d'installer sur son poste de travail le logiciel qui va avec : module PKCS#11 ou CSP. Cela introduit malheureusement un frein au nomadisme des supports cryptographiques, leur utilisation n'est pas *plug and play* mais nécessite l'installation de ces librairies logicielles. Il ne suffit donc pas de brancher sa clé cryptographique USB à un nouvel ordinateur pour pouvoir l'utiliser, contrairement à l'habitude que l'on a des

Copyright © 2012 Eyrolles.

clés mémoire USB qui fonctionnent instantanément dans tous les environnements.

Détaillons les rôles respectifs de chacun des maillons de la chaîne de la figure 5-6, dans le cas de la signature électronique d'un document PDF.

- Au sein de l'application, l'utilisateur décide de réaliser une signature sur un document PDF qui lui a été présenté.
- L'application commande au niveau « contrôle de la cryptographie » la réalisation de la signature et lui transmet le hash du document à signer (voir le chapitre 8 sur la signature électronique pour plus de détails).
- Le niveau « contrôle de la cryptographie » demande à l'utilisateur de saisir son code PIN et le transmet, *via* PC/SC à la puce elle-même, puis, après validation du code PIN par la puce, lui communique le hash à signer et l'ordre de faire le calcul RSA avec la clé privée.
- La puce réalise le calcul RSA à l'aide de la clé privée et renvoie, toujours *via* PC/SC, le résultat au niveau « contrôle de la cryptographie ».
- Le niveau « contrôle de la cryptographie » effectue une première mise en forme de ce résultat et le transmet au niveau « application ».
- L'application intègre le résultat du calcul RSA avec d'autres éléments qu'il se procure par ailleurs (horodatage, preuve de validité du certificat) dans le fichier PDF : le fichier est maintenant signé.

Cet exemple illustre l'utilité des différentes couches.

- L'application sait, au niveau macroscopique, quelles données signer, à quel format fournir la signature, etc., indépendamment du support cryptographique qui sera disponible en dessous. Ainsi, le concepteur de l'application n'a pas à adapter son logiciel à toutes les offres du marché.
- Le niveau « contrôle de la cryptographie » sait comment enchaîner les appels à la puce de manière satisfaisante pour réaliser les opérations secrètes, pour le type de support avec lequel il a été commercialisé.
- Au niveau physique, la puce est la seule à détenir des secrets (la clé privée) et à pouvoir s'en servir. Elle agit comme esclave du niveau supérieur, de qui elle reçoit les instructions. Elle ne fournira jamais au niveau du dessus la clé privée, mais acceptera à la demande de s'en servir en interne pour produire le calcul demandé, sous réserve de présentation du code PIN.

Nous allons maintenant décrire le cycle de vie des certificats : comment ils sont générés, inscrits et utilisés dans leurs supports physiques ou logiciels, et comment est gérée leur fin de vie.

Copyright © 2012 Eyrolles.

Le cycle de vie du certificat

Les différents rôles du domaine de la certification électronique

L'ensemble des éléments techniques et organisationnels impliqués dans l'émission de certificats est généralement dénommé « PKI », pour P*ublic Key Infrastructure*. En français, on parle aussi d'ICP (Infrastructure à clé publique) ou d'IGC (Infrastructure de gestion de clés). Ces termes sont synonymes.

Un certificat a pour fonction de certifier l'identité de son porteur, et de lier cette identité à une clé publique. Le premier acteur à prendre en compte est donc **le porteur du certificat.**

Le certificat est destiné à garantir l'identité du porteur à une personne distincte de ce dernier ; ceux qui utilisent les certificats, par exemple pour vérifier les authentifications ou les signatures électroniques, sont appelés **les utilisateurs de certificats**.

Les autres acteurs de la certification sont ce que l'on appelle **les prestataires de services de certification électronique (PSCE)**. Le décret du 30 mars 2001 en donne la définition suivante.

Décret du 30 mars 2001 – Article 1

Au sens du présent décret, on entend par [...] prestataire de services de certification électronique : toute personne qui délivre des certificats électroniques ou fournit d'autres services en matière de signature électronique.

Cette définition extrêmement large nous amène à définir d'autres rôles, afin d'obtenir un découpage plus fin des différentes fonctions.

L'autorité de certification (AC) est une entité morale qui a pour rôle la définition des règles qui régissent le cycle de vie des certificats, et l'application de ces règles. L'AC fixe les règles par écrit sous la forme d'un document public, appelé la « politique de certification » (PC). Ce document l'engage, ainsi que les porteurs et les utilisateurs de certificats, et l'ensemble des acteurs de la chaîne.

Un PSCE peut comporter une ou plusieurs AC. Elles peuvent être organisées de manière hiérarchique, chacune certifiant l'AC de niveau inférieur, ou exister en parallèle, sans lien entre elles.

Une AC correspond à une « famille de certificats ». Tous les certificats de la même famille, émis par la même AC, le sont en respectant les mêmes règles, édictées dans la politique de certification de l'AC.

L'autorité d'enregistrement (AE) est une entité qui procède à la vérification de l'identité du porteur en vue de lui remettre un certificat. Cette opération est parfois appelée « enrôlement ». L'AE doit respecter les

Copyright © 2012 Eyrolles.

obligations découlant de la politique de certification en termes de pièces à vérifier, de conservation des documents, de procédure de contrôle et de délivrance (rencontre en face à face éventuelle avec le futur porteur...).

L'opérateur de certification (OC) est l'entité chargée de l'exploitation de l'infrastructure technique de délivrance de certificats.

Deux autres rôles peuvent être définis, souvent assumés par l'AC elle-même ou l'AE.

L'autorité de validation (AV) peut être interrogée par l'utilisateur de certificat qui souhaite vérifier la validité d'un certificat.

L'autorité de révocation (AR) peut être saisie par le porteur de certificat ou son responsable (par exemple, l'entreprise à laquelle il appartient) pour inscrire le certificat dans la liste de certificats révoqués.

Ainsi, comme illustré dans la figure 5-8, sous le contrôle de l'autorité de certification, l'autorité d'enregistrement délivre les certificats aux porteurs en s'appuyant sur l'infrastructure exploitée par l'opérateur de certification. La révocation du certificat se fait auprès de l'autorité de révocation, qui s'appuie également sur l'infrastructure technique. L'utilisateur du certificat doit accorder sa confiance à l'autorité de certification et peut vérifier la validité du certificat du porteur auprès de l'autorité de validation.

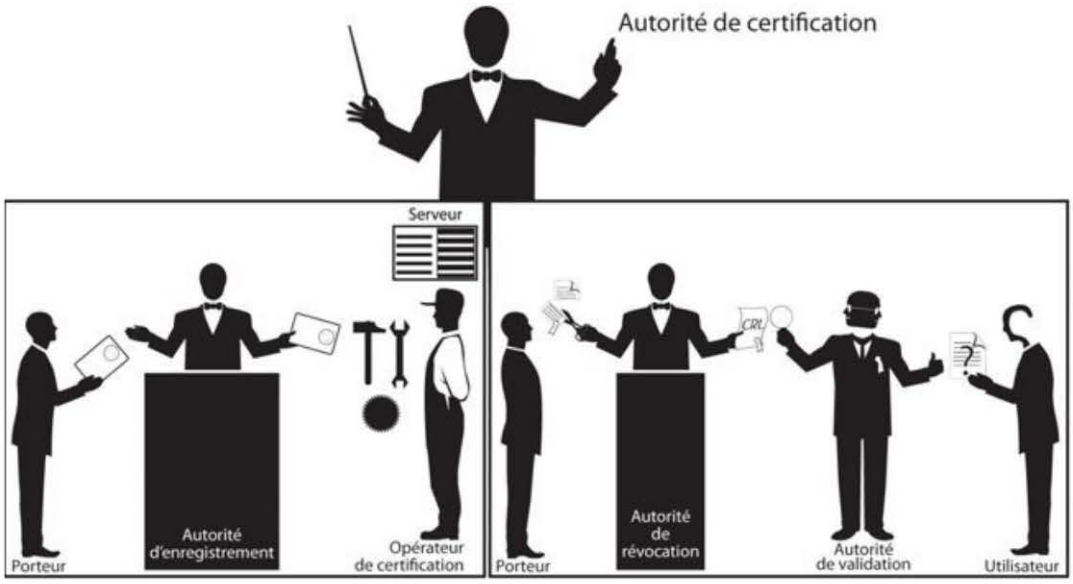


Figure 5-8 : Les acteurs de la PKI

Copyright © 2012 Eyrolles.

Exemple d'organisation : Certigreffe

Le PSCE Infogreffe, GIE des greffiers de tribunaux de commerce, a créé une autorité de certification appelée Certigreffe, qui délivre la famille de certificats du même nom.

Les futurs porteurs, pour obtenir leur certificat, s'adressent au greffe du tribunal de commerce le plus proche de leur domicile. En tant qu'autorité d'enregistrement, le greffe vérifie les pièces d'identité et les justificatifs présentés à l'appui de la demande et effectue la rencontre en face à face nécessaire à la délivrance du certificat.

L'infrastructure technique est exploitée par CertEurope, opérateur de certification qualifié. CertEurope joue aussi le rôle d'autorité de révocation, *via* un service en ligne et par téléphone, et d'autorité de validation, *via* la tenue à jour de la liste de certificats révoqués.

Les étapes de la vie d'un certificat

La demande et la délivrance du certificat

Les certificats de personnes physiques

La demande d'un certificat pour une personne physique peut être effectuée par le futur porteur lui-même, ou par un tiers en cas de délégation, par exemple, par son responsable hiérarchique ou par le service des ressources humaines.

La demande est adressée à l'autorité d'enregistrement (AE), qui vérifie l'identité du porteur avant de transmettre la demande validée à l'opérateur de certification (OC).

La génération de la bi-clé RSA peut être réalisée à trois niveaux.

- Directement par le futur porteur, de manière simultanée à la demande de certificat. Dans ce cas, le processus inclut la fabrication d'une « preuve de possession » de la clé privée qui est transmise à l'opérateur de certification (voir ci-dessous).
- Par l'AE lorsqu'elle reçoit la demande de certificat : dans ce cas, il s'agit en général d'une génération sur un support physique. Le code PIN du support est généré automatiquement dans le processus de « personnalisation électrique » du support (c'est-à-dire lors de son initialisation par la génération de la bi-clé), et envoyé directement au porteur du certificat, sans jamais être connu par l'AE, afin de garantir que l'AE n'a pas eu la possibilité d'utiliser la clé privée en lieu et place du porteur.
- Par l'OC lors de la génération du certificat. Les mêmes procédures de protection du code PIN s'imposent alors à lui.

La preuve de possession de la clé privée (PoP, *Proof of Possession*) consiste en un calcul RSA réalisé par la clé privée et portant sur le hash de la clé publique. La clé publique est transmise avec la PoP et permet à l'OC de vérifier que ce calcul a bien été effectué avec la clé privée correspondante.

Copyright © 2012 Eyrolles.

Il a ainsi la certitude que le demandeur du certificat possède bien la clé privée ; cela évite qu'un individu malveillant puisse faire réaliser un certificat à son nom portant sur la clé de quelqu'un d'autre.

Une fois le certificat généré et scellé par l'OC à l'aide de la clé privée de l'autorité de certification (AC), il est transmis soit au porteur, soit à l'AE, pour l'inscrire dans le support. Une fois le support remis et le code PIN reçu par le porteur, le certificat est prêt à l'usage !

Obtenir un certificat de serveur

Un certificat de serveur sera délivré pour un serveur précis et pour un usage précis, par exemple la réalisation de cachets, de jetons d'horodatage ou l'établissement de sessions SSL.

L'administrateur du serveur génère directement sur celui-ci, ou sur le matériel cryptographique lié au serveur, une requête de certificat appelée « CSR » pour *Certificate Signing Request*. La CSR contient une PoP et l'ensemble du contenu du certificat, à l'exclusion de son scellement. C'est ce que l'on appelle un *to be signed certificate*, ou TBS *Certificate*.

La CSR est transmise à l'AE qui vérifie l'identité et la légitimité du demandeur, par exemple sur la base de la possession par le demandeur du nom de domaine du serveur, inscrit dans le TBS Certificate.

La demande est alors transmise à l'OC qui scelle le certificat et le retransmet au demandeur, qui l'installera sur le serveur.

Les certificats autosignés

Un certificat autosigné est un certificat que le porteur a scellé lui-même à l'aide de sa clé privée. Sa provenance n'est ainsi pas garantie par une autorité de certification tierce.

Dans ce cas, il n'y a pas de formalisme imposé pour la génération du certificat, puisqu'elle est faite « en vase clos » par le porteur. Les seules contraintes sont celles qui pèsent sur la confidentialité de la clé privée.

Nous verrons plus loin deux cas d'usage des certificats autosignés :

- les certificats des autorités de certification, dans la section « La chaîne de la certification » de ce chapitre ;
- les certificats utilisés dans le modèle PGP, dans la section « Le modèle PGP » de ce chapitre.

La gestion des clés privées et des certificats en fonction de l'usage

Les règles de gestion des clés privées et des certificats dépendent de l'usage qui doit en être fait.

Un certificat destiné à être employé à des fins d'authentification ne sera plus utilisé une fois qu'il a expiré ou qu'il a été révoqué, car l'authentification est une action de courte durée. Le certificat doit être présent dans l'annuaire ou

Copyright © 2012 Eyrolles.

la base de données du service qui authentifie les utilisateurs. Si la clé privée correspondante est perdue ou compromise, il ne sera jamais nécessaire de la recouvrer, elle peut donc n'exister qu'en un seul exemplaire.

Un certificat destiné à être employé à des fins de signature électronique continuera à être utilisé après son expiration, car les signatures nécessitent une vérification *a posteriori*. Il doit donc être conservé. Il est d'ailleurs, à cette fin, inclus dans chaque signature réalisée. Le certificat de signature n'a pas *a priori* besoin d'être inscrit dans un annuaire ou publié, car il contient les éléments permettant d'identifier son porteur. La clé privée, quant à elle, ne doit jamais être dupliquée, car en cas de perte ou de compromission, on en génère simplement une nouvelle.

Un certificat destiné à être employé à des fins de chiffrement doit être publié à l'attention de tous les correspondants possibles du porteur, afin qu'ils puissent s'en servir pour chiffrer des messages à son intention. En revanche, une fois le certificat révoqué ou expiré, il n'est plus nécessaire de le conserver. Contrairement au besoin d'unicité de la clé privée que nous avons vu pour l'authentification et la signature électronique, il est en revanche important que la clé privée correspondant à un certificat de chiffrement soit conservée dans un « séquestre » qui offre la possibilité d'un recouvrement en cas de perte. En effet, sans la clé privée, les données chiffrées seraient à jamais indéchiffrables, donc perdues.

Le tableau 5-2 reprend ces règles de gestion de manière synthétique.

Tableau 5-2 : Gestion des clés et certificats selon les usages

	Clé privée	Certificat
Authentification	Doit exister en un seul exemplaire. Ne nécessite pas de conservation après sa fin de vie.	Doit être inscrit dans l'annuaire du service. Ne nécessite pas de conservation après la fin de vie de la clé privée, sauf à des fins de traçabilité.
Signature électronique	Doit exister en un seul exemplaire. Ne nécessite pas de conservation après sa fin de vie.	Ne nécessite pas de publication. Doit être conservé au-delà de sa limite de validité pour permettre les vérifications de signatures.
Chiffrement	Un second exemplaire doit être séquestré pour permettre le déchiffrement des données en cas de perte de la clé originale. Nécessite une conservation après sa fin de vie pour permettre le déchiffrement.	Doit être publié à destination de tous les émetteurs de messages chiffrés à l'attention du titulaire. Ne nécessite pas de conservation après la fin de vie de la clé privée, sauf à des fins de traçabilité.

Copyright © 2012 Eyrolles.

Ainsi, lorsqu'un futur porteur de certificat fait une demande de certificat à des fins de signature électronique ou d'authentification, ce n'est en général pas le PSCE qui génère la clé privée, mais le demandeur lui-même, selon le schéma 5-9 suivant.

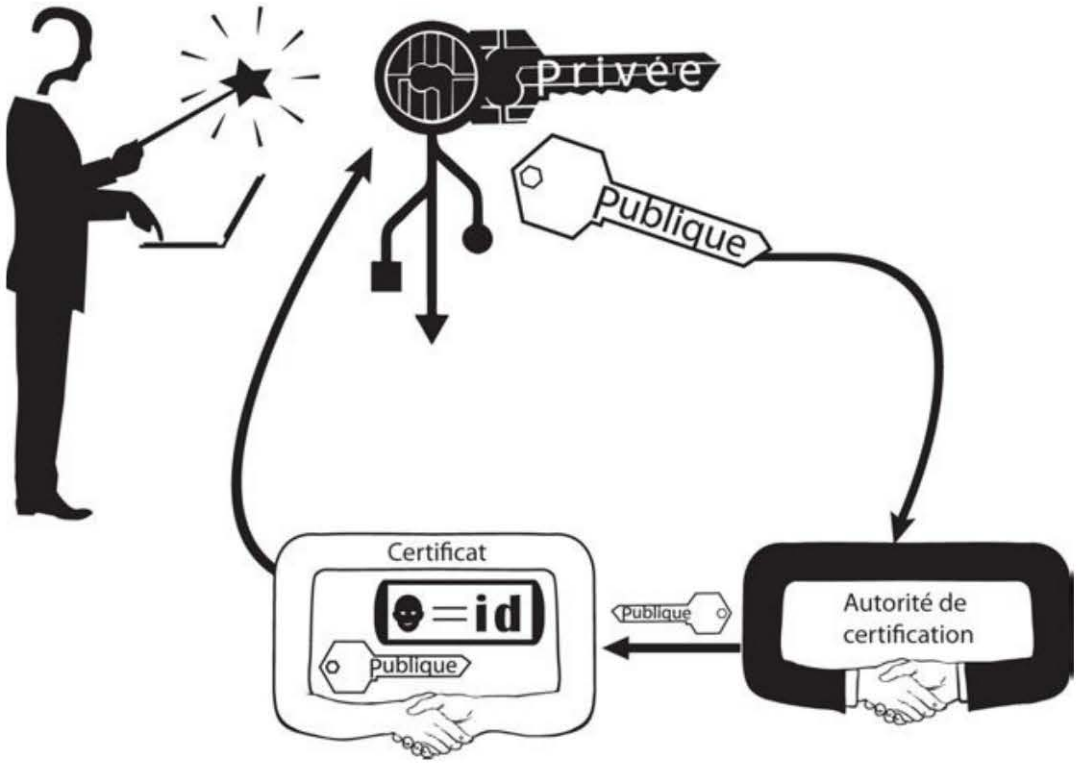


Figure 5-9 : Génération de la clé privée pour un certificat d'authentification ou de signature électronique

Dans le cas où le certificat doit être employé à des fins de confidentialité, la perte de la clé privée entraînerait l'impossibilité de déchiffrer les données transmises, et donc leur perte irrévocable. Dans le but de garantir la sécurité des données échangées, on procède alors à un séquestre de la clé privée, sous le contrôle d'un tiers de confiance tenu par des procédures très strictes visant à garantir le porteur du certificat contre toute diffusion de sa clé privée, comme l'illustre la figure 5-10.

Copyright © 2012 Eyrolles.

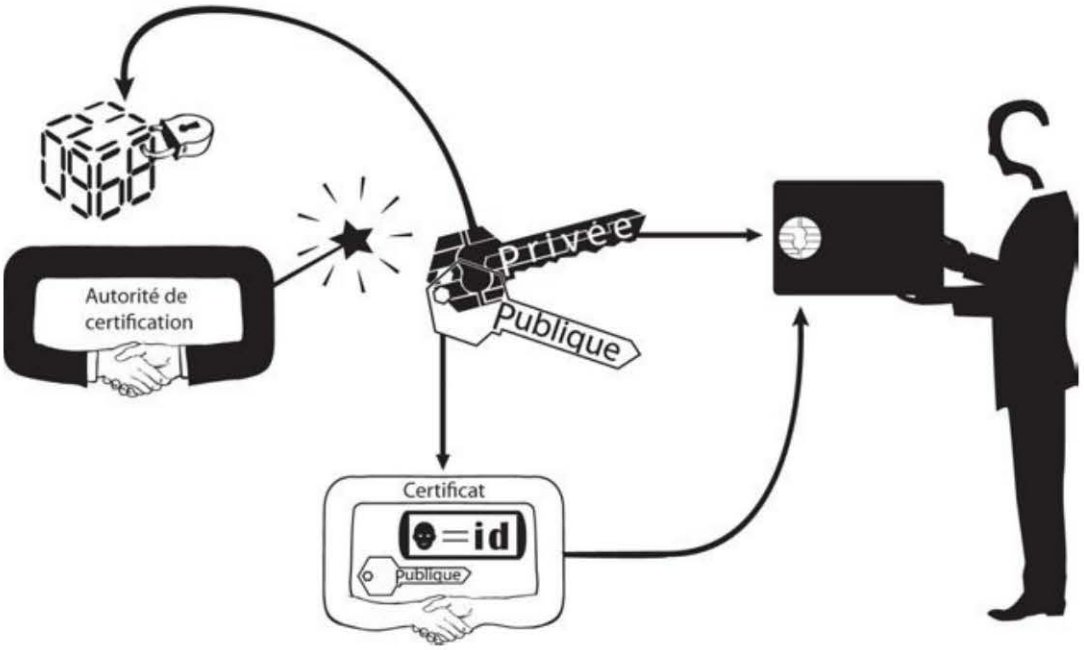


Figure 5-10 : Génération de la clé privée pour un certificat de chiffrement

La révocation

Au cours du cycle de vie du certificat, il peut arriver qu'il soit nécessaire de lui retirer sa confiance : c'est le cas à chaque fois qu'un certificat doit cesser d'être utilisé avant sa date d'expiration.

Ce cas de figure se produit, par exemple, lorsqu'un porteur perd son support cryptographique, lorsqu'un collaborateur quitte l'entreprise ou lorsqu'il n'a plus de délégation de pouvoir lui permettant d'engager l'entreprise, mais aussi lorsqu'un des champs contenus dans le certificat est obsolète (changement de nom ou d'adresse e-mail).

L'opération consistant à ôter la confiance mise dans un certificat s'appelle la « révocation ».

Les opérations nécessaires à la révocation, illustrées dans la figure 5-11, sont les suivantes.

- Le porteur du certificat, ou son responsable dans le cas où le porteur a quitté l'entreprise, fait une demande de révocation auprès de l'autorité de certification qui a émis son certificat.

  Selon les cas, la demande sera adressée à l'autorité d'enregistrement ou à une autorité de révocation dédiée à cette fonction, mais dans tous les cas, l'opération est sous le contrôle de l'autorité de certification.
- L'autorité de certification vérifie l'identité du demandeur, et surtout la légitimité de sa demande, en général à l'aide d'un secret dédié à cet usage : question secrète ou mot de passe, par exemple.

Copyright © 2012 Eyrolles.

Cette étape nécessite que le secret ait été défini en amont, par exemple lors de la délivrance du certificat.

Elle est indispensable afin d'éviter qu'un tiers puisse révoquer frauduleusement un certificat. Imaginons le cas d'une entreprise qui demanderait la révocation des certificats de signature électronique de ses concurrents la veille de la date limite de remise des plis pour un appel d'offres : si sa demande était prise en compte, le marché serait sévèrement faussé !

- L'autorité de certification ajoute le certificat dans la liste de certificats révoqués (LCR), ou *Certificate Revocation List* (CRL), sous un délai contractuel fixé dans la politique de certification.

  La liste de certificats révoqués est scellée cryptographiquement par l'AC et mise à disposition des utilisateurs de certificats afin qu'ils puissent à tout moment vérifier la validité du certificat et lui accorder ou non leur confiance.

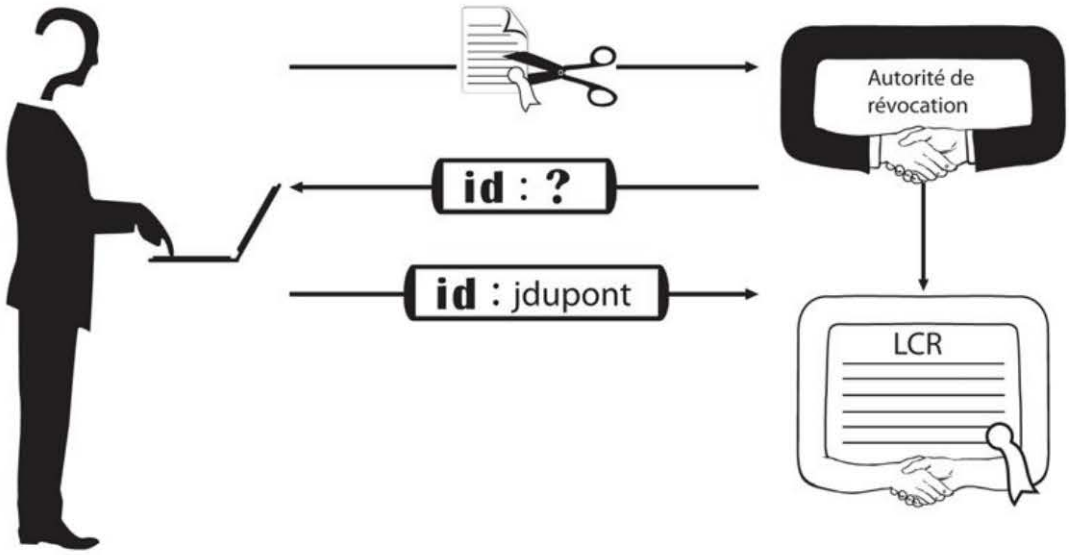


Figure 5-11 : La révocation d'un certificat

La LCR comporte principalement les informations suivantes :

- l'identification de l'autorité de certification émettrice ;
- un numéro unique et croissant de LCR ;
- le point de distribution de la LCR (c'est-à-dire l'URL où il est possible de la télécharger) ;
- une date d'émission et une date de mise à jour ;
- pour chaque certificat révoqué :
  - le numéro de série du certificat ;
  - la date de révocation ;

Copyright © 2012 Eyrolles.

  - optionnellement, la raison de la révocation (compromission du certificat, compromission de l'autorité de certification, cessation d'activité…) ;
- un scellement apposé par l'autorité de certification sous la forme d'un cachet, qui en garantit la provenance et l'intégrité.

La LCR peut être publiée par l'autorité de certification à chaque nouvelle révocation de certificat, ou périodiquement, par exemple une fois par jour.

Optionnellement, l'autorité de certification peut émettre des Delta LCR , c'est-à-dire des compléments à une LCR déjà publiée, qui sont à prendre en compte en attendant la publication de la prochaine LCR à jour. Ce mécanisme est peu répandu.

La norme RFC 5280 permet également la suspension temporaire d'un certificat, ce qui représente un statut distinct dans la LCR. Cette possibilité est rarement utilisée.

La publication de la LCR par l'autorité de certification est indispensable pour offrir aux utilisateurs la possibilité de valider les certificats, comme nous allons le voir au paragraphe suivant.

La validation de certificat

La validation de certificat est une opération qui doit être effectuée par tout utilisateur de certificat à chaque fois qu'il fait usage d'un certificat.

Rappelons que les utilisateurs de certificats ne sont pas les porteurs (les titulaires dont l'identité est certifiée), mais leurs correspondants, c'est-à-dire les personnes ou les serveurs qui doivent vérifier une signature électronique, authentifier un interlocuteur ou chiffrer des données à l'attention de quelqu'un (voir à ce sujet le chapitre 6 sur la confidentialité).

En l'absence de validation de certificat, l'utilisateur pourra vérifier que le certificat provient bien d'une autorité de certification digne de confiance, qu'il a bien été attribué à la personne dont l'identité figure dans le champ CN, mais ne saura pas si le certificat est toujours digne de confiance, c'est-à-dire si la clé privée correspondante est toujours entre les mains de son titulaire légitime, ni si ce titulaire fait toujours partie de l'entreprise qui lui a délivré le certificat.

Afin de permettre la validation de certificat, deux mécanismes principaux sont prévus :

- la liste de certificats révoqués ;
- le protocole OCSP (*Online Certificate Status Protocol*).

Utilisation de la liste de certificats révoqués

La LCR, comme nous l'avons vu précédemment, est publiée périodiquement par l'autorité de certification pour indiquer les certificats auxquels il ne faut plus accorder sa confiance. Chaque certificat contient le point

Copyright © 2012 Eyrolles.

de distribution de la LCR, c'est-à-dire l'adresse à laquelle elle peut être téléchargée. Il peut s'agir, par exemple, d'une URL (http://...) ou d'un emplacement dans un annuaire LDAP.

La plupart des outils permettant l'utilisation de certificats s'appuient automatiquement sur ce champ du certificat pour le valider avant d'en accepter l'utilisation, et affichent des messages explicites en cas de certificat révoqué.

Utilisation du protocole OCSP

Le protocole OCSP, normalisé par la norme RFC 2560, permet à l'utilisateur de déléguer la validation du certificat à une autorité de validation (AV). Le rôle de l'AV peut être sous le contrôle de l'AC qui a émis le certificat, ou pris en charge par une entité tierce, qui a alors une fonction de tiers de confiance.

Comme l'illustre la figure 5-12, le déroulement du protocole est le suivant.

- L'utilisateur interroge l'AV sur la validité du certificat, sur la base de l'AC émettrice et du numéro de série.
- L'AV télécharge régulièrement la LCR de chacune des AC sur lesquelles elle propose la fonction de validation.
- L'AV vérifie, dans la LCR à jour de l'AC indiquée, si le certificat est présent ou non.
- L'AV constitue une « réponse OCSP » dans laquelle elle indique le statut de révocation du certificat : valide, révoqué, suspendu, ou inconnu si, par exemple, la LCR est indisponible.
- L'AV scelle la réponse OCSP à l'aide d'un cachet serveur, qui en garantit la provenance et l'intégrité, et la transmet en retour au demandeur.
- Le demandeur vérifie le scellement de la réponse par l'AV, puis fait confiance à l'indication qu'elle a donnée pour accorder ou non sa confiance au certificat.

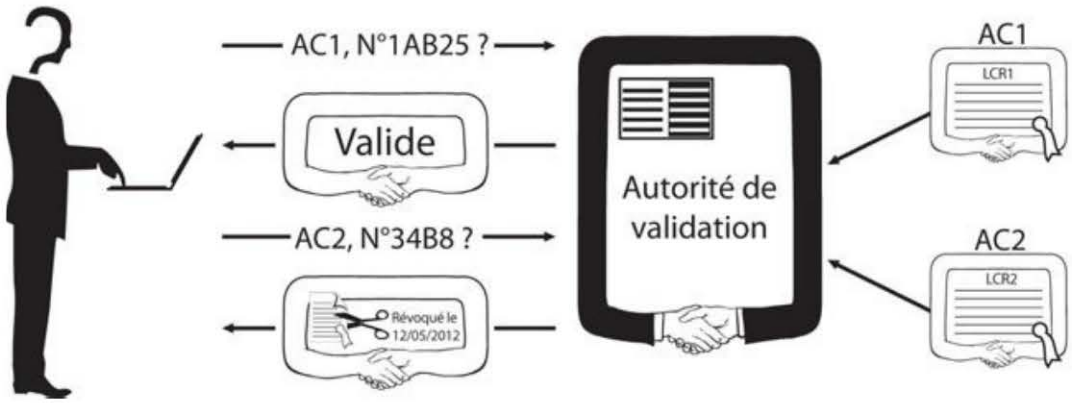


Figure 5-12 : Le protocole OCSP

Copyright © 2012 Eyrolles.

Validation de certificat et signature électronique

Afin de rendre une signature vérifiable hors ligne, il est pratique d'inclure directement dans cette signature une preuve de validité du certificat du signataire, sous la forme de la LCR complète ou d'une réponse OCSP portant sur le certificat du signataire.

La plate-forme de dématérialisation des marchés publics Achatpublic.com, par exemple, se positionne comme autorité de validation et inclut automatiquement dans toute signature électronique une réponse OCSP.

Dans le cadre du téléservice Réseaux et canalisations, l'Ineris a fait le choix d'inclure la LCR systématiquement dans les signatures. L'inconvénient est que la LCR est plus volumineuse que la réponse OCSP, mais l'avantage est qu'il n'y a alors pas besoin d'une autorité de validation dans la chaîne de la confiance.

Le renouvellement

Après l'expiration ou la révocation d'un certificat, il est nécessaire de le renouveler.

Le renouvellement est réalisé de la même manière que la demande initiale, mais des simplifications peuvent être mises en œuvre.

- Les contrôles peuvent être allégés, le dossier d'enregistrement étant déjà connu.
- Si l'authentification nécessaire au renouvellement est effectuée à l'aide du certificat initial avant son expiration, il est même possible de réaliser l'ensemble du renouvellement à distance.

Lors du renouvellement d'un certificat, il est possible de certifier à nouveau la même clé publique, ou de procéder à la génération d'une nouvelle bi-clé.

La première option est plus simple techniquement, et permet une continuité, en particulier en cas d'usage du certificat pour du chiffrement. En revanche, elle n'offre pas les garanties de sécurité pour lesquelles il a été prévu de procéder à un renouvellement : en effet, si un certificat comporte une date d'expiration, c'est pour éviter le risque que la clé privée ne soit compromise, le risque d'attaques augmentant naturellement avec le temps. Il est donc fortement conseillé de renouveler la bi-clé lors du renouvellement du certificat.

Copyright © 2012 Eyrolles.

La chaîne de la certification

Une succession d'autorités de certification

À part dans le modèle PGP, que nous évoquerons plus loin, le certificat d'un utilisateur ou d'un serveur est émis par une autorité de certification (AC). Celle-ci scelle le certificat du porteur par un cachet (cette opération est en fait réalisée sous le contrôle de l'AC par l'opérateur de certification).

Ainsi, pour vérifier la validité du certificat d'un porteur, il faut vérifier ce scellement. Or, cette vérification repose sur le certificat de l'AC… qu'il faut vérifier à son tour !

Le certificat de l'AC a lui-même souvent été émis par une AC d'un niveau supérieur, et ainsi de suite. Il est donc nécessaire d'effectuer la vérification de l'ensemble de cette chaîne d'AC jusqu'à celle du sommet, qui s'appelle (paradoxalement) « l'AC racine ».

L'AC racine a scellé elle-même son propre certificat : c'est ce que l'on appelle un certificat « autosigné ».

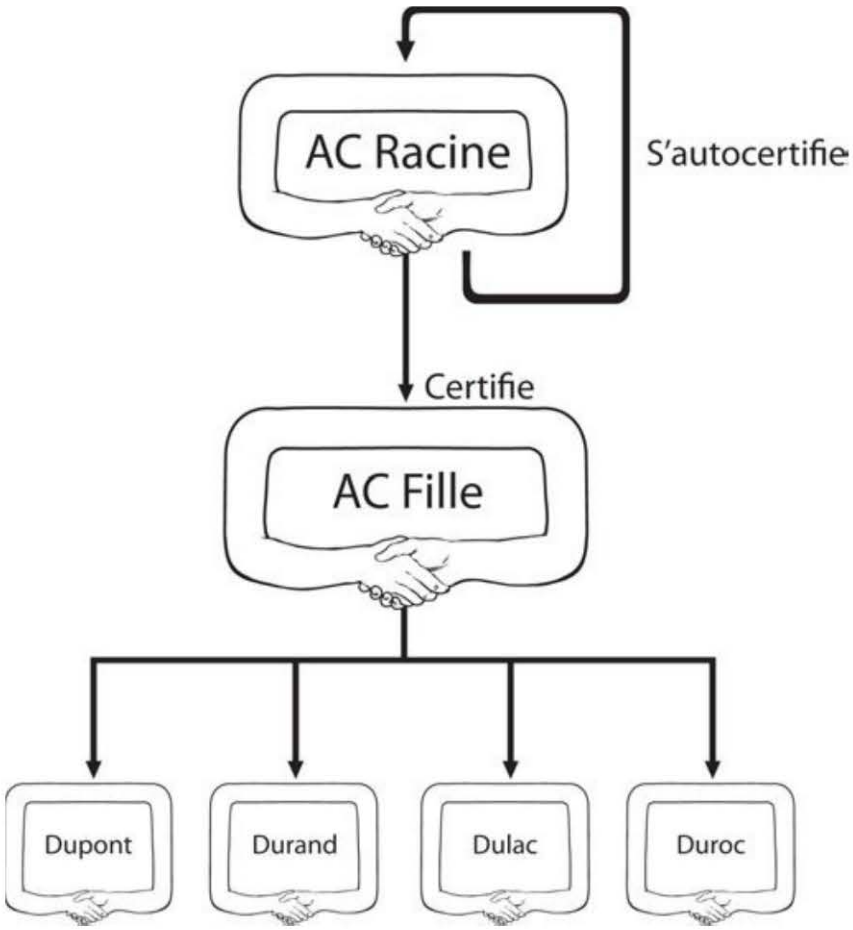


Figure 5-13 : La chaîne de la certification

Copyright © 2012 Eyrolles.

Il est possible, pour deux PSCE ayant des engagements similaires, de prendre un engagement réciproque sur la validité des certificats émis par l'autre. C'est ce que l'on appelle la « certification croisée » ou *cross-certification*. Ce schéma de confiance, illustré dans la figure 5-14, est mis en œuvre de la manière suivante :

- chaque PSCE exploite une chaîne d'autorités de certification, dont la racine est autosignée ;
- l'AC racine de chacun des PSCE certifie l'AC fille de l'autre, qui dispose alors de deux certificats : l'un émis par sa propre AC racine, l'autre émis par l'AC racine du PSCE partenaire ;
- ainsi, chaque certificat de porteur dispose de deux chaînes de la certification : l'une remontant à l'AC racine « d'origine », l'autre remontant à l'AC racine du partenaire.

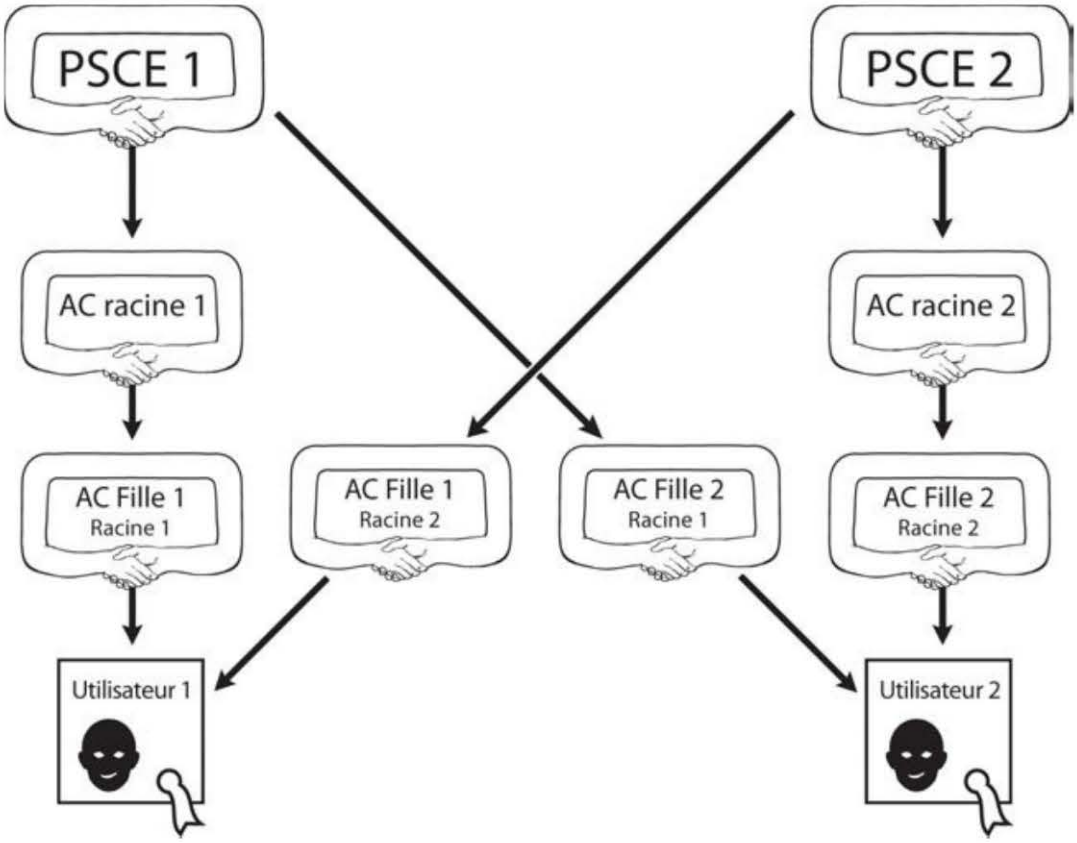


Figure 5-14 : La certification croisée

Copyright © 2012 Eyrolles.

Les différents niveaux de sécurité des certificats

La nécessité de niveaux de sécurité différents

Toutes les applications dématérialisées qui emploient des certificats n'ont pas les mêmes besoins de sécurité. Il arrive qu'au sein d'un même service, le niveau de sécurité requis pour différentes fonctions ou pour différents utilisateurs ne soit pas le même.

Ainsi, par exemple, dans la plate-forme de dématérialisation des procédures administratives Planet Limousin, le service de demande d'aide à la Région ne nécessite pas une authentification très forte du demandeur, puisqu'il n'y a aucun intérêt à demander une aide au nom de quelqu'un d'autre ; en revanche, la signature électronique du courrier d'attribution d'une aide doit émaner avec une fiabilité très grande du Président de Région.

Les niveaux de sécurité qui existent dans le domaine de la certification correspondent donc à un triple impératif :

- offrir le niveau de sécurité adéquat en fonction des enjeux et des contraintes, tels que déterminés dans l'étude de sécurité qui doit être menée en début de projet ;
- présenter un prix acceptable pour les utilisateurs et/ou le fournisseur du service, puisque l'utilisation d'un support cryptographique entraîne nécessairement un surcoût par rapport à un certificat sur support logiciel, et qu'une procédure d'enregistrement avec face à face et contrôle des papiers d'identité est plus coûteuse qu'une simple vérification automatique d'adresse e-mail ;
- permettre des temps de déploiement adaptés aux enjeux du projet.

Historiquement, les différents niveaux de sécurité des certificats ont été définis sous la forme de « classes ». La législation européenne a introduit la notion de certificat « qualifié ». Le RGS français, quant à lui, a défini des niveaux de sécurité différents sous la forme d'« étoiles ».

Nous allons détailler ces différentes notions dans les paragraphes ci-dessous.

Les classes de certificats

Introduite à l'origine par la société Verisign, la notion de classes de certificats est très répandue aujourd'hui dans tous les pays, y compris en France, où elle n'a pas encore été supplantée par les niveaux définis par le RGS.

Les classes de certificats correspondent aux types de vérifications réalisées au cours de la phase d'enregistrement du porteur en vue de la délivrance de son certificat.

Copyright © 2012 Eyrolles.

On distingue trois classes de certificats.

- La classe 1 correspond à des certificats délivrés sans contrôle d'identité, et ne garantissant que l'existence de l'adresse e-mail du porteur.
- La classe 2 correspond à des certificats délivrés à distance, sur contrôle de copie de pièces d'identité.
- La classe 3 correspond à des certificats délivrés suite à une rencontre physique entre l'autorité d'enregistrement et le porteur (le « face à face »), avec un contrôle de l'original de la pièce d'identité.

Lorsqu'une famille de certificats est délivrée sur un support cryptographique physique (carte à puce ou clé USB), le symbole + est ajouté à la classe. Ainsi, les certificats de classe 3+ sont délivrés en face à face, après contrôle de la pièce d'identité originale, et uniquement sur support physique, ce qui garantit l'existence de la clé privée en un seul exemplaire.

Il est à noter que la classe de certificat ne dit rien des procédures organisationnelles et techniques mises en place par l'autorité de certification : sécurité des locaux, protection des serveurs, confidentialité du traitement des données personnelles… Il s'agit donc d'une notion pratique mais insuffisante à apporter des garanties sur l'ensemble de la chaîne de la sécurité mise en œuvre. C'est pourquoi le législateur est allé plus loin en créant la notion de certificat qualifié et, dans le RGS, des niveaux de sécurité englobant un spectre plus large que le seul enregistrement des porteurs.

Les certificats qualifiés

La notion de certificat qualifié a été introduite par la directive européenne 1999/93/CE du 13 décembre 1999, portant sur un cadre communautaire pour les signatures électroniques.

Cette notion ne s'applique qu'aux seuls certificats utilisés à des fins de signature électronique. La principale caractéristique des certificats qualifiés est de comporter « une mention indiquant que le certificat est délivré à titre de certificat qualifié ».

Toutefois, le certificat qualifié doit être délivré par un PSCE répondant à de nombreuses exigences en termes de fiabilité organisationnelle, technique et financière, ainsi qu'en ce qui concerne la gestion des clés privées, qui ne doivent pas pouvoir être dupliquées. Les PSCE peuvent eux-mêmes se faire qualifier afin de bénéficier d'une présomption de conformité aux exigences liées à la délivrance de certificats qualifiés, mais cette démarche n'est pas obligatoire.

Cette directive a été transposée en droit français par le décret du 30 mars 2001. Les certificats qualifiés répondent aux obligations suivantes.

Copyright © 2012 Eyrolles.

Décret du 30 mars 2001 – Article 6

Un certificat électronique qualifié doit comporter :

a) Une mention indiquant que ce certificat est délivré à titre de certificat électronique qualifié.

b) L'identité du prestataire de services de certification électronique ainsi que l'État dans lequel il est établi.

c) Le nom du signataire ou un pseudonyme, celui-ci devant alors être identifié comme tel.

d) Le cas échéant, l'indication de la qualité du signataire en fonction de l'usage auquel le certificat électronique est destiné.

e) Les données de vérification de signature électronique qui correspondent aux données de création de signature électronique.

f) L'indication du début et de la fin de la période de validité du certificat électronique.

g) Le code d'identité du certificat électronique.

h) La signature électronique sécurisée du prestataire de services de certification électronique qui délivre le certificat électronique.

i) Le cas échéant, les conditions d'utilisation du certificat électronique, notamment le montant maximal des transactions pour lesquelles ce certificat peut être utilisé.

L'intérêt de la notion de certificat qualifié repose dans l'interopérabilité des certificats au niveau européen : l'utilisation de tels certificats permet la création de signatures électroniques dites « avancées » en droit européen ou « sécurisées » en droit français, dont la validité juridique doit être reconnue de manière équivalente dans tous les pays membres de l'Union européenne.

Les responsabilités du prestataire de services de certification électronique

La loi pour la confiance dans l'économie numérique (LCEN) définit les responsabilités du PSCE qui délivre les certificats de signature électronique qualifiés.

LCEN – Article 33

Sauf à démontrer qu'ils n'ont commis aucune faute intentionnelle ou aucune négligence, les prestataires de services de certification électronique sont responsables du préjudice causé aux personnes qui se sont fiées raisonnablement aux certificats présentés par eux comme qualifiés dans chacun des cas suivants.

1. Les informations contenues dans le certificat, à la date de sa délivrance, étaient inexactes.

2. Les données prescrites pour que le certificat puisse être regardé comme qualifié étaient incomplètes.

Copyright © 2012 Eyrolles.

3. La délivrance du certificat n'a pas donné lieu à la vérification que le signataire détient la convention privée correspondant à la convention publique de ce certificat.

4. Les prestataires n'ont pas, le cas échéant, fait procéder à l'enregistrement de la révocation du certificat et tenu cette information à la disposition des tiers.

Les PSCE ont la possibilité de limiter l'usage des certificats, par exemple en ce qui concerne le montant des transactions réalisées à l'aide du certificat, mais ces limites doivent figurer dans le certificat et être accessibles aux utilisateurs.

Ils doivent par ailleurs offrir des garanties financières suffisantes pour couvrir ces responsabilités.

Les étoiles du RGS

Le Référentiel général de sécurité définit, pour un certain nombre de fonctionnalités, trois niveaux croissants de sécurité.

- Une étoile (*) correspond au niveau adapté aux applications pour lesquelles les risques de tentatives d'usurpation sont moyens.
- Deux étoiles (**) correspond au niveau adapté aux applications pour lesquelles les risques de tentatives d'usurpation sont forts.
- Trois étoiles (***) correspond au niveau adapté aux applications pour lesquelles les risques de tentatives d'usurpation sont très forts.

On remarque immédiatement que les cas où le risque est faible n'ont pas été pris en compte par le RGS. Ce point est problématique dans la mesure où ce cas de figure existe et est même très fréquent, et le RGS s'impose à l'ensemble des administrations françaises. Ainsi, dans la sécurisation des téléservices, le RGS ne permet pas de recourir à une signature à un niveau inférieur à (*), qui est déjà relativement contraignant et coûteux si l'on souhaite délivrer des certificats au grand public.

Le RGS inclut des politiques de certification types correspondant aux trois niveaux de sécurité pour les certificats devant remplir les fonctions suivantes :

- authentification de serveur ;
- authentification de personne ;
- signature électronique ;
- authentification et signature électronique : seuls les niveaux (*) et (**) sont disponibles, le double usage n'étant pas conforme aux principes du niveau (***) qui requiert la séparation des usages sur des certificats différents : cela se justifie par les exigences différentes qui portent sur la gestion des clés privées, comme nous l'avons vu dans le tableau 5-2 ;

Copyright © 2012 Eyrolles.

- cachet ;
- confidentialité.

D'autres fonctions de sécurité sont abordées par le RGS, telles que l'horodatage, la gestion des clés cryptographiques, etc.

Les exigences du RGS portent sur l'ensemble des aspects organisationnels, fonctionnels et techniques mis en œuvre dans le cycle de vie des certificats, et pas uniquement, comme pour les classes de certificats vues précédemment, sur le processus d'enregistrement. On peut toutefois établir un parallèle entre les deux types de nomenclatures sur ce seul aspect d'enregistrement :

- RGS (*) correspond à la classe 2 ;
- RGS (**) correspond à la classe 3+ ;
- RGS (***) correspond à la classe 3+ pour des certificats qualifiés.

Le niveau de sécurité requis par l'application sera déterminé par une étude de sécurité, par exemple avec la méthode EBIOS (Expression des besoins et identification des objectifs de sécurité), à laquelle nous consacrons un paragraphe dans le chapitre 14 du présent ouvrage.

Comment et à qui accorder sa confiance ?

Les magasins de certificats de confiance

Il existe de très nombreuses autorités de certification, exploitées par des PSCE de toutes origines, et ayant des pratiques difficiles à vérifier pour l'utilisateur.

En effet, non seulement la politique de certification, qui décrit les engagements de l'AC, est en général rédigée dans la langue du pays de l'AC, mais de plus, il est difficile de s'assurer que les moyens mis en œuvre correspondent effectivement aux engagements.

Peut-on *a priori* faire confiance à un certificat émis par une autorité de certification chilienne ? Existe-t-il dans ce pays un dispositif d'audit et de qualification des AC ? L'État qui a instauré cet éventuel dispositif est-il lui-même digne de confiance ?

C'est pourquoi l'État français a mis en œuvre le dispositif de qualification que nous avons évoqué précédemment. Toutefois, disposer de niveaux de sécurité n'est pas suffisant, puisqu'en fonction du service que l'on met en œuvre, on devra s'appuyer sur des certificats d'un niveau plus ou moins élevé : il faut alors savoir distinguer, lorsqu'un certificat est présenté, s'il correspond bien au moins au niveau minimal requis.

Il convient donc, pour la vérification de certificats, de disposer de listes d'autorités de certification ou de familles de certificats éligibles, et d'exclure tout certificat émis par une AC ne faisant pas partie de cette liste.

Copyright © 2012 Eyrolles.

C'est le rôle des « magasins de certificats de confiance ».

On trouve un magasin de certificats de confiance dans la plupart des applications utilisant des certificats :

- le navigateur Internet s'appuie sur son magasin de certificats pour authentifier les sites web dignes de confiance : en particulier, Internet Explorer s'appuie sur le magasin inclus dans CAPI et prérempli avec les AC ayant passé un accord avec Microsoft ;
- un outil de vérification de signature électronique s'appuie sur un magasin de certificats pour recenser les familles de certificats de confiance : en particulier, Adobe Reader, qui inclut les fonctions de vérification de signature des documents PDF, en inclut un, prérempli avec les AC ayant passé un accord avec Adobe ;
- un serveur web qui réalise de l'authentification des utilisateurs par certificat s'appuie sur un magasin de certificats pour accepter ou non leur authentification...

Les internautes se servent majoritairement des magasins de certificats fournis en standard avec les logiciels. Mais ces magasins contiennent des certificats racine provenant de PSCE du monde entier, et qui ont été enregistrés au titre de leurs relations contractuelles avec les éditeurs. Ces familles de certificats peuvent être fiables… ou ne pas l'être ! Le fait qu'une AC soit référencée par Microsoft, Adobe ou Mozilla ne signifie pas qu'elle soit recevable dans le cadre juridique français, ni même qu'elle offre des garanties de sécurité suffisantes.

Cette prévalidation d'AC par les outils techniques constitue une faille de sécurité importante dans la chaîne de la confiance, d'autant plus que les utilisateurs n'y sont absolument pas sensibilisés, et que les menus servant à gérer ces éléments sont cachés dans les tréfonds les moins utilisés des options de configuration.

La bonne pratique, recommandée pour le grand public, mais plus aisément mise en œuvre en entreprise, consiste à vider les magasins de certificats de leur contenu par défaut pour n'y inscrire que les familles de certificats devant effectivement recueillir la confiance dans le contexte précis de l'utilisateur.

Certains services en ligne incluent en amont un filtrage qui évite à leurs utilisateurs d'avoir à se poser la question de la chaîne de la confiance – ou d'oublier de se la poser !

C'est le cas, par exemple, de la plate-forme de dématérialisation des marchés publics Achatpublic.com, qui recense les familles de certificats autorisées dans le cadre législatif correspondant à son activité, et signale à l'utilisateur toute utilisation d'un certificat provenant d'une autre source. Il reste ainsi possible pour un signataire de choisir un certificat

Copyright © 2012 Eyrolles.

non référencé, mais le destinataire le saura et pourra prendre les mesures adéquates : rejeter l'offre du candidat pour cause d'invalidité de sa signature, ou accepter sa signature si le certificat provient d'une AC étrangère offrant les mêmes garanties de sécurité que les AC françaises référencées, auprès desquelles le signataire n'aurait pas pu acheter de certificat du fait, par exemple, de l'éloignement géographique.

Le téléservice Réseaux et canalisations de l'Ineris, quant à lui, a opté pour une limitation stricte de l'usage aux seuls certificats référencés en France : l'applet de signature électronique incluse dans le service effectue un filtre préalable et ne laisse pas au signataire la possibilité de sélectionner un certificat qui ne soit pas conforme. Ainsi, aucun avertissement et aucun choix ne sont nécessaires du côté du destinataire de la signature, la confiance dans l'AC est établie de fait par le référencement effectué en amont par le service.

À quel niveau accorder sa confiance ?

Comme décrit dans la figure 5-15, il y a plusieurs niveaux possibles pour accorder sa confiance à un certificat.

Si l'on souhaite simplement reconnaître comme valide le certificat d'un seul utilisateur, on inscrira dans le magasin de certificats de confiance le seul certificat de cet utilisateur. Dans ce cas, les autres certificats émis par la même autorité de certification ne seront pas immédiatement acceptés, mais nécessiteront tous une validation par l'utilisateur. Ce choix permet un maillage très fin des interlocuteurs fiables, mais nécessite une vérification et une validation à chaque nouvel interlocuteur.

La confiance que l'on accorde à un certificat repose moins dans le porteur de ce certificat lui-même que dans les procédures mises en œuvre par l'autorité de certification qui le lui a remis. C'est pourquoi le choix le plus fréquent consiste à accorder sa confiance à des AC, en fonction du niveau d'accréditation (et donc de sécurité) qu'elles offrent. Ainsi, sur la figure 5-15, un PSCE exploite, sous une AC racine, deux familles de certificats : l'une d'elles, sécurisée (par exemple, qualifiée RGS (**) ou de classe 3+), offre un bon niveau de fiabilité ; l'autre, sans accréditation (par exemple, de classe 1 pour des besoins de démonstration), permet un déploiement plus souple des certificats mais avec un niveau de sécurité moindre. En enregistrant dans son magasin d'AC de confiance uniquement la première de ces AC, l'utilisateur pourra accorder sa confiance à l'AC « sécurisée » tout en restant méfiant vis-à-vis des certificats émis par l'AC « simple ». Tous les certificats émis par l'AC sécurisée seront validés automatiquement, ceux émis par l'AC simple provoqueront un message d'alerte et nécessiteront une vérification par l'utilisateur.

Copyright © 2012 Eyrolles.

Enfin, il est possible d'inscrire directement l'AC racine dans le magasin. Dans ce cas, tous les certificats émis par cette AC racine et par ses AC filles seront acceptés sans contrôle : aussi bien les certificats de classe 3+ émis par l'AC sécurisée que les certificats sans qualification émis par l'AC simple.

Même si le PSCE est un professionnel sérieux et fiable, éventuellement qualifié lui-même au sens du standard européen ETSI 101456, il reste libre d'appliquer des contraintes de sécurité différentes pour chacune de ses familles de certificats : accorder entièrement sa confiance à tous les certificats émis par ce PSCE constitue ainsi une faille de sécurité, puisque tous ces certificats n'ont pas le même niveau de fiabilité.

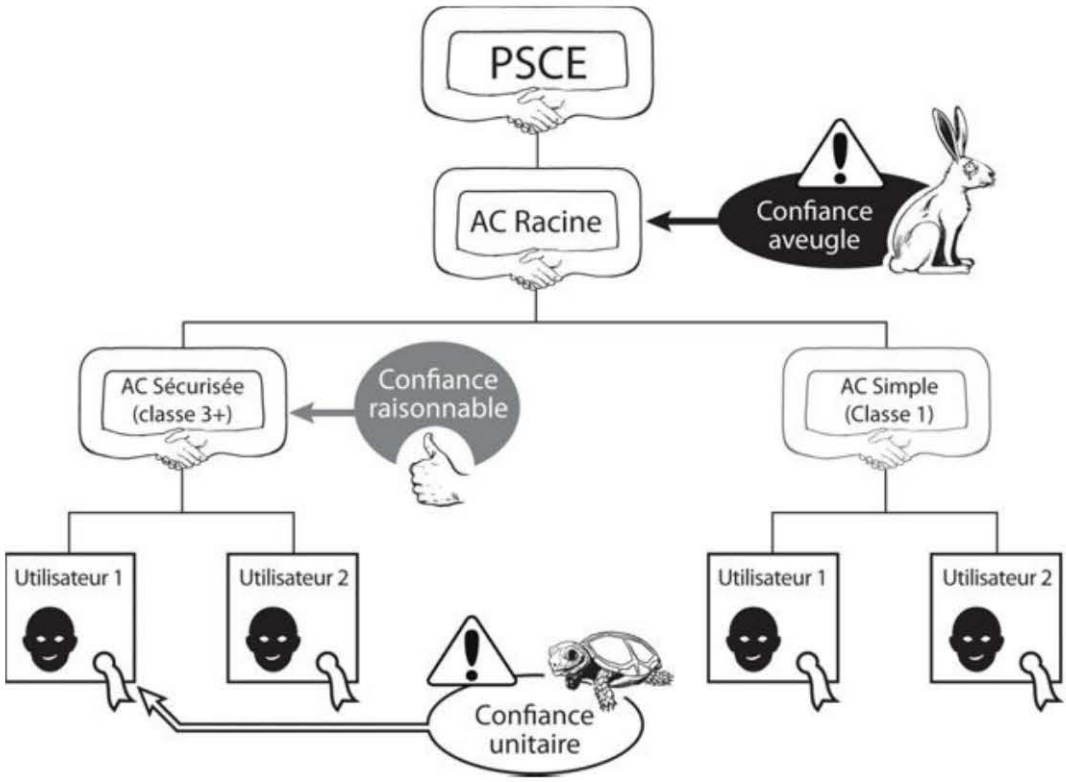


Figure 5-15 : À quel niveau accorder sa confiance ?

Le tableau 5-3 présente les avantages et les inconvénients de l'attribution de la confiance à chacun de ces niveaux de la chaîne de la certification.

Copyright © 2012 Eyrolles.

Tableau 5-3 : Avantages et inconvénients des différents niveaux de confiance

	Avantages	Inconvénients
Confiance accordée au certificat individuel	Niveau de sécurité très fin. Permet, par exemple, de contrôler, en plus de la validité du certificat, les habilitations ou les délégations de pouvoir accordées au porteur.	Nécessite une vérification et une acceptation pour chaque nouvel interlocuteur.
Confiance accordée à la famille de certificats	Permet de se fier aux procédures mises en œuvre par l'AC, qui est homogène pour tous les porteurs de certificats. Ne nécessite qu'une validation pour toute la famille de certificats. Très adapté lorsqu'il existe une liste limitative d'AC de confiance dans le contexte juridique de l'application.	N'inclut pas de contrôle au niveau de la personne : ils doivent être réalisés soit de manière humaine, par exemple lors d'une vérification de signature, soit au niveau applicatif, par exemple par la gestion des habilitations. Nécessite une vérification et une validation en cas d'interlocuteur muni d'un certificat appartenant à une autre famille.
Confiance accordée au PSCE	Aucun contrôle n'est nécessaire de la part de l'utilisateur : la complexité lui est masquée.	Faille de sécurité si le PSCE exploite des AC de niveaux de sécurité différents.

Tiers de confiance et autorité publique : hériter de la confiance du plus haut niveau

Les concepteurs d'applications dématérialisées ou les simples utilisateurs n'ont en général pas la compétence requise ou ne disposent pas des moyens nécessaires pour vérifier eux-mêmes la fiabilité des autorités de certification.

Dans ces conditions, accorder soi-même sa confiance « en aveugle » reviendrait à jouer à la roulette russe. C'est pourquoi, comme nous l'avons vu dans le chapitre sur la qualification des PSCO, il faut, pour accorder sa confiance, s'appuyer sur des qualifications officielles délivrées par les services de l'État, qui ont pour mission de s'assurer de l'efficience des mesures de sécurité selon des référentiels normatifs officiels.

Ce n'est ainsi en définitive ni à un porteur de certificat, ni à un PSCE que l'on accorde sa confiance, mais bien à l'État qui garantit, au plus haut niveau, la conformité des prestataires de services.

Copyright © 2012 Eyrolles.

Identité numérique et certificats : deux exemples de projets

La carte nationale d'identité électronique

De nombreux pays d'Europe ont adopté un titre d'identité électronique, sous la forme d'une carte à puce. Parmi eux, on peut citer l'Allemagne, l'Autriche, la Belgique, l'Estonie, la Finlande, l'Italie, les Pays-Bas, l'Espagne, la Suède…

Le but d'un tel choix est double :

- sécuriser la carte d'identité vis-à-vis de la fraude, en rendant plus complexe la fabrication de faux ;
- favoriser le développement de services dématérialisés, en fournissant aux citoyens un moyen d'authentification et de signature électronique.

Dans certains pays, cette carte est très utilisée pour les e-services, qu'ils soient privés ou publics. Ainsi, par exemple, la carte d'identité estonienne, qui a valu au pays son surnom de « e-stonia », est utilisée comme moyen d'authentification pour toutes les téléprocédures du secteur public, et notamment pour le vote par Internet.

Dans d'autres pays, en revanche, malgré la fourniture gratuite d'un lecteur de carte, les usages ne décollent pas : c'est le cas notamment en Belgique.

En France, le projet d'une carte nationale d'identité électronique existe depuis le début des années 2000. Conçue par l'Agence nationale des titres sécurisés (ANTS), la CNIE devait, d'après le texte voté par l'Assemblée nationale le 6 mars 2012, comporter deux puces entièrement étanches : la première, sans contact, contenant les données d'état civil et répondant ainsi à la première préoccupation, et la seconde, semblable à une puce de carte bancaire, pouvant servir à accueillir des certificats électroniques dans le but du développement de la dématérialisation auprès du grand public.

Toutefois, suite à une censure du Conseil constitutionnel le 22 mars 2012, seule la puce sans contact semble devoir être conservée. Cette puce « régalienne » contiendra, outre les données d'état civil (le nom de famille, le ou les prénoms, le sexe, la date et le lieu de naissance, le nom d'usage, le domicile), des données biométriques (la taille, la couleur des yeux, les empreintes digitales et la photographie).

Seuls pourront accéder à ces données « les agents chargés des missions de recherche et de contrôle de l'identité des personnes, de vérification de la validité et de l'authenticité des passeports et des cartes nationales d'identité électroniques ».

La loi instituant cette carte incluait également la constitution d'un large fichier biométrique centralisé, qui a également été rejeté par le Conseil constitutionnel.

Copyright © 2012 Eyrolles.

Le coup de frein donné à ces projets montre leur extrême sensibilité dans la perception française de l'identité et des libertés individuelles.

Mais les travaux relatifs à la sécurisation des titres d'identité ne se limitent pas à la seule CNIE, comme l'illustre le témoignage de monsieur le Préfet Bertrand Maréchaux, directeur de l'ANTS.

Parole d'expert

Monsieur le Préfet Bertrand Maréchaux, directeur de l'Agence nationale des titres sécurisés

L'ANTS déploie actuellement des cartes d'agents publics permettant l'authentification forte et la signature électronique pour la perfection des actes juridiques qui incombent aux services de l'État et des mairies. Pour quel niveau de sécurité avez-vous opté ?

De nombreuses expérimentations sont en cours ou achevées avec succès, notamment avec le ministère de la Justice et des Libertés, le ministère de la Défense et des Anciens Combattants, et avec des mairies pour la gestion des données d'état civil dans le cadre de la Communication électronique des données d'état civil (COMEDEC).

Chaque projet est indépendant pour ce qui est du niveau de sécurité requis et du processus d'enregistrement. À titre d'exemple, la signature électronique des magistrats mise en œuvre lors de l'expérimentation qui a eu lieu à Bordeaux fin 2011 s'appuie sur un certificat RGS (***).

Le rôle de l'ANTS consiste à concevoir la carte, à fixer les normes en collaboration avec l'ANSSI, à gérer les interfaces et à réaliser ou non l'enregistrement des porteurs selon les projets. L'ANTS garantit la conformité de la carte et du certificat au niveau de sécurité requis, mais n'impose pas ce niveau de sécurité, qui est fonction des contraintes et des usages propres à chaque déploiement.

Les cartes, quant à elles, sont personnalisées graphiquement et électriquement par l'Imprimerie nationale.

Dans le cadre du projet de carte nationale d'identité électronique (CNIE), les citoyens devaient bénéficier sur leur carte d'une puce « e-services » pouvant héberger des certificats. Cette disposition a été censurée par le Conseil constitutionnel. Comment faut-il prendre cette censure ? Selon vous, cet engagement de l'État sur la fourniture de moyens techniques est-il de nature à favoriser ou entraver le développement de l'économie numérique ?

L'usage n'est pas de commenter la décision de cette haute instance mais d'en comprendre le message : la question du jumelage entre une puce et un titre nécessitait l'intervention d'une proposition de loi, mais celle-ci n'a pas défini de façon assez précise les détails déterminant le fonctionnement de la puce « e-services ».

De fait, cette censure du Conseil constitutionnel n'est pas la traduction d'une prise de position de l'État sur l'intérêt ou non de s'engager sur le développement de l'identité numérique mais la position de la haute juridiction sur une modalité spécifique envisagée du développement de celle-ci.

Copyright © 2012 Eyrolles.

Si cette puce « e-services » avait été adoptée, les citoyens souhaitant utiliser leur CNIE à des fins d'authentification sur Internet ou de signature électronique auraient pu se procurer un certificat auprès d'une autorité de certification privée. Où aurait été placée la limite entre l'identité d'état civil, garantie par l'État, et l'identité numérique ?

Le rôle de l'État n'est pas de s'immiscer dans les transactions privées, mais de garantir l'identité des personnes physiques, et de faciliter la procédure d'enrôlement garantissant l'identité à ceux qui auraient acquis un certificat électronique auprès d'une autorité de certification privée.

Nous aurions mis en œuvre un tiers de confiance dont le rôle aurait été de garantir aux prestataires de services de certification électronique l'identité des demandeurs de certificats, afin de supprimer les possibilités de fraude tout en protégeant la confidentialité des identifiants et des transactions.

Le label Idénum

Lancé publiquement en 2010 par la Secrétaire d'État chargée de la Prospective et du développement de l'économie numérique, et porté de manière opérationnelle par la Caisse des dépôts depuis 2011, le label Idénum a pour vocation d'améliorer la confiance dans l'économie numérique tout en simplifiant l'accès des internautes aux services dématérialisés, qu'ils soient offerts par des collectivités publiques ou des acteurs privés.

Le principe est de favoriser la signature électronique et le contrôle d'accès aux services par certificat, en définissant un niveau de sécurité correspondant aux besoins de la grande majorité des applications.

Le projet a également pour but de promouvoir la distribution de ces certificats par un modèle économique adapté au grand public, mais aussi au B to B (relations interentreprises).

Les certificats labellisés Idénum seront délivrés sur un support cryptographique physique, et permettront l'authentification et la signature électronique.

Parole d'expert

Fabrice Mattatia, responsable d'Investissements numériques, CDC

Le label Idénum vise à harmoniser le niveau de sécurité des certificats exigés par les services dématérialisés vis-à-vis des internautes pour l'authentification et la signature électronique. Quel est le modèle proposé ?

Le projet vise surtout à harmoniser le niveau de sécurité des certificats proposés aux internautes par les différents fournisseurs de services. Il s'agit de créer pour l'identité numérique l'équivalent du système CB pour la carte bancaire : un standard technique unique, plusieurs émetteurs, des produits interopérables acceptés de manière indiscriminée sur tous les sites participant au réseau.

Le label couvre les aspects techniques liés au PSCE sous-jacent, mais aussi les processus de vérification de l'identité des demandeurs et de délivrance du support du certificat et du code PIN associé mis en œuvre par le fournisseur de services.

Copyright © 2012 Eyrolles.

Afin de garantir une cohérence avec les politiques publiques, le label s'appuie aussi bien sur le RGS que sur le cahier des charges de référencement de l'administration électronique.

Quels bénéfices en attendez-vous pour le développement de l'économie numérique ?

L'objectif est de faciliter la dématérialisation au sens large, qu'elle concerne les échanges entre le grand public et les différents acteurs économiques, entre les entreprises ou avec l'administration. Il s'agit à la fois d'apporter plus de sécurité dans l'accès aux différents comptes grâce à la fonction d'authentification, et de promouvoir le remplacement des échanges papier par des échanges électroniques grâce à la signature électronique.

Avec un seul outil, l'internaute aura accès à différents services qui, aujourd'hui, lui imposent chacun un moyen d'accès différent qui lui est propre. Il aura également accès à des services qui, aujourd'hui, n'existent pas, faute de la disponibilité sur le marché de signature électronique interopérable.

Si de tels outils étaient généralisés à l'ensemble de la population, on pourrait ainsi dématérialiser des centaines de millions de formulaires, générant une économie globale pour la société de milliards d'euros. C'est l'économie déjà réalisée par la seule assurance maladie obligatoire grâce au système Sesam-Vitale, qui génère un milliard d'euros d'économies par an pour des assurés qui l'utilisent vingt fois par an en moyenne.

Quelles sont les applications types visées par le projet Idénum, dans les sphères publique et privée ?

Pour le grand public, il s'agit d'abord de couvrir des besoins d'accès à des comptes personnels avec une forte valeur ajoutée : par exemple, le DMP (Dossier médical personnel), le compte bancaire, les jeux d'argent en ligne, l'administration électronique en général.

L'internaute pourra également accéder à des fonctionnalités nouvelles : éviter des échanges papier grâce à la signature électronique de souscription de contrats d'assurance ou d'épargne, de télécom, d'énergie, etc., mais aussi bénéficier de fonctionnalités étendues sur des services déjà existants, comme les virements externes à partir de son compte en banque.

Pour les professionnels, les certificats Idénum permettront de sécuriser les échanges avec l'administration (comme les déclarations sociales ou la candidature aux marchés publics), mais également avec leurs partenaires privés : signature de courriers électroniques, commandes, ordres, etc. Ils permettront également de sécuriser les réseaux sociaux professionnels en validant en amont l'identité du titulaire de chaque page.

Quels supports sont envisagés pour les certificats Idénum ?

Idénum vise un niveau de sécurité identique quel que soit le support. Les certificats pourront donc aussi bien être sur des cartes à puce, des clés cryptographiques USB, des cartes SIM ou MicroSD.

Idénum s'adapte ainsi aux nouvelles pratiques de navigation, qui sont de plus en plus mobiles : il y aura bientôt plus de « mobinautes » que d'internautes.

Copyright © 2012 Eyrolles.

Les conséquences catastrophiques d'une sécurité insuffisante : la faillite de Diginotar

Les faits

Nous allons illustrer le concept de chaîne de la sécurité par le douloureux exemple du prestataire de services de certification électronique hollandais Diginotar, qui a fait faillite en 2011 suite à une compromission de son système d'information.

Les faits tels qu'ils ont été rendus publics dans le rapport d'audit de la société Fox-it du 5 septembre 2011 sont les suivants : Diginotar émettait des certificats de plusieurs niveaux de sécurité, notamment des certificats qualifiés, des certificats SSL pour les serveurs, et des certificats produits sous contrôle de l'État hollandais.

Un pirate est parvenu à générer de vrais faux certificats sur l'infrastructure de Diginotar après avoir obtenu un accès aux serveurs. Les clés privées de Diginotar étaient bien exploitées sur des matériels cryptographiques (HSM), qui n'ont pas été mis en cause dans le piratage qui a eu lieu : c'est le serveur qui faisait appel à ces HSM qui était piraté. Les certificats forgés par le pirate ont été utilisés notamment pour réaliser une attaque *man in the middle* : un faux serveur google.com permettait de filtrer tous les accès aux services légitimes à ce service sur le territoire iranien, où le pirate a ainsi potentiellement eu accès à tous les comptes Gmail et à tous les documents Google Docs du pays.

Une attaque *man in the middle* (l'homme du milieu) consiste à se placer en coupure du flux légitime : les échanges sont retransmis inchangés après avoir été écoutés.

Retiré de la liste des autorités de certification digne de confiance, Diginotar ne s'est pas remis du scandale.

Les causes

Les causes du piratage telles que nous pouvons les analyser à partir des informations publiques sont les suivantes.

Analyse de sécurité insuffisante : les enjeux d'un piratage potentiel ont sans doute été sous-estimés lors de la création de l'entreprise et de la conception de son système d'information. Étant donné l'importance des enjeux pour les clients de Diginotar et le fait que la sécurité soit le cœur de métier de l'entreprise, une faille de sécurité avait nécessairement une conséquence vitale pour l'entreprise.

Failles de sécurité technique :

- l'ensemble des machines de l'opérateur de certification étaient dans un même domaine Windows, sans cloisonnement. Ainsi, pirater une machine donnait accès à l'ensemble ;

Copyright © 2012 Eyrolles.

- aucun antivirus n'était actif sur les machines, or le pirate s'est appuyé notamment sur un logiciel malveillant connu qui aurait été détecté par tout antivirus (mais également sur un logiciel développé par lui-même qu'il a pu installer grâce aux brèches ouvertes) ;
- il existait une sonde de détection d'intrusion, mais elle n'a fait remonter aucune alerte : cela pose la question de la fiabilité de ce type de logiciel et de la capacité des clients à les tester.

Failles de sécurité applicative :

- les administrateurs système accédaient aux machines par un simple identifiant/mot de passe, sans authentification forte ;
- aucun système de traçabilité sécurisée n'était en place, le pirate a pu supprimer les traces de son « travail » sans qu'aucune alerte soit notifiée ;
- les appels au service de contrôle de révocation portant sur des numéros de série de certificats inconnus ne produisaient pas d'alerte.

Failles de sécurité comportementale :

- les mots de passe étaient faibles, facilement attaquables par force brute (voir le chapitre 4 et sa section sur la bonne gestion des mots de passe) ;
- les contrôles de sécurité étaient vraisemblablement absents ou faits sans aucun zèle, les exploitants techniques ayant confiance dans le système qu'ils étaient censés surveiller !

Une défaillance du système national d'audit : Diginotar ne disposait pas d'une qualification. Les accréditations lui permettant de délivrer des certificats qualifiés ont vraisemblablement été données sans un réel contrôle de la qualité des mesures de protection mises en œuvre. La responsabilité de l'État hollandais, qui avait confié l'émission de certificats à ce prestataire, est ainsi également à remettre en cause.

Du fait des failles présentes sur l'ensemble de la chaîne de la sécurité, la catastrophe a été possible. Devant les attaques d'un pirate décidé et compétent, pallier une seule de ces failles n'aurait pas été suffisant. Pour éviter le piratage, il aurait fallu que le réseau soit cloisonné, que les accès soient contrôlés de manière sûre, qu'un antivirus soit actif, que l'application de délivrance des certificats soit mieux conçue, et que les exploitants soient mieux formés.

Les causes en amont sont sans doute la volonté de la direction générale de Diginotar de réduire les coûts, et les insuffisances du dispositif d'audit et de qualification hollandais.

Copyright © 2012 Eyrolles.

Les conséquences

Les conséquences de ce triste exemple se situent à plusieurs niveaux.

Elles frappent tout d'abord les utilisateurs concernés. Lorsqu'on connaît l'importance qu'a eue l'utilisation des moyens modernes de communication dans le développement des révolutions arabes, il est possible de se demander combien d'opposants au régime iranien sont aujourd'hui surveillés ou menacés du fait d'accès de tiers à leur espace de communication (bien qu'aucun élément ne permette de garantir que le piratage de Diginotar ait été commandité par le pouvoir iranien).

Elles touchent ensuite l'entreprise Diginotar elle-même, puisqu'elle a fait faillite.

Enfin, elles atteignent l'ensemble de la chaîne de la confiance au niveau international : un discrédit important a été jeté sur la fonction de prestataire de services de certification électronique, et sur les professionnels de la sécurité en général :

- en aval sur tous les certificats émis par ce PSCE, même ceux qui ont été valablement produits ;
- mais surtout, en amont, sur le système de contrôle mis en place par l'État hollandais, et donc par ricochet sur tous les autres PSCE du pays et sur l'ensemble des certificats électroniques hollandais – voire européens.

Parole d'expert

Armelle Trotin, présidente de LSTI

LSTI est accréditée par le Cofrac et habilitée par l'ANSSI pour procéder à la qualification des prestataires de services de confiance au regard du Référentiel général de sécurité. Quels moyens mettez-vous en œuvre pour garantir la qualité des prestataires que vous auditez ?

Tout d'abord, il est important de préciser que LSTI ne garantit pas la qualité des prestataires audités, mais leur conformité aux exigences liées à leur métier, ces exigences pouvant être de nature normative ou réglementaire. Ainsi, la sécurité effective garantie par un audit dépend en grande partie de la pertinence technique du référentiel.

Un référentiel d'audit est en général constitué conjointement par l'ensemble des parties prenantes : les utilisateurs, qui poussent pour des exigences de qualité très élevée, les prestataires, qui modèrent par les aspects économiques et techniques, les autorités réglementaires, et les organismes d'audit. Il s'agit donc toujours d'un compromis, et en aucun cas d'une garantie absolue.

Notre accréditation par le Cofrac, fondée sur un audit réalisé dans nos locaux, reconnaît la conformité de LSTI aux normes de bonnes pratiques des activités de certification : il s'agit d'une attestation de compétence généraliste. L'habilitation décernée par l'ANSSI vient compléter cette reconnaissance par son aspect extrêmement ciblé,

Copyright © 2012 Eyrolles.

spécifique à la sécurité informatique et à la dématérialisation, et en particulier à la mise en œuvre du RGS chez les PSCO.

Sur le terrain, nos audits portent aussi bien sur les aspects documentaires que sur des inspections techniques sur site. Les audits sont réalisés de manière périodique, tous les 12 mois. Ils donnent lieu à un rapport de conformité et à des demandes de corrections en cas de non-conformités identifiées.

Nos auditeurs sont formés par nos soins : ils doivent participer à un certain nombre d'audits en compagnie d'auditeurs déjà habilités par nous avant de pouvoir être autonomes. Ce tutorat est ensuite complété, pour un suivi dans le temps, par un audit de supervision réalisé sur le terrain au moins tous les deux ans par un super-auditeur. Le maintien de l'habilitation d'un auditeur est également subordonné à la réalisation d'un nombre minimal d'audits annuels. Par ailleurs, tous nos auditeurs passent un examen pour obtenir une habilitation de l'ANSSI.

Le maintien à jour de notre compétence passe également par notre participation à l'élaboration des référentiels normatifs : ETSI, AFNOR, RGS...

Quel est votre degré de responsabilité par rapport aux éventuelles failles de sécurité (organisationnelles, techniques ou autres) que vous constatez (ou non) chez les prestataires que vous auditez ?

Nous sommes soumis à une double obligation : obligation de moyens et obligation d'action.

Lors des audits, qui doivent être réalisés de bonne foi et par des auditeurs qualifiés, un organisme de certification doit tout mettre en œuvre pour constater les dérives des pratiques et les manquements au référentiel d'audit. Il peut évidemment arriver que l'audit ne révèle pas l'intégralité des non-conformités, mais la fréquence annuelle des contrôles garantit un bon degré de couverture du référentiel normatif.

Nous avons par ailleurs une obligation d'action en cas d'identification d'un manquement grave au référentiel d'audit. Si nous constations une anomalie sans imposer les mesures correctives correspondantes, ou sans retirer la qualification au candidat en cas de refus d'action, notre responsabilité pourrait être mise en cause directement en cas d'incident découlant de cette anomalie.

Une certification conforme ou une qualification ne réduit pas la responsabilité du prestataire qui l'a obtenue : elle sert à faire la preuve de ses efforts de conformité par rapport à la loi, au référentiel normatif, aux bonnes pratiques de l'état de l'art.

La faillite de Diginotar a montré que les manquements de sécurité d'un PSCO peuvent avoir des conséquences catastrophiques pour le prestataire et pour ses clients. Selon vous, le dispositif de qualification mis en place en France nous met-il à l'abri d'un « Diginotar français » ?

Tout d'abord, en l'absence d'un équivalent du RGS aux Pays-Bas, Diginotar n'était pas un prestataire qualifié. Si tel avait été le cas, l'organisme auditeur aurait certainement été entendu dans les conséquences du piratage.

Toutefois, ce qui est majoritairement reproché à Diginotar n'est pas d'avoir été l'objet d'attaques, mais d'une part de ne pas s'en être rendu compte rapidement et d'autre part, de ne pas avoir réagi, notamment par une communication rapide vers les clients et les utilisateurs de certificats.

Copyright © 2012 Eyrolles.

La qualification RGS inclut des exigences liées à la surveillance des attaques et à la réaction, sous la forme de l'existence d'un plan de crise. Elle impose au prestataire de faire une analyse de risque, de la mettre à jour régulièrement et de prendre les mesures nécessaires identifiées par cette analyse de risque. Nos auditeurs vérifient l'existence et la pertinence de l'étude de sécurité et du plan de crise.

Si la qualification RGS ne protège pas nos prestataires de services des tentatives de piratage, elle garantit au moins qu'ils aient mis en œuvre des mesures de protection conformes à l'état de l'art, et prévu un plan d'action de nature à préserver au mieux les intérêts de leurs clients en cas d'attaque.

Les solutions alternatives au modèle actuel

Le modèle très répandu de gestion des certificats, appelé « Infrastructure à clé publique », ou P*ublic Key Infrastructure* (PKI) en anglais, consiste à centraliser tous les éléments de sécurité auprès d'un tiers de confiance, le prestataire de services de certification électronique.

Ce paradigme crée à la fois une assez grande facilité de surveillance (les audits nécessaires portent sur un environnement restreint, maîtrisé), et une grande faiblesse du système de sécurité, puisqu'il suffit d'attaquer avec succès un prestataire pour porter atteinte à la sécurité de très nombreux autres acteurs, les clients du PSCE, qu'il s'agisse d'entreprises qui protègent leur système d'information ou d'individus qui achètent des certificats à des fins, par exemple, de signature électronique.

Le risque lié aux PKI est connu de longue date mais n'a pas empêché le déploiement à très large échelle de cette solution, et même sa prise en compte dans les textes de lois, notamment les directives européennes et leur transposition dans les droits nationaux des pays membres de l'Union.

La faillite de Diginotar met en lumière les risques liés à la PKI et entraîne deux types de réactions :

- du côté des PSCE, une vérification des conditions d'exploitation des services et un durcissement de la politique de sécurité ;
- du côté des théoriciens de la sécurité informatique, l'accélération de la recherche de solutions alternatives.

Nous allons illustrer cela par trois exemples de modèles alternatifs.

Le modèle PGP

Créé en 1991 par Philip Zimmermann, cryptologue et activiste de la protection des droits individuels, le modèle PGP se veut une alternative au modèle centralisé des infrastructures à clé publique dans lequel une autorité de certification se porte garante de l'identité des porteurs de certificats.

Copyright © 2012 Eyrolles.

Le principe de PGP est participatif, comme l'illustre la figure 5-16 : chaque individu génère sa propre bi-clé (voir le chapitre 2 pour plus de détails) et son propre certificat, qu'il diffuse à ses correspondants. Ceux-ci peuvent alors à leur tour certifier l'identité du porteur de certificat, sur la base de la confiance qu'ils ont en lui. En recoupant les niveaux de confiance accordés par les autres utilisateurs du système, chacun peut à son tour déterminer s'il fait lui-même confiance ou non à un correspondant.

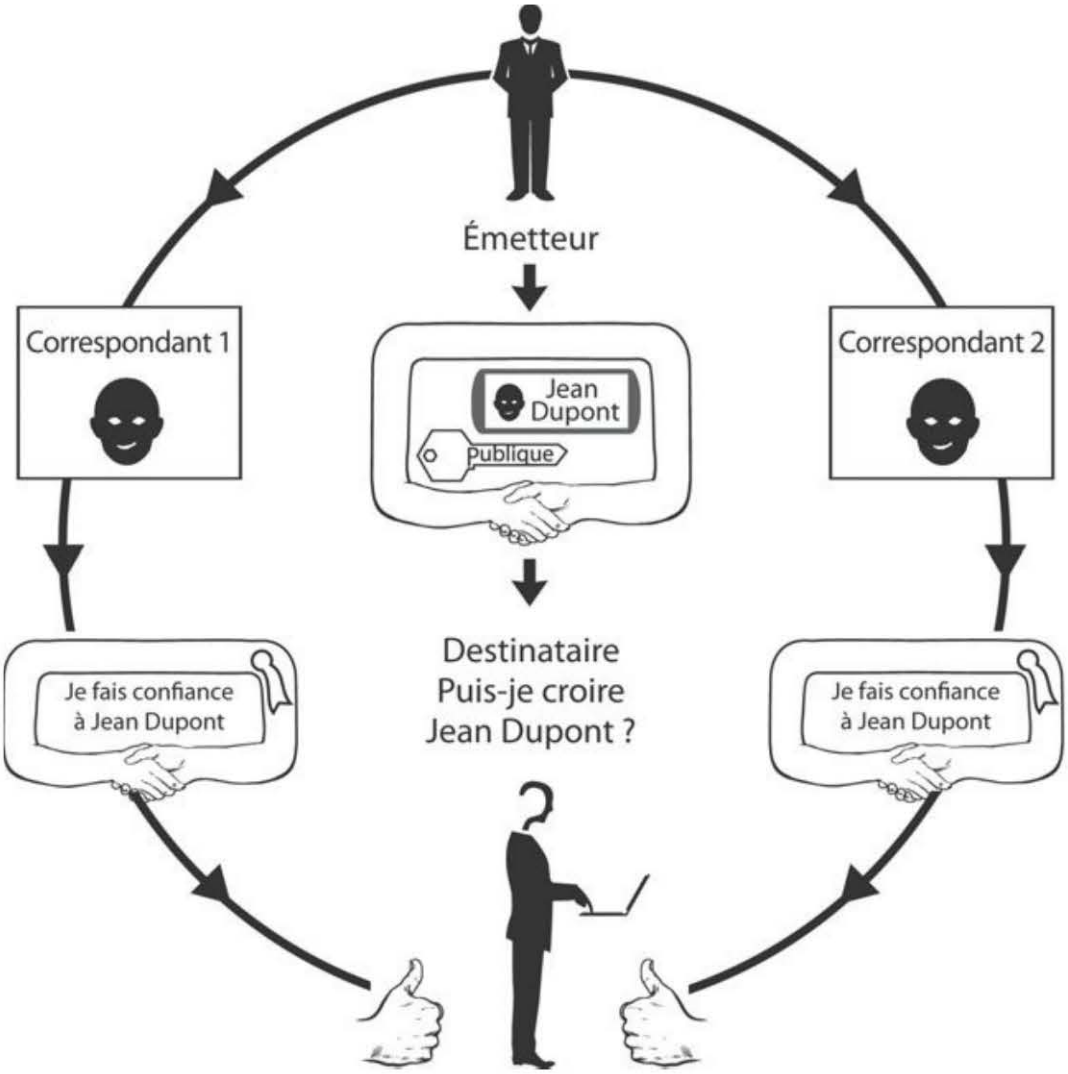


Figure 5-16 : Le modèle PGP

Il n'y a ainsi pas de contrôle formel des identités : la sécurité du système repose sur un « réseau de confiance » qui se bâtit petit à petit.

Si ce modèle réduit le risque de catastrophe en cas de compromission d'une AC (comme dans l'exemple de Diginotar), il ne permet pas en revanche d'avoir confiance *a priori* dans l'identité d'un signataire, puisqu'un

Copyright © 2012 Eyrolles.

nouvel entrant dans le système bénéficiera d'un niveau de confiance faible. PGP ne permet donc les échanges que dans un cercle fermé d'utilisateurs qui se connaissent, et qui ont accepté à l'origine un certificat autosigné transmis par un moyen non sécurisé, l'e-mail par exemple.

Parole d'expert

Philip Zimmermann, cryptologue

Vous avez depuis toujours attiré l'attention sur les risques liés aux infrastructures à clé publique (PKI, *Public Key Infrastructure*). Selon vous, quels en sont les inconvénients majeurs ?

La protection de serveurs par SSL, qui s'appuie sur les certificats, n'offre pas une sécurité suffisante du fait de la possibilité d'attaques *man in the middle* si l'autorité de certification est piratée. Les PKI centralisées, du fait de la complexité de leur gestion, introduisent un maillon faible dans la chaîne de la sécurité.

Les navigateurs Internet sont obligés de faire confiance aux certificats des autorités de certification car le modèle de confiance est trop complexe pour être porté à la connaissance des utilisateurs. Cette faille conceptuelle ne peut pas être modifiée, elle est inhérente au modèle de la PKI.

La difficulté à gérer correctement le cycle de vie des certificats (expiration et renouvellement des clés, révocation des certificats) provoque l'apparition de nombreux faux messages d'alerte aux utilisateurs, qui prennent l'habitude de presser le bouton OK sans réfléchir.

Quels enseignements tirez-vous du piratage de Diginotar ?

En Occident, et dans les démocraties en général, nous vivons dans un environnement bienveillant, où l'État est *a priori* là pour défendre les parties légitimes du commerce électronique. Par exemple, nous utilisons le protocole SSL pour sécuriser les paiements : il existe de la traçabilité et des assurances en cas de compromission de l'autorité de certification. Le système légal protège les consommateurs et les banques en cas de défaillance de la PKI.

En revanche, dans les pays soumis à une dictature, Internet est un outil de résistance face à l'oppression. Les attaques *man in the middle* qui ont pu être réalisées en Iran grâce au piratage de Diginotar ont sans doute permis au pouvoir en place d'avoir accès aux communications privées des opposants au régime, et ainsi de les identifier et de les arrêter. Dans de tels pays, les attaques contre la sécurité informatique sont perpétrées par ceux-là même qui ont le contrôle du système légal et judiciaire. Il n'existe donc pas de garde-fou. Tant qu'un système de sécurité plus fiable que les certificats n'est pas disponible, il faut considérer que des rencontres physiques sont plus sûres que des échanges *via* Internet dans un contexte de résistance.

Cela pose la question de la responsabilité des acteurs du secteur de la « confiance » : les failles de sécurité et le retard de communication de Diginotar ont mis en danger la vie de centaines de personnes. La direction et les employés de Diginotar auraient-ils agi ainsi s'il s'agissait de leur propre vie ou de celle de leurs enfants ?

Copyright © 2012 Eyrolles.

Il est du devoir des professionnels de la sécurité d'avertir sur les risques et de lever des alertes vis-à-vis de la confiance réelle que l'on peut mettre dans les systèmes « sécurisés » actuels. Et, bien entendu, de chercher des solutions...

Existe-t-il des solutions ?

Tout d'abord, des approches différentes doivent être mises en œuvre en fonction du contexte légal et des enjeux : le paiement en ligne n'a pas les mêmes contraintes que la résistance à l'oppression politique, les mêmes solutions ne devraient pas s'appliquer.

Des technologies alternatives sont en cours de conception et de test (NDLA, voir ci-dessous). Le monde de la cryptologie a pris conscience de la réalité du problème. Il y a une réelle volonté internationale de trouver les modèles alternatifs, et une masse critique d'applications qui en ont besoin : cela prendra du temps, mais les solutions du futur émergeront nécessairement du fait que le problème est incontournable.

Reste à avoir une volonté politique – et l'argent suffisant pour payer les chercheurs !

Nota Bene : Philip Zimmermann est également le créateur du protocole ZRTP de confidentialité de la voix sur IP.

Le modèle Convergence

Le modèle Convergence a pour objectif de permettre à l'internaute de choisir librement un « notaire » à qui il sous-traite les opérations de vérification relatives aux certificats des sites web.

Ainsi, au lieu d'installer directement les autorités de certification racine dans le navigateur et de devoir gérer lui-même les alertes de sécurité, l'utilisateur choisit son tiers de confiance, à qui il délègue toutes ces vérifications pour une navigation entièrement transparente du point de vue de la sécurité.

La fonction de « notaire » peut être remplie par toute entité qui décide de se positionner sur ce domaine : fournisseur d'accès à Internet, fédération professionnelle, voire l'individu lui-même.

La fonction de sécurité est ainsi répartie entre un grand nombre d'acteurs, tout en ne reposant pas sur l'utilisateur final.

Le lecteur intéressé trouvera plus d'informations sur le site dédié au projet *http://convergence.io*.

Le modèle Sovereign Keys

Le modèle Sovereign Keys repose sur la publication dans une liste officielle, sur le modèle des DNS, des clés cryptographiques utilisées par les éditeurs de site web.

En cas de problème sur le certificat d'un site web, le comportement actuel des navigateurs consiste à afficher à l'internaute un message d'alerte,

Copyright © 2012 Eyrolles.

en général incompréhensible pour le grand public. La plupart du temps, ces alertes sont dues à des problèmes purement techniques ou organisationnels (certificat expiré, sous-domaine non pris en compte…), et le comportement de l'immense majorité des internautes est d'ignorer l'alerte et de continuer la navigation. De ce fait, lorsque l'alerte concerne un véritable problème de sécurité, elle est également ignorée.

À quoi servent des messages d'alerte que les utilisateurs ne comprennent pas ?

Un exemple récent consiste en une attaque *man in the middle* contre Facebook en Syrie, en mai 2011 : un serveur espion, ayant usurpé l'URL de Facebook, observait l'ensemble des flux entre les utilisateurs et le site légitime de Facebook avant de les retransmettre. Contrairement au cas décrit dans le paragraphe précédent sur Diginotar, les attaquants n'ont pas pris la peine de pirater une autorité de certification pour se procurer un vrai certificat et passer inaperçus : un faux certificat levant une vraie alerte a simplement été utilisé… et les utilisateurs ont ignoré l'alerte !

Dans le modèle Sovereign Keys, toutes les alertes de sécurité adressées aux utilisateurs sont supprimées, et le navigateur résout de lui-même les problèmes de sécurité, pour aboutir à une connexion au vrai serveur si celui-ci a déclaré sa « clé souveraine » dans le système, ou à un refus de la connexion si l'usurpation d'identité est avérée.

Le lecteur intéressé trouvera plus d'informations sur le site de l'Electronic Frontier Fundation : ***https://www.eff.org***.

Copyright © 2012 Eyrolles.

Copyright © 2012 Eyrolles.

Chapitre 6

La confidentialité

Qu'est-ce qui est confidentiel… et vis-à-vis de qui ?

La confidentialité peut être définie comme le maintien du secret relatif à des informations afin d'éviter une utilisation frauduleuse de celles-ci.

Il existe un besoin de confidentialité dès lors qu'il existe un « couple » constitué : d'une part, des données sensibles, et d'autre part, d'une personne potentiellement intéressée par l'accès à ces données.

On peut définir un très grand nombre de couples de ce type :

- un numéro de carte bancaire/toute personne susceptible d'acheter ;
- la réponse d'une entreprise à un marché public/un concurrent ;
- une base de données de clients/une entreprise de marketing ;
- un mot de passe d'accès aux e-mails/un conjoint jaloux…

Les données et les potentiels attaquants peuvent être de nature très différente, et les enjeux très variables d'un cas à l'autre : comment comparer les conséquences d'un conflit domestique avec la faillite potentielle d'une entreprise suite à la divulgation d'un secret industriel non encore breveté ?

C'est pourquoi il existe de nombreuses solutions, qu'il convient d'adapter au contexte spécifique du projet. Nous verrons ainsi que le chiffrement des données, s'il offre une forte garantie de confidentialité, n'est pas sans contraintes ni sans risques, alors que la gestion des droits d'accès, pour légère qu'elle soit en termes de sécurité pure, peut parfois être une mesure suffisante.

Avant de parcourir les différentes solutions techniques qui nous permettent de garantir la confidentialité au sein des projets de dématérialisation, nous allons aborder les contraintes spécifiques qui s'imposent en ce qui concerne les données à caractère personnel, au sens de la CNIL.

Copyright © 2012 Eyrolles.

Le cas particulier des données à caractère personnel

Lors de la conception de systèmes de traitement informatisé, il est impératif de prendre en compte la loi Informatique et libertés n° 78-17 du 6 janvier 1978, modifiée par la loi n° 2004-801 du 6 août 2004 relative à la protection des personnes physiques à l'égard des traitements de données à caractère personnel.

La CNIL définit une « donnée à caractère personnel » comme une information relative à une personne identifiée, ou qui permet d'identifier une personne directement ou indirectement. Cette définition très large inclut non seulement les éléments évidents (prénom, nom, date de naissance…) et les données biométriques (empreintes digitales, ADN…), mais plus largement les données indirectes que sont une adresse (postale, e-mail, téléphonique, IP…), l'identifiant d'un bien appartenant à la personne (numéro d'immatriculation d'un véhicule) ou des informations métier liées à la personne (services auxquels elle est inscrite, prestations dont elle bénéficie…).

Le traitement de données à caractère personnel est soumis à cinq grands principes :

- **la finalité :** le traitement prévu doit correspondre à une finalité légitime pour le responsable du traitement ;
- **la proportionnalité :** seules les données nécessaires au traitement doivent être collectées ;
- **la durée limite de conservation :** elle doit être définie en fonction de la finalité et les données doivent être détruites à l'issue de cette durée ;
- **la sécurité et la confidentialité :** le responsable du traitement doit prendre les mesures nécessaires pour éviter la divulgation des données ;
- **le respect des droits des personnes :** le responsable du traitement doit informer les personnes de la finalité du traitement, du caractère obligatoire ou facultatif de la fourniture de leurs informations personnelles, des personnes destinataires des informations et de leur droit d'accès et de rectification.

Le responsable du traitement est soumis à une obligation de déclaration à la CNIL des fichiers informatiques, préalablement au début du traitement.

Il existe bien entendu de nombreuses limitations, qu'il serait trop long d'énumérer ici, aux données que l'on peut collecter (numéro de Sécurité sociale, informations à caractère ethnique…) et aux usages qui peuvent en être faits (communication politique…).

Copyright © 2012 Eyrolles.

Il est important de garder en mémoire un type particulier de données à caractère personnel : les données de santé, qui sont également soumises à un ensemble de règles.

Les lois encadrant le traitement des données personnelles ont pour vocation de protéger les citoyens contre les abus potentiels rendus aisés par la puissance de l'outil informatique. Il est fondamental de les respecter afin de conserver l'humain au cœur de la dématérialisation, et de ne pas en faire un simple « instrument » aux mains d'outils techniques omniscients et tout-puissants !

Voyons maintenant de quels procédés techniques dispose le concepteur de services dématérialisés pour garantir le respect de la confidentialité.

Limiter l'accès aux données : la gestion des habilitations

Le procédé le plus répandu pour protéger des informations confidentielles gérées dans un service dématérialisé est la gestion des habilitations : même si la base de données ou le répertoire de stockage des fichiers contient l'ensemble des informations disponibles au sein du service, chaque utilisateur n'accède qu'à des « vues » restreintes aux informations qu'il est habilité à consulter.

Les droits des utilisateurs sont en général regroupés sous forme de « profils » correspondant chacun à un métier concret. Le profil sera ensuite conjugué, de manière applicative, avec l'entité d'appartenance de l'utilisateur, de manière à apporter un filtrage supplémentaire.

Illustrons cela par un exemple concret. La société ETSCAF, cabinet de conseil sur la sécurité en entreprise, a développé une méthode de prévention des accidents, et fournit à ses clients un logiciel permettant d'accompagner la mise en œuvre de la démarche sous la forme de « visites comportementales de sécurité » (VCS). Dans ce logiciel :

- un utilisateur qui a le profil « visiteur » peut programmer le calendrier de ses visites, en saisir les comptes-rendus et consulter ses propres statistiques et comptes-rendus ;
- un utilisateur qui a le profil « coordonnateur sécurité » peut consulter les statistiques et tous les comptes-rendus de visites de son site de rattachement (par exemple, une usine) ;
- un utilisateur qui a le profil « coordonnateur sécurité » et qui est rattaché au plus haut niveau de l'arborescence (le siège social) peut consulter les statistiques et tous les comptes-rendus de l'ensemble des usines de l'entreprise.

Copyright © 2012 Eyrolles.

Dans cet exemple, le filtrage n'est pas mis en œuvre à proprement parler à des fins de sécurité des informations, mais dans un but de confidentialité « de courtoisie » : chaque manager de service peut ne pas avoir envie que son collègue ait un accès direct à ses performances relatives à la mise en œuvre des VCS.

On retrouvera le même principe dans de très nombreux téléservices administratifs : les citoyens accèdent à leurs propres dossiers, et les agents de la collectivité publique à ceux qu'ils sont habilités à traiter.

Ce type de solution ne garantit aucunement la confidentialité des données vis-à-vis des administrateurs techniques du système d'information : l'exploitant de la base de données, sous réserve qu'il ait la connaissance métier de l'application, pourra consulter l'ensemble des informations présentes dans le système.

Cet élément est très important à prendre en compte, en particulier dans le cas des e-mails. La protection de la messagerie fonctionne sur ce principe de gestion des droits : chacun accède à son courrier électronique à l'aide de son mot de passe, et ne prend connaissance que des messages qui lui sont adressés.

Toutefois, l'administrateur du serveur de messagerie a potentiellement accès à l'ensemble des échanges de l'entreprise. Dès 1998, un grand groupe français a ainsi décidé du déploiement de certificats de chiffrement à l'ensemble de son état-major dans le but d'assurer la confidentialité des e-mails au cours d'une période de restructuration stratégique de l'entreprise, afin d'éviter les fuites des plans sociaux prévisionnels vers les syndicats au travers des services techniques.

Nous allons maintenant nous pencher vers cette deuxième solution technique employée pour la garantie de la confidentialité : le chiffrement.

Rendre les données inintelligibles : le chiffrement

Le chiffrement, souvent appelé improprement « cryptage » depuis la large publicité donnée à ce terme par une célèbre chaîne de télévision, consiste à rendre une donnée inintelligible à tous sauf à son destinataire légitime.

Nous ne referons pas ici un historique du chiffrement à travers les âges, des simples procédés de brouillage vieux de plusieurs millénaires aux méthodes cryptographiques modernes, en passant par les procédés de substitution popularisés par Blaise de Vigenère, puis par la machine Enigma dont le décodage a en partie décidé de l'issue de la Seconde Guerre mondiale. Il reste néanmoins important de noter que, depuis l'invention de l'écriture, pouvoir communiquer sans que l'information puisse

Copyright © 2012 Eyrolles.

être interceptée a été une préoccupation majeure de l'humanité, principalement à des fins militaires et économiques.

Nous avons vu au chapitre 2 à la section consacrée à la cryptographie deux types de chiffrement : symétrique et asymétrique. Nous allons maintenant voir plus en détail comment ces deux mécanismes sont employés conjointement, puis porter notre attention sur les précautions à prendre lorsque l'on met en œuvre le chiffrement de données.

Le chiffrement dans la pratique : un dispositif à deux étages

Au chapitre 2, nous avons détaillé deux mécanismes permettant de chiffrer des données :

- la cryptographie symétrique, qui utilise la même clé pour le chiffrement et le déchiffrement, et qui permet de traiter avec de bonnes performances des données volumineuses : l'algorithme phare de cette catégorie est AES ;
- la cryptographie asymétrique, qui utilise des clés différentes pour le chiffrement (clé publique) et le déchiffrement (clé privée), et qui ne permet de chiffrer que des données de taille restreinte, avec des performances limitées : l'algorithme phare de cette catégorie est RSA.

Nous allons voir comment ces deux mécanismes sont mis en œuvre pour le chiffrement et le déchiffrement des données.

Le chiffrement

Dans la pratique, le chiffrement emploie les deux techniques simultanément, comme l'illustre la figure 6-1.

1. L'émetteur de la donnée confidentielle génère une clé de chiffrement symétrique, sous la forme d'une suite aléatoire de bits.
2. L'émetteur chiffre les données confidentielles à l'aide de la cryptographie symétrique, en employant l'algorithme AES et la clé qu'il vient de générer.
3. L'émetteur se procure la clé publique du destinataire, en l'extrayant de son certificat : cela nécessite que, lors d'un échange préalable, ce certificat lui ait été transmis, ou qu'il ait pu le trouver dans un annuaire d'entreprise, par exemple.
4. L'émetteur chiffre la clé symétrique qu'il a générée lors de la première étape à l'aide de la cryptographie asymétrique, en employant l'algorithme RSA et la clé publique du destinataire.
5. La donnée chiffrée et la clé de déchiffrement elle-même chiffrée sont réunies dans une « enveloppe », que l'émetteur peut transmettre au destinataire.

Copyright © 2012 Eyrolles.

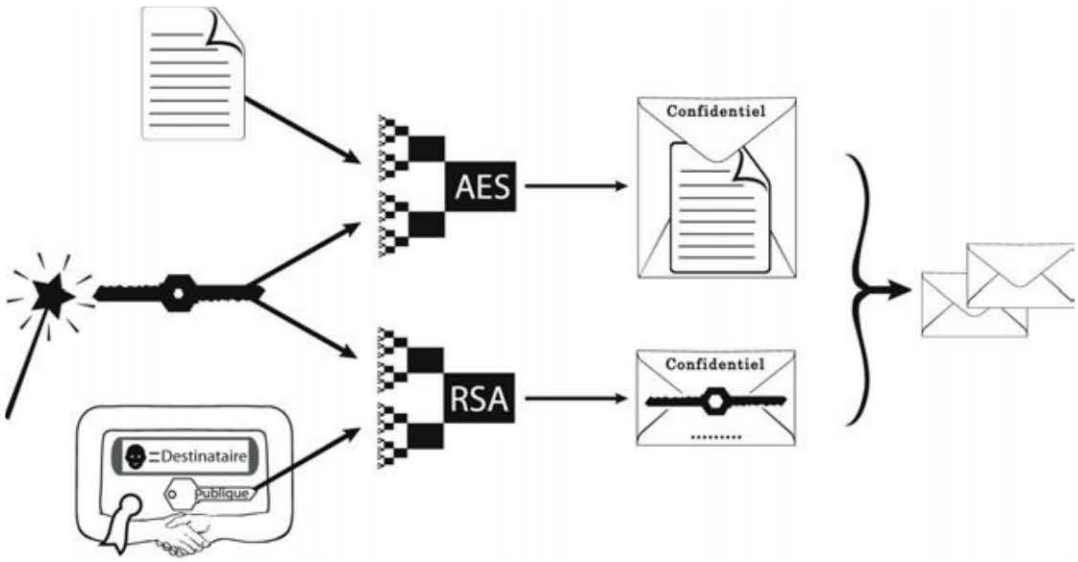


Figure 6-1 : Le chiffrement : un mécanisme à deux étages

La transmission de l'enveloppe chiffrée ne comporte aucun risque, même en cas d'interception. En effet, on ne peut déchiffrer la donnée confidentielle sans disposer de la clé symétrique, et pour accéder à cette dernière, qui a été chiffrée avec la clé publique du destinataire, il faut disposer de sa clé privée. Or, c'est le principe de la cryptographie asymétrique, la clé privée est sous le contrôle exclusif de son porteur.

Ainsi, l'utilisation successive des deux types de cryptographies permet :

- de résoudre le problème posé par la cryptographie symétrique : celui du partage de la clé secrète entre l'émetteur et le destinataire ;
- de résoudre le problème posé par la cryptographie asymétrique : la taille limitée des données que l'on peut chiffrer. En effet, ici, on ne chiffre qu'une clé, qui est de petite taille.

En outre, dans le cas où l'émetteur souhaite faire parvenir le même document à plusieurs destinataires, le mécanisme est très économique en ressources, puisque le chiffrement des données elles-mêmes peut être le même, seule la clé symétrique étant chiffrée plusieurs fois, avec la clé publique de chacun des destinataires.

Le format d'enveloppe chiffrée le plus répandu est CMS, aussi appelé PKCS#7, et repris dans la norme RFC 2630. C'est ce format qui est employé dans la norme de courrier électronique sécurisé S/MIME.

Le déchiffrement

Le déchiffrement comporte les étapes inverses du chiffrement, comme l'illustre la figure 6-2.

Copyright © 2012 Eyrolles.

1. Le destinataire reçoit l'enveloppe chiffrée ; il en extrait la clé chiffrée et les données chiffrées.
2. Le destinataire déchiffre la clé symétrique à l'aide de la cryptographie asymétrique, en employant l'algorithme RSA et sa propre clé privée.
3. Le destinataire déchiffre les données à l'aide de la cryptographie symétrique, en employant l'algorithme AES et la clé symétrique qu'il vient de déchiffrer. Il a alors accès aux données en clair.

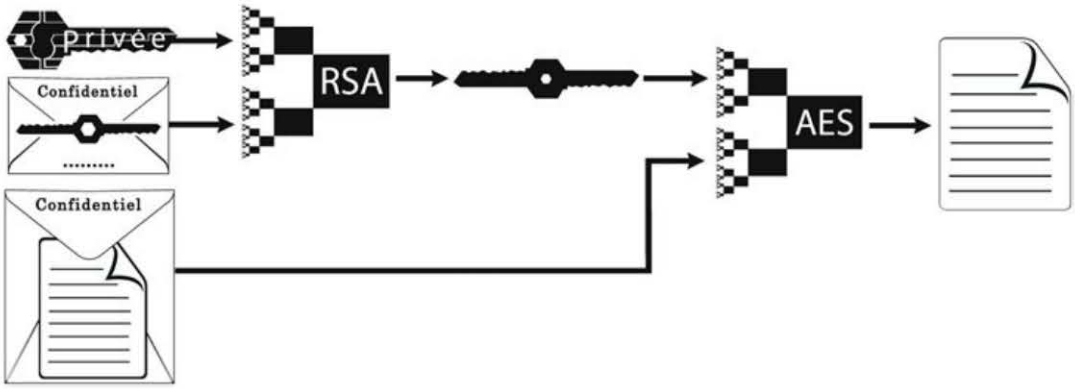


Figure 6-2 : Le déchiffrement

Nous allons maintenant voir quelques exemples de mise en œuvre du chiffrement dans des contextes concrets.

Quelques exemples de mise en œuvre du chiffrement

La dématérialisation des marchés publics

Dans la dématérialisation des marchés publics, la confidentialité des candidatures et des offres des entreprises doit impérativement être garantie, aussi bien vis-à-vis des concurrents que de l'opérateur de la plate-forme de dématérialisation, et même de la personne publique qui passe le marché, jusqu'à la date de la séance officielle d'ouverture des plis.

Dans ce but, l'opérateur de service de dématérialisation Achatpublic.com a mis en œuvre une solution de chiffrement extrêmement robuste.

1. Pour chaque personne publique, un certificat de chiffrement est généré et inséré dans la base de données de la plate-forme. La clé privée correspondante est générée et séquestrée par un tiers de confiance, qui l'achemine directement à la personne publique, sans que cette clé privée soit jamais connue d'Achatpublic.com. De cette manière, la confidentialité est assurée vis-à-vis de l'opérateur.
2. Lorsque l'entreprise soumissionnaire souhaite déposer son pli, chacune de ses enveloppes (candidature et offre pour chaque lot) est chiffrée

Copyright © 2012 Eyrolles.

sur son poste avec une clé symétrique générée aléatoirement. Chacune de ces clés symétriques est ensuite chiffrée à l'aide de la clé publique du pouvoir adjudicateur, puis l'ensemble (enveloppes chiffrées et clé de déchiffrement elles-mêmes chiffrées) est alors envoyé sur la plate-forme. De cette manière, la confidentialité est garantie contre toute interception lors du dépôt, les documents n'ont existé en clair que sur le poste du soumissionnaire.

3. Une fois la salle des marchés fermée, l'acheteur peut librement télécharger les plis chiffrés ; puis le téléchargement des clés de déchiffrement donne lieu à une traçabilité forte garantissant quelles enveloppes ont été ouvertes ou non. Ainsi, si une entreprise est rejetée au niveau de la candidature, il est possible de prouver que son offre n'a pas été déchiffrée : la confidentialité est garantie vis-à-vis du pouvoir adjudicateur lui-même.

Le vote par Internet

Certaines opérations électorales requièrent une confidentialité absolue du vote, au moment de son expression, pendant la conservation du bulletin dans l'urne, au moment du dépouillement, et *a posteriori* sans limite dans le temps ; sans quoi la sincérité du scrutin ne pourrait pas être assurée.

C'est pourquoi la CNIL exige cette garantie dans le vote par Internet, sous la forme de plusieurs mesures complémentaires dont nous citons l'essentiel ci-dessous.

CNIL – Délibération n° 2010-371 du 21 octobre 2010 portant adoption d'une recommandation relative à la sécurité des systèmes de vote électronique

I.2. La séparation des données nominatives des électeurs et des votes

Le dispositif doit garantir que l'identité de l'électeur ne peut pas être mise en relation avec l'expression de son vote, et cela à tout moment du processus de vote, y compris après le dépouillement. [...]

II.1.5. Les clés de chiffrement

La génération des clés destinées à permettre le déchiffrement des bulletins de vote doit être publique et se dérouler avant l'ouverture du scrutin. Cette procédure doit être conçue de manière à prouver de façon irréfutable que seuls le président du bureau et ses assesseurs prennent connaissance de ces clés, à l'exclusion de toute autre personne y compris les personnels techniques chargés du déploiement du système de vote. La Commission estime que le nombre de clés de chiffrement doit être au minimum de trois, la combinaison d'au moins deux de ces clés étant indispensable pour permettre le dépouillement.

Copyright © 2012 Eyrolles.

II.2.2. Le chiffrement du bulletin de vote

Le bulletin de vote doit être chiffré par un algorithme public réputé « fort » dès son émission sur le poste de l'électeur et être stocké dans l'urne, en vue du dépouillement, sans avoir été déchiffré à aucun moment, même de manière transitoire. La liaison entre le terminal de vote de l'électeur et le serveur des votes doit faire l'objet d'un chiffrement distinct de celui qui s'applique au bulletin pour assurer la sécurité tant du procédé d'authentification de l'électeur que la confidentialité de son vote. La mise en place du canal de communication doit intégrer une authentification du serveur de vote.

Par ailleurs, le stockage du bulletin dans l'urne ne doit pas comporter d'horodatage, pour éviter tout rapprochement avec la liste d'émargement.

Ce qui est spécifique au cas du vote électronique, c'est que la confidentialité porte sur :

- le bulletin, avant le dépouillement du scrutin ;
- le lien entre le bulletin et l'identité de l'électeur, une fois le dépouillement réalisé.

Les mesures prises pour garantir cette double exigence sont de diverses natures :

- le bulletin doit être chiffré de manière ininterrompue entre son émission sur le poste de l'électeur et son dépouillement lors d'une séance publique ;
- le bulletin chiffré doit être transmis dans un canal lui-même sécurisé (*via* le protocole SSL) ;
- le stockage du bulletin chiffré et de l'émargement doit être réalisé de manière séparée ;
- si l'émargement doit être horodaté, le dépôt du bulletin chiffré dans l'urne électronique, quant à lui, ne doit pas l'être.

Il existe diverses solutions techniques qui permettent de répondre aux exigences de la CNIL en termes de confidentialité du vote. Certaines utilisent des algorithmes cryptographiques élaborés (par exemple, ElGamal), d'autres font précéder le dépouillement (c'est-à-dire le déchiffrement des bulletins) d'un ou plusieurs « mélanges » garantissant qu'aucun lien ne puisse être reconstitué entre le bulletin chiffré et le bulletin en clair.

On notera la recommandation de scinder la clé de déchiffrement des bulletins en fragments, dont au moins deux sont nécessaires au dépouillement. Cette mesure permet d'assurer deux fonctions de sécurité. D'une part, elle évite la perte des données en cas de perte de sa clé par un membre du bureau de vote et d'autre part, elle force la mise en œuvre du « principe des quatre yeux » : il faut au moins la présence de deux personnes pour pouvoir procéder au dépouillement.

Copyright © 2012 Eyrolles.

Par ailleurs, il est nécessaire de conserver pendant toute la durée de recours contentieux l'ensemble des éléments permettant de rejouer le dépouillement et le décompte des bulletins : des mesures organisationnelles de partage des secrets et de stockage des éléments confidentiels au coffre viennent compléter cet arsenal technique.

Enfin, le dispositif de sécurisation mis en place par la CNIL ne serait pas complet s'il ne s'appuyait sur une exigence d'audit systématique par un expert indépendant de la solution technique et des procédures mises en œuvre dans chaque scrutin : revue du code source de la solution, scellement du code source et du code exécutable, confidentialité de l'acheminement des identifiants et mots de passe permettant aux électeurs de voter, audit des conditions d'exploitation de la solution, de génération et de conservation des secrets, audit des traces applicatives et des logs techniques, dont l'intégrité doit être garantie…

On peut aujourd'hui dire qu'il est possible de garantir la sécurité d'un scrutin réalisé par Internet, à condition de mettre en œuvre l'ensemble des moyens nécessaires !

Attention : chiffrer des données nécessite quelques précautions !

Nous avons vu dans les exemples de la dématérialisation des marchés publics et du vote électronique que le chiffrement n'est pas toujours suffisant pour garantir la confidentialité des données, et qu'il doit, pour être efficace, s'accompagner de mesures organisationnelles (appel à un tiers de confiance, cérémonies de génération des clés) et d'une traçabilité fiable.

Nous allons maintenant mettre en lumière trois risques qu'il faut impérativement prendre en compte lors de la mise en œuvre du chiffrement dans un projet de dématérialisation : la traçabilité portant sur les données confidentielles, le risque de perte de données et les risques liés à la génération des clés.

La porte est bien verrouillée… mais y a-t-il des fenêtres ?

Nous verrons dans la partie 4 dédiée à la traçabilité le rôle essentiel que tient dans un projet de dématérialisation la conservation de l'historique des événements qui se sont déroulés sur la plate-forme.

Ainsi, de nombreuses données vont être amenées à figurer dans les traces applicatives ou dans les logs techniques, à des fins de traitement métier ou de reconstitution des actions.

Dès lors, la question se pose : a-t-on bien chiffré les données sensibles partout où elles sont présentes ? Il faut être extrêmement attentif, lors de la constitution d'un système portant de fortes contraintes de confidentialité, aux éléments que l'on peut faire figurer ou non dans les traces.

Rien ne sert de chiffrer des données si on peut les retrouver en clair dans les traces de l'application ou dans des index de recherche !

Copyright © 2012 Eyrolles.

Ainsi, dans le vote électronique, il est fondamental de pouvoir tracer qui a voté ou non – et il est tout aussi essentiel de ne pas pouvoir tracer pour qui un individu a voté ! Supposons, par exemple, que le choix du candidat se fasse sur la plate-forme, puis que le poste de l'électeur ne prenne la main que pour la constitution du bulletin chiffré correspondant : en traçant le contenu de la page de sélection, il serait possible de lever l'anonymat du vote malgré la précaution de chiffrement du bulletin ! Il est donc préférable que l'ensemble du processus de choix se fasse sur le poste de l'électeur (par exemple, en JavaScript ou dans une applet Java), et indispensable de vérifier que le code correspondant ne laisse aucune trace ni sur le serveur, ni sur le poste de l'électeur.

Un autre piège pour le concepteur repose dans l'inclusion d'un moteur de recherche au sein d'une application web permettant, par exemple, à un utilisateur de rechercher des informations parmi des données personnelles lui appartenant : même si les accès sont contrôlés par la gestion des habilitations, il faut, pour que le moteur de recherche soit fonctionnel, qu'il puisse rechercher parmi des données indexées… en clair ! Ainsi, si les données confidentielles sont chiffrées dans la base de données de référence, il peut arriver qu'elles soient en clair dans un fichier d'indexation – ce qui est bien évidemment à proscrire.

Et si l'on perd la clé… y a-t-il un serrurier ?

Chiffrer des données, c'est les rendre incompréhensibles à tous, sauf à leur destinataire légitime, qui dispose d'une clé, sous son contrôle exclusif, pour les déchiffrer. Mais si le destinataire perd sa clé, il deviendra impossible d'accéder à nouveau aux données chiffrées.

Prenons le cas de la dématérialisation des marchés publics : si la personne publique perd sa clé de déchiffrement, les offres des candidats ne pourront pas être examinées, et il faudra procéder à une nouvelle passation du marché, ce qui peut faire perdre plusieurs mois et entraîner une rupture d'approvisionnement. C'est pour cette raison que, dans l'exemple que nous avons pris, les clés de déchiffrement sont séquestrées par le tiers de confiance qui les a émises, et peuvent être fournies à nouveau à leur titulaire (et seulement à lui !), selon une procédure documentée et tracée.

Dans notre exemple du vote par Internet, de même, si la clé permettant de déchiffrer le contenu de l'urne était perdue, il faudrait procéder à une nouvelle élection, avec toutes les conséquences imaginables en termes de coûts et de délais. La solution préconisée par la CNIL consiste à scinder la clé en un certain nombre de fragments, dont une sous-partie définie devra être assemblée pour la reconstitution. Ainsi, on pourra générer trois fragments dont deux seront nécessaires au déchiffrement. En cas de perte d'un fragment ou d'absence d'un membre du bureau de vote, le dépouillement demeurera ainsi possible.

Copyright © 2012 Eyrolles.

Le risque de divulgation des données confidentielles doit être mis en balance avec le risque d'indisponibilité en cas de perte de la clé de déchiffrement.

Lors de l'étude de sécurité, avant de prendre la décision de mettre en œuvre le chiffrement, le risque de divulgation des données confidentielles devra être mis en balance avec le risque de perte de ces mêmes données. Il faudra systématiquement envisager un mécanisme de secours, sous la forme de séquestre des clés, de séquestre des données en clair dans un environnement hors-ligne sécurisé, ou de partage des secrets avec une redondance garantissant une sécurité suffisante.

Et si ma clé était un passe-partout ?

Le chiffrement utilise deux éléments complémentaires : les algorithmes (symétrique : AES, asymétrique : RSA), et les clés qu'ils utilisent.

Ainsi, la robustesse du chiffrement dépendra d'une part de la qualité de l'algorithme et d'autre part, de la qualité du générateur de clés.

Si les clés asymétriques sont en général générées dans des conditions sécurisées lors de l'émission du certificat, en revanche, les clés symétriques de chiffrement sont générées de manière aléatoire à chaque fois qu'un chiffrement est nécessaire.

Ainsi, même avec un algorithme de chiffrement « fort » (comme AES) et une taille de clé importante (par exemple, 128 bits), le chiffrement sera illusoire si la clé employée comporte systématiquement 120 bits dont la valeur aurait été fixée de manière déterministe par le fournisseur du module de génération de clés.

Il est donc fondamental de pouvoir faire confiance à l'éditeur des briques techniques employées pour la sécurité : soit qu'il soit totalement indépendant des enjeux liés à la confidentialité des données, soit que le code source du générateur d'aléas ait été audité par un expert en cryptographie.

Ainsi, lorsque le logiciel Applatoo, édité par France Télécom, a été audité par l'ANSSI en vue de sa qualification au niveau de sécurité EAL2+, il a été demandé de renforcer cet élément, le logiciel open source qui avait été employé initialement n'ayant pas été jugé suffisamment robuste. Cet exemple montre tout l'apport d'une labellisation officielle des outils de sécurité informatique.

Voyons maintenant quels procédés sont disponibles, au-delà du chiffrement, pour la transmission des secrets utiles aux applications dématérialisées.

Transmettre des secrets

Nous avons vu qu'il est aisé de transmettre des données confidentielles lorsque tous les destinataires disposent d'un certificat de chiffrement. Dans la pratique, ce n'est pas applicable aux contextes dans lesquels

Copyright © 2012 Eyrolles.

les destinataires ne sont pas une communauté restreinte et connue, par exemple pour les applications « grand public ».

Le cas le plus répandu où le besoin de transmettre des secrets se présente est l'envoi de codes d'accès à une application. Reprenons l'exemple du vote par Internet. Il est nécessaire que l'organisateur du scrutin fasse parvenir à chaque électeur un identifiant (de préférence anonyme) et un mot de passe lui permettant d'exprimer son vote.

En l'absence d'un canal de transmission sécurisé, il est nécessaire de scinder le secret en deux parties interdépendantes, et d'acheminer chacune de ces parties par un canal différent.

On pourra ainsi, par exemple, transmettre l'identifiant par courrier postal et le mot de passe par SMS ou par e-mail, les deux éléments étant nécessaires pour accéder au service (ici, pour voter).

Ce mécanisme peut être renforcé par l'usage d'un « défi » supplémentaire : au lieu d'envoyer directement le mot de passe, le service envoie à l'utilisateur un lien à usage unique permettant d'afficher le mot de passe à l'écran après avoir saisi l'identifiant (transmis par un canal papier) et la réponse à une question personnelle connue du système : date de naissance, lieu de naissance, matricule, revenu fiscal de référence… Le choix de cette question complémentaire dépend bien entendu des données disponibles dans la base de données de référence.

Ce service de remise du secret contre réponse à un défi peut avantageusement être confié à un tiers de confiance, qui garantira la confidentialité des secrets, la remise uniquement aux demandeurs légitimes et la traçabilité de l'ensemble des opérations.

Une fois les secrets générés et transmis à leurs utilisateurs légitimes, il convient que chacun d'entre eux puisse les conserver et les utiliser de manière sécurisée.

Conserver et utiliser des secrets

Il existe deux cas principaux d'utilisation de secrets dans les applications dématérialisées :

- les mots de passe des utilisateurs, utilisés pour les authentifier ;
- les clés et les mots de passe à usage du système lui-même, employés automatiquement.

Protéger les mots de passe des utilisateurs

L'authentification d'un utilisateur par mot de passe consiste à comparer la chaîne de caractères qu'il a saisie et transmise à celle qui est conservée dans l'annuaire ou la base de données du service. Or, la conservation du

Copyright © 2012 Eyrolles.

mot de passe dans la base de données constitue un risque important : d'une part, les mots de passe sont ainsi accessibles aux administrateurs système, et d'autre part, en cas de piratage, leur divulgation peut donner au pirate la possibilité d'usurper l'identité de l'ensemble des utilisateurs. Cette façon de faire n'est pas compatible avec la nécessité de responsabiliser l'utilisateur vis-à-vis de ses actions sur la plate-forme en le rendant pleinement responsable de la gestion de son mot de passe, puisqu'il pourra toujours arguer que le secret n'était pas sous son contrôle exclusif.

C'est pourquoi il est recommandé de ne conserver sur la plate-forme qu'un hash du mot de passe de l'utilisateur. En effet, la connaissance du hash ne permet pas de reconstituer le mot de passe lui-même. Ainsi, pirater ou copier la base des hash de mots de passe ne permettra pas d'usurper l'identité des utilisateurs. En revanche, la connaissance d'un hash est suffisante pour vérifier la présentation du mot de passe : il suffit de calculer le hash du mot de passe présenté et de le comparer à celui qui est conservé pour avoir la certitude que le bon mot de passe a été saisi.

Bien entendu, l'utilisation de mots de passe n'offrira jamais le niveau de sécurité d'un procédé d'authentification forte (mot de passe dynamique à usage unique ou certificat)… Mais le coût de la mise en œuvre en est bien moindre, ainsi que la technicité de l'utilisation.

Protéger les clés et les mots de passe du système

Les services dématérialisés ont souvent besoin de gérer en interne des secrets, qui servent à l'établissement de sessions sécurisées, au déchiffrement de données, à la réalisation de cachets ou d'horodatages, etc.

Une éventuelle fuite de ces secrets peut se révéler catastrophique pour le système, car ils sont en général les piliers de la sécurité du système. Il est donc insuffisant de les conserver sur le serveur sous forme de fichiers de configuration. Il existe plusieurs façons de les protéger.

Tout d'abord, il est possible de faire saisir un mot de passe au démarrage du système par un administrateur qui en a la responsabilité, puis de ne conserver ce mot de passe qu'en mémoire vive, sans jamais l'écrire dans l'espace de stockage du serveur. Ce mot de passe pourra, par exemple, servir à déchiffrer une clé privée stockée sous la forme d'un fichier PKCS#12 comme nous l'avons vu dans le chapitre 5 sur les certificats. Cette façon de procéder offre un bon niveau de sécurité, mais nécessite la présence d'un administrateur humain en cas de redémarrage du service, et engendre donc soit un risque d'indisponibilité du service, soit des coûts humains pour garantir en permanence la présence d'un personnel habilité.

Il est ensuite possible de partager le secret entre les fichiers de configuration et le code exécutable de l'application : par exemple, le mot de passe est stocké chiffré dans un fichier, et la clé de déchiffrement est « en dur »

Copyright © 2012 Eyrolles.

dans le service. Il est alors important de garantir l'impossibilité d'analyser le code exécutable pour en extraire le secret. C'est le rôle du mécanisme de protection appelé l'« obfuscation ».

On peut encore recourir à un matériel cryptographique ou HSM, mais cela ne fait que repousser le problème, car il faut également sécuriser l'accès au HSM, et donc là encore gérer un secret. En revanche, l'usage d'un HSM garantit que les clés qu'il contient n'en seront jamais extraites, ce qui n'est pas le cas si l'on se contente de les stocker sous forme logicielle.

Enfin, en dernier recours, la sécurité des secrets de l'application reposera sur les mécanismes de sécurité technique (pare-feu, détection d'intrusion, contrôle d'accès physique et logique…) et organisationnelle (procédures, habilitations, partage des responsabilités…) mis en œuvre.

Pour conclure sur le sujet de la confidentialité, voyons comment rompre le lien entre certaines données sensibles et les personnes concernées grâce à l'anonymisation.

Rompre le lien entre les personnes et les données : l'anonymisation

Nous avons vu dans l'exemple relatif au vote par Internet que ce ne sont pas toujours les données qui sont confidentielles, mais parfois leur lien avec une personne identifiée.

Il en va ainsi, par exemple, de données médicales que l'on souhaiterait utiliser en vue d'établissement de statistiques. Il est important de pouvoir compter les cas de contamination d'une maladie virale, mesurer l'efficacité des traitements proposés aux patients, mettre la progression de la maladie en relation avec les conditions de vie des patients, leur milieu socio-culturel, leur consommation de tabac, d'alcool, de drogues, leurs antécédents familiaux, la fréquence de leurs déplacements…

Dans des études de ce type, il est important de savoir que des données différentes se rapportent au même patient. Mais il est également primordial, pour respecter les droits fondamentaux de ce patient, de ne jamais révéler son identité en dehors du cercle du personnel soignant qui le prend en charge.

On procédera alors à l'anonymisation des données : l'identité de la personne sera remplacée par un identifiant systématique, mais sans lien avec les données à caractère personnel permettant de reconstituer la relation.

Dans d'autres cas, il sera possible de faire appel à un pseudonyme, qui garantira l'anonymat de la personne mais permettra de reconstituer le lien en cas de besoin. Cela pourra être le cas, par exemple, dans un système de

Copyright © 2012 Eyrolles.

traçabilité où l'identifiant d'un utilisateur sera remplacé par une référence conservée dans son compte de manière confidentielle (soit chiffrée, soit soumise à un contrôle d'accès).

Les fonctions de hash sont des outils pratiques pour procéder à l'anonymisation. Il faut cependant rester prudent lorsqu'on les emploie, car si l'algorithme de calcul des « identifiants anonymes » est connu, il sera possible de reconstituer les liens entre la liste des personnes concernées et la liste de leurs identifiants en faisant un calcul exhaustif des identifiants possibles à partir de la liste des utilisateurs.

Copyright © 2012 Eyrolles.

PARTIE 3

La signature électronique



Copyright © 2012 Eyrolles.

Copyright © 2012 Eyrolles.

Chapitre 7

La signature électronique en pratique

Signature manuscrite et signature électronique : deux actes très ressemblants

L'acte de signature est une expérience que nous faisons tous, sinon quotidiennement, du moins régulièrement : lorsque nous payons par chèque, lorsque nous concluons un contrat, lorsque nous rédigeons un courrier, lorsque nous remplissons un formulaire de demande, lorsque nous validons une décision professionnelle, lorsque nous retirons un recommandé au guichet de La Poste…

La signature existe depuis la nuit des temps, comme en témoignent les cartouches des pharaons sur les bâtiments d'Égypte, les sceaux-cylindres de la Mésopotamie, les sceaux montés sur bagues des anciens Romains, et leur successeur, les chevalières des Nobles de l'Ancien Régime.

Marque d'autorité, de propriété, de revendication ou d'engagement, la signature a toujours eu pour but :

- pour le signataire, de se déclarer l'auteur ou d'accepter le contenu d'un document ;
- pour le lecteur du document, d'identifier sa provenance et de vérifier sa valeur juridique.

La réalisation d'une signature nécessite quatre éléments :

- **un individu**, le signataire, qui peut agir en son nom propre ou au nom d'une entité qu'il représente ;
- **un document** à signer, qui peut être de natures diverses tant pour le fond (contrat, lettre, formulaire…) que pour la forme (papyrus, parchemin, simple papier, papier sécurisé, formulaire CERFA…) ;
- **un instrument d'écriture** (stylet, plume, stylo…) ;

Copyright © 2012 Eyrolles.

- **un geste**, que le signataire est le seul à savoir réaliser avec l'instrument d'écriture : la signature à proprement parler.

Dans le cas particulier d'un cachet de cire, la cire est l'instrument d'écriture, et le geste « secret » repose dans l'apposition de la bague que le signataire est le seul à posséder.

La signature électronique est un cas particulier de signature, qui porte sur un document de nature électronique et non physique.

La réalisation de la signature électronique nécessite quatre éléments, dans un parallèle quasiment parfait avec la signature manuscrite, comme l'illustre la figure 7-1 :

1. **un individu**, le signataire, qui peut agir en son nom propre ou au nom d'une entité qu'il représente, muni d'un terminal informatique pour réaliser l'opération de signature ;
2. **un document** à signer, qui peut être de natures diverses tant pour le fond (contrat, lettre, formulaire…) que pour la forme (document issu d'un traitement de texte, fichier PDF, fichier image, données informatiques au format XML, CSV ou autres…) ;
3. **un instrument de signature** (la carte à puce, la clé USB ou le magasin logiciel support du certificat) ;
4. **un secret**, que le signataire est le seul à connaître : le code de déblocage de sa clé privée sur le support du certificat, appelé en général « code PIN » (*Personal Identification Number*) : c'est l'équivalent du code de la carte bancaire.

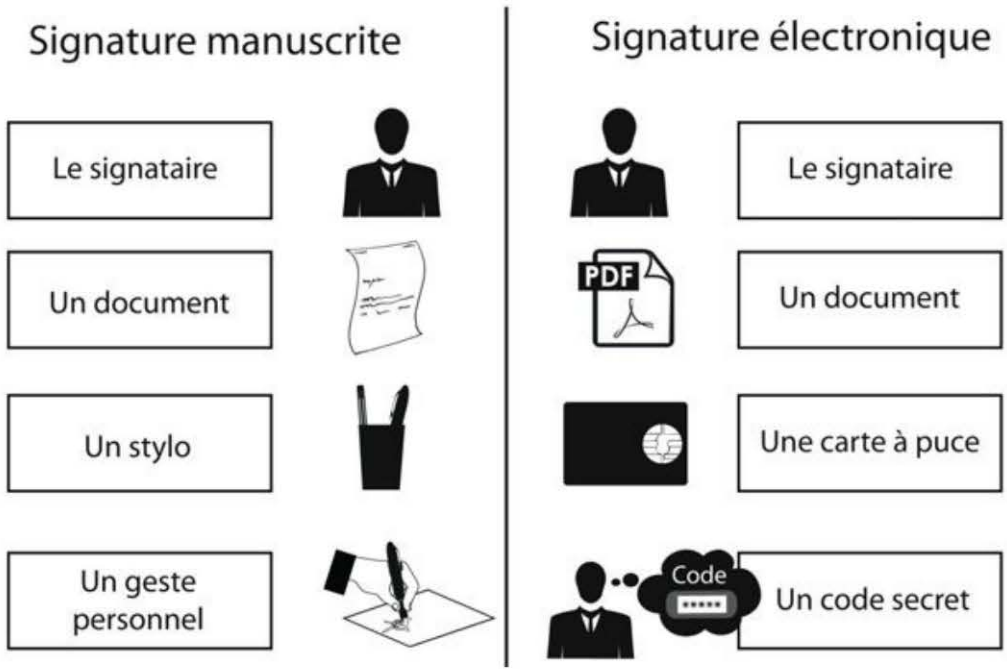


Figure 7-1 : Le parallèle entre les signatures manuscrite et électronique

Copyright © 2012 Eyrolles.

Nous verrons plus loin qu'il existe de nombreuses façons de réaliser la signature électronique dans la pratique, mais le parallèle établi ci-dessus reste valide, l'essentiel étant que le signataire dispose d'un **moyen cryptographique** permettant de réaliser techniquement la signature (point 3), et d'un **moyen d'authentification** permettant de déclencher l'usage de ce moyen cryptographique (point 4).

Pour poursuivre le parallèle, précisons que la signature manuscrite consiste en un signe graphique que le signataire est (en théorie) le seul à savoir faire, et que l'on peut vérifier en le comparant à un modèle conservé par la banque ou par les autorités publiques (image sur la carte d'identité), alors que la signature électronique consiste en un calcul mathématique qui ne peut être réalisé que grâce au moyen cryptographique conservé sous le contrôle du signataire, et que l'on peut vérifier grâce à une donnée informatique (le certificat), émise et rendue infalsifiable par un prestataire de services de certification électronique.

Enfin, de même que la signature manuscrite est indissociable du document signé (l'encre marque le papier), la signature électronique est liée au document signé par le fait que le calcul mathématique effectué prend en entrée des données provenant de ce document (une empreinte, ou hash, qui dépend de l'ensemble des bits du document).

La pratique de la signature est ainsi très proche dans les domaines manuscrit et électronique. Il faut toutefois noter quelques différences fondamentales.

Signature manuscrite et signature électronique : quelques différences pratiques

Du point de vue de l'usage, deux différences fondamentales sont à souligner entre les deux types de signatures.

Tout d'abord, une signature manuscrite est directement visible sur le document, sous la forme d'un signe graphique, souvent apposé près du nom du signataire. En revanche, la signature électronique, de par sa nature cryptographique, n'est pas directement visible et compréhensible par l'humain. Elle nécessite une interface de visualisation et de vérification, qui en affichera la provenance et la validité. Certains formats de signature ne seront vérifiables que dans un outil dédié à cet usage, indépendamment de l'interface habituelle de visualisation du document : par exemple, une signature électronique apposée sur un document Word (antérieur à Microsoft Office 2010) sera un fichier à part, qui ne se visualisera pas dans Word mais avec un outil de vérification de signature. D'autres formats permettent une visualisation plus proche des habitudes, comme le format PDF,

Copyright © 2012 Eyrolles.

dans lequel la signature peut être visualisée directement sous une forme graphique avec le logiciel Adobe Reader, qui sert aussi à lire le document.

La seconde différence concerne la nécessité de vérifier une signature électronique. La théorie voudrait que l'on vérifie une signature manuscrite avant de lui accorder sa confiance. Toutefois, dans la pratique, hormis le caissier du supermarché ou le banquier pour les retraits de grosses sommes d'argent au guichet, les signatures manuscrites sont rarement contrôlées.

Les signatures électroniques, en revanche, sont systématiquement vérifiées : quel sens cela aurait-il de juste vérifier qu'il y a bien un fichier portant l'extension d'une signature, sans vérifier si ce fichier est bien une signature, par qui elle a été apposée et si elle porte bien sur le bon document ?

La signature étant une marque d'engagement qui confère une valeur juridique au document sur lequel elle est apposée, il importe de bien comprendre le cadre juridique qui s'applique à la signature électronique.

Comprendre le cadre juridique : un passage obligé

La mise en œuvre de la signature électronique dans un projet répond nécessairement à un besoin juridique. Dans le cas inverse, il faudrait, en amont, s'interroger sur l'utilité de la mise en œuvre de la signature !

Le vocabulaire lié à la signature électronique a une double origine : technique, depuis l'invention de l'algorithme RSA en 1976, et juridique, depuis la promulgation de la directive 1999/93/CE du Parlement européen et du Conseil, du 13 décembre 1999, sur un cadre communautaire pour les signatures électroniques. Il est fondamental d'employer les mots et les notions dans leur sens le plus précis, lors de l'expression du besoin, de la mise en œuvre et de la communication vers le grand public. L'approche juridique va nous y aider.

Dans ce chapitre, nous détaillerons tout d'abord le droit français de la signature électronique, puis nous aborderons les différences qui existent entre la directive européenne de 1999 et sa transposition dans notre pays.

En France, la loi n° 2000-230 du 13 mars 2000 portant adaptation du droit de la preuve aux technologies de l'information et relative à la signature électronique, a défini dans l'article 1316-4 du Code civil le cadre juridique applicable pour la signature électronique.

Le décret du 30 mars 2001 a ensuite approfondi la notion de signature électronique en développant les notions de « signature électronique sécurisée » et de « signature électronique présumée fiable ».

Copyright © 2012 Eyrolles.

L'article 1316-4 du Code civil : la définition de la signature électronique

Nous avons déjà évoqué, dans le chapitre 1 sur la dématérialisation, les articles précédents du Code civil, qui fixent le cadre général de la dématérialisation, mais n'abordent pas le sujet de la signature.

Cette notion est introduite par le célèbre article 1316-4, dont nous détaillons les deux alinéas ci-dessous.

Code civil – Article 1316-4 (1er alinéa)

La signature nécessaire à la perfection d'un acte juridique identifie celui qui l'appose. Elle manifeste le consentement des parties aux obligations qui découlent de cet acte. Quand elle est apposée par un officier public, elle confère l'authenticité à l'acte.

Deux choses fondamentales sont à remarquer.

Tout d'abord, cet alinéa ne porte pas sur la signature électronique, mais sur la signature en général, qu'elle soit manuscrite ou électronique. Aucune distinction n'est faite entre les deux cas.

Ensuite, il s'agit de la première définition de la signature dans le droit français. Auparavant, la signature était un usage lié à l'habitude, à la tradition, mais ne faisait pas l'objet d'une description précise.

À quoi sert la signature ?

Elle sert à la perfection d'actes juridiques. À défaut de signature, le document ne sera pas dénué de valeur juridique, mais il ne constituera qu'un « *commencement de preuve* ».

En quoi consiste la signature ?

Elle consiste en une identification du signataire. Pour faire le parallèle avec la définition pratique établie précédemment, cette identification certaine du signataire reposera sur l'existence d'un « secret » détenu par le seul signataire : sa capacité à former le signe manuscrit qui constitue sa signature sur papier, ou l'élément cryptographique secret qui lui sert à faire un calcul dans le cas de la signature électronique.

Qu'emporte la signature ?

La signature emporte le consentement du signataire aux termes du document signé.

Cet élément de définition n'est pas neutre. En effet, nous verrons plus loin que la signature électronique offre, outre ses propriétés juridiques, des propriétés fonctionnelles intéressantes : elle permet de garantir la provenance et l'intégrité du document. On peut donc être tenté, dans un processus dématérialisé, de généraliser l'usage de la signature électronique

Copyright © 2012 Eyrolles.

pour ses propriétés de sécurité informatique. Mais ce faisant, on risque de se trouver face à un effet indésirable : donner une valeur juridique à un document qui ne le nécessite pas.

Ainsi, si dans le processus de constitution et d'échanges de versions de travail d'un document, on prend l'habitude de signer systématiquement chaque version transmise pour garantir à son destinataire la provenance et l'intégrité, on court le risque de marquer son consentement sur une version temporaire qui ne reflète pas les intentions réelles du signataire. Peut-on imaginer un ministre signant une version non définitive d'un texte de loi ? Quelle serait la valeur de ce document ?

Il en va de même d'un candidat à un marché public qui, au lieu de signer uniquement son acte d'engagement, signerait l'ensemble des documents inclus dans son offre : s'il joint à son pli une plaquette commerciale, il se trouvera lié par ce document, qui n'était en principe joint qu'à titre informatif. Si ce document décrit des performances du produit supérieures à celles auxquelles il s'engage dans son offre, quelles performances l'acheteur sera-t-il en droit de réclamer ? Le fournisseur court le risque d'être obligé de respecter les termes de sa plaquette commerciale, moins avantageux pour lui que ceux de son mémoire technique !

Ainsi, il faut faire attention à signer tous les documents que l'on *doit* signer, mais *seulement ceux-là*.

Le cas particulier des officiers publics

L'établissement d'un acte authentique découle de la signature d'un officier public (par exemple, un notaire ou un huissier de justice). La loi du 13 mars 2000 n'introduit aucune particularité pour ces signatures, si ce n'est la qualité de la personne qui les appose.

Nous verrons plus loin que le décret 2001-272 du 30 mars 2001 introduit, pour la signature électronique, des niveaux de sécurité différents. Même si rien dans les textes n'indique que cette subtilité ait été introduite explicitement pour les officiers publics, cette interprétation est assez répandue.

Abordons maintenant le second alinéa de l'article 1316-4 du Code civil.

Code civil – Article 1316-4 (2nd alinéa)

Lorsqu'elle est électronique, elle consiste en l'usage d'un procédé fiable d'identification garantissant son lien avec l'acte auquel elle s'attache. La fiabilité de ce procédé est présumée, jusqu'à preuve contraire, lorsque la signature électronique est créée, l'identité du signataire assurée et l'intégrité de l'acte garantie, dans des conditions fixées par décret en Conseil d'État.

Copyright © 2012 Eyrolles.

La signature électronique est… une signature !

Ce dernier alinéa de la loi du 13 mars 2000 aborde enfin la notion de signature électronique à proprement parler. Il convient de porter une attention toute particulière aux termes choisis. En effet, le législateur n'a pas écrit « la signature électronique est… », mais « lorsqu'elle est électronique, elle… ».

Par ce choix délibéré est exprimé le fait que la signature électronique n'est qu'un cas particulier de signature. Dans la continuité des articles précédents, qui établissaient l'équivalence du papier et de l'électronique, la signature électronique n'est qu'un cas particulier de signature, et pas une notion juridique à part.

Une signature électronique n'est rien d'autre qu'une signature, qui porte sur un document de nature électronique. Tout ce qui a été dit précédemment sur la signature s'applique donc à la signature électronique.

En quoi consiste la signature électronique ?

La signature électronique consiste en l'usage d'un procédé fiable d'identification. Comme nous l'avons vu dans le chapitre sur les certificats et dans le chapitre sur le RGS, la fiabilité de ce procédé repose sur la qualité du certificat de signature employé, et en particulier sur le procédé d'enregistrement de l'utilisateur, c'est-à-dire les moyens mis en œuvre pour garantir que le porteur du certificat est bien la personne qu'il prétend être et pour protéger sa clé privée. Nous détaillerons au chapitre 8 sur la définition technique de la signature électronique les différents moyens d'identification employables pour réaliser des signatures électroniques, toute la subtilité de la mise en œuvre dépendant de l'interprétation du mot « fiable » dans l'expression « un procédé fiable d'identification ».

Ce procédé d'identification doit « garantir son lien avec l'acte auquel il s'attache » : nous verrons dans la définition technique de la signature électronique comment les mécanismes cryptographiques permettent de créer et de maintenir ce lien de manière irréfutable. Cette exigence, qui n'est pas exprimée pour la signature manuscrite, pose le principe équivalent au fait que l'encre marque le papier de manière indélébile et est donc indissociable du document signé.

Un élément est fondamental à faire ressortir : inclure dans un document le scan d'une signature manuscrite ne répond absolument pas à la définition. En effet, il suffirait de disposer d'un document signé par un individu pour copier l'image de sa signature (ou la scanner s'il s'agit d'une signature papier) pour constituer un document signé par cette personne ! Cela ne peut en aucun cas constituer « un procédé fiable d'identification », puisque ce travail de faussaire est aujourd'hui à la portée de n'importe quel enfant un peu familier avec l'outil informatique.

Copyright © 2012 Eyrolles.

Enfin, cet alinéa introduit la notion de signature électronique « présumée fiable », qui a été développé dans le décret du 30 mars 2001.

Le décret du 30 mars 2001

Le décret du 30 mars 2001 pose de nombreuses définitions et met en place le cadre de qualification des dispositifs de création de signature électronique (les cartes à puce et clés USB), des prestataires de services de certification électronique et des certificats qu'ils délivrent.

Nous invitons le lecteur à se reporter directement au texte pour plus de détails. Nous nous contenterons de parcourir ici les définitions de la signature électronique, de la signature électronique sécurisée et de la signature électronique emportant présomption de fiabilité.

Mais avant tout, intéressons-nous à la définition qui est donnée du signataire.

Le signataire

Le décret du 30 mars 2001 définit ainsi le signataire.

Décret du 30 mars 2001 – Article 1

Au sens du présent décret, on entend par [...] signataire : toute personne physique, agissant pour son propre compte ou pour celui de la personne physique ou morale qu'elle représente, qui met en œuvre un dispositif de création de signature électronique.

La notion à faire ressortir ici est qu'au sens du droit français, un signataire est une personne physique. Nous verrons plus loin que, dans le droit européen, la notion de signataire peut être étendue aux personnes morales. Pour établir une équivalence avec cette notion de signature de personne morale, nous aborderons également la notion de « cachet », qui est techniquement l'équivalent d'une signature, mais n'est pas apposé par une personne physique.

Il est à noter que l'usage d'un pseudonyme dans le certificat de signature électronique qualifié est possible.

Décret du 30 mars 2001 – Article 6

Un certificat électronique qualifié doit comporter : [...] le nom du signataire ou un pseudonyme, celui-ci devant alors être identifié comme tel.

Les différents niveaux de signature électronique

La signature électronique « simple »

Le décret du 30 mars 2001 commence par établir que le strict respect de la loi du 13 mars 2000 est suffisant pour réaliser des signatures électroniques.

Copyright © 2012 Eyrolles.

Décret du 30 mars 2001 – Article 1

Au sens du présent décret, on entend par [...] signature électronique : une donnée qui résulte de l'usage d'un procédé répondant aux conditions définies à la première phrase du second alinéa de l'article 1316-4 du Code civil.

Les deux autres notions introduites ensuite (signature électronique sécurisée et signature électronique emportant présomption de fiabilité) sont des types particuliers de signatures électroniques correspondant à des niveaux de sécurisation croissants.

La signature électronique « sécurisée »

Cette définition présente un niveau particulier de sécurisation de la signature électronique.

Décret du 30 mars 2001 – Article 1 (suite)

Au sens du présent décret, on entend par [...] signature électronique sécurisée : une signature électronique qui satisfait [...] aux exigences suivantes :

- être propre au signataire ;
- être créée par des moyens que le signataire puisse garder sous son contrôle exclusif ;
- garantir avec l'acte auquel elle s'attache un lien tel que toute modification ultérieure de l'acte soit détectable.

On peut noter que le fait que la signature électronique « soit propre au signataire » est redondant avec l'exigence de la loi du 13 mars 2000 qui veut que la signature « identifie celui qui l'appose ».

En revanche, l'exigence que le signataire puisse garder ses moyens de signature (c'est-à-dire sa clé privée) sous son contrôle exclusif exclut du champ de la signature électronique sécurisée le cas d'un serveur informatique qui réaliserait automatiquement des signatures au nom du signataire, sans validation par celui-ci.

La notion peut être interrogée dans les cas où le moyen de signature se trouverait sur un serveur mais ne serait déclenché que sur demande explicite du signataire : dans un tel mode de fonctionnement, le signataire peut-il garder ses moyens de signature sous son contrôle *exclusif*, ou ne court-il pas le risque que les exploitants du serveur emploient ses moyens de signature à son insu ? Cela dépendra des garanties de sécurité mises en œuvre, des engagements pris par l'exploitant du service de signature électronique, et de la convention de preuve établie dans le cadre de ce service comme nous le verrons dans le chapitre consacré à la convention de preuve.

L'exigence de la loi du 13 mars 2000 sur le fait que la signature électronique « garantisse un lien avec l'acte auquel elle s'attache » est ici précisée : il

Copyright © 2012 Eyrolles.

est exigé que la signature électronique sécurisée permette la détection de toute modification ultérieure du document. Cette exigence est tout à fait en accord avec l'état de l'art des solutions de signature électronique couramment utilisées, comme nous le verrons dans le chapitre 8.

Ainsi, la « signature électronique sécurisée » est très répandue et forme la majeure partie des signatures électroniques réalisées.

La signature électronique « présumée fiable »

Le niveau suivant est la signature électronique « présumée fiable » :

Décret du 30 mars 2001 – Article 2

La fiabilité d'un procédé de signature électronique est présumée jusqu'à preuve contraire :

- si ce procédé met en œuvre une signature électronique sécurisée ;
- s'il est établi grâce à un dispositif sécurisé de création de signature électronique ;
- si la vérification de cette signature repose sur l'utilisation d'un certificat électronique qualifié.

Cet article précise dans quelles conditions un procédé de signature électronique emporte présomption de fiabilité. Une signature établie dans ces conditions entraîne le renversement de la charge de la preuve. Cela signifie que :

- dans le cas général, en cas de contestation de la validité d'une signature électronique, la partie défenderesse doit apporter la preuve de la validité ;
- en revanche, pour une signature « emportant présomption de fiabilité », c'est la partie qui conteste la validité de la signature qui doit apporter la preuve de son invalidité.

Les conditions à remplir sont les suivantes :

- la signature électronique doit être sécurisée, au sens de l'article 1 du même décret (voir encadré précédent) ;
- la carte à puce ou la clé USB sur laquelle se trouve la clé privée du signataire doit être un « dispositif de création de signature électronique sécurisé », c'est-à-dire avoir été certifié par l'Agence nationale pour la sécurité des systèmes d'information (ANSSI) (voir le chapitre 5 abordant les supports du certificat pour plus de détails). À noter qu'aucun magasin logiciel ne correspond à ce niveau d'exigence ;
- le certificat du signataire doit être « qualifié », comme nous l'avons vu dans le chapitre 5 consacré aux certificats.

Certains considèrent que ce type de signature électronique a été défini pour garantir un haut niveau de fiabilité aux signatures électroniques des officiers publics qui établissent des actes authentiques.

Copyright © 2012 Eyrolles.

Voyons maintenant les grandes lignes du cadre communautaire pour les signatures électroniques, en faisant ressortir les principales différences avec notre droit national.

La signature électronique en Europe : la directive de 1999

La directive 1999/93/CE du Parlement européen et du Conseil, du 13 décembre 1999, sur un cadre communautaire pour les signatures électroniques, est le texte fondateur de la signature électronique en Europe.

Parallèle entre les définitions européennes et françaises

Le signataire

Voici comment la directive de 1999 définit le signataire.

Directive 1999/93/CE – Article 2

Aux fins de la présente directive, on entend par : [...] « signataire », toute personne qui détient un dispositif de création de signature et qui agit soit pour son propre compte, soit pour celui d'une entité ou personne physique ou morale qu'elle représente.

La principale différence avec le droit français est que le mot « personne » est ici applicable aussi bien à une personne physique qu'à une personne morale.

Les différents niveaux de signature

Les définitions suivantes de la signature électronique sont également à mettre en regard des définitions françaises.

Directive 1999/93/CE – Article 2

Aux fins de la présente directive, on entend par :

1) « signature électronique », une donnée sous forme électronique, qui est jointe ou liée logiquement à d'autres données électroniques et qui sert de méthode d'authentification ;

2) « signature électronique avancée », une signature électronique qui satisfait aux exigences suivantes :

a) être liée uniquement au signataire ;

b) permettre d'identifier le signataire ;

c) être créée par des moyens que le signataire puisse garder sous son contrôle exclusif ;

d) être liée aux données auxquelles elle se rapporte de telle sorte que toute modification ultérieure des données soit détectable.

On peut noter trois points principaux qui ressortent de ces définitions.

Copyright © 2012 Eyrolles.

L'article 1316-4 du Code civil a introduit dans la définition de la signature électronique la notion de lien « garanti » entre le procédé d'identification et l'acte auquel il s'attache, alors que la signature électronique au sens européen est « jointe ou liée logiquement » aux données signées.

La signature sert dans le droit européen de « méthode d'authentification », sans précision quant à ce qui est ainsi authentifié : est-ce le signataire, le document, ou les deux ? Le droit français, quant à lui, a précisé que la signature « identifie celui qui l'appose ».

Enfin, la signature électronique « avancée » est l'équivalent de ce que le droit français appelle la signature électronique « sécurisée ».

La notion de signature électronique « présumée fiable » introduite en France par le décret du 30 mars 2001 provient également de la directive de 1999.

Directive 1999/93/CE – Article 5

Effets juridiques des signatures électroniques

Les États membres veillent à ce que les signatures électroniques avancées basées sur un certificat qualifié et créées par un dispositif sécurisé de création de signature :

a) répondent aux exigences légales d'une signature à l'égard de données électroniques de la même manière qu'une signature manuscrite répond à ces exigences à l'égard de données manuscrites ou imprimées sur papier ;

b) soient recevables comme preuves en justice.

On retrouve bien dans cette définition les trois contraintes correspondant à la signature présumée fiable ; en revanche, les exigences d'effet juridique ont été modifiées :

- l'équivalence avec la signature manuscrite est établie en droit français dès le niveau de la signature électronique « simple » ;
- la recevabilité comme preuve en justice a été transposée en France sous la forme de présomption de fiabilité.

L'interopérabilité des certificats de signature électronique au niveau européen

La directive de 1999 instaure l'obligation pour les États membres de reconnaître les certificats de signature électronique émis dans les autres pays.

Au moment où nous rédigeons cet ouvrage, les référentiels européens de reconnaissance mutuelle des certificats sont en cours de mise en œuvre, notamment au travers de l'élaboration et de la publication de la *Trusted Lists of Certification Service Providers* qui recense les autorités de certification de confiance au niveau de l'Union. Il est à noter que, le RGS incluant des exigences supérieures par rapport au seul cadre européen, l'établissement

Copyright © 2012 Eyrolles.

d'équivalences n'est pas aisé pour les utilisateurs français, en particulier pour les collectivités publiques, auxquelles le RGS s'impose.

Directive 1999/93/CE – Article 7

Aspects internationaux

Les États membres veillent à ce que les certificats délivrés à titre de certificats qualifiés à l'intention du public par un prestataire de services de certification établi dans un pays tiers soient reconnus équivalents, sur le plan juridique, aux certificats délivrés par un prestataire de services de certification établi dans la Communauté :

a) si le prestataire de services de certification remplit les conditions visées dans la présente directive et a été accrédité dans le cadre d'un régime volontaire d'accréditation établi dans un État membre ;

b) si un prestataire de services de certification établi dans la Communauté, qui satisfait aux exigences visées dans la présente directive, garantit le certificat ;

c) si le certificat ou le prestataire de services de certification est reconnu en application d'un accord bilatéral ou multilatéral entre la Communauté et des pays tiers ou des organisations internationales.

L'usage des pseudonymes

La directive de 1999 permet l'usage de pseudonymes dans les certificats de signature électronique.

Directive 1999/93/CE – Article 8

Protection des données

Sans préjudice des effets juridiques donnés aux pseudonymes par la législation nationale, les États membres ne peuvent empêcher le prestataire de services de certification d'indiquer dans le certificat un pseudonyme au lieu du nom du signataire.

Cette possibilité est encadrée afin de permettre une identification fiable du signataire.

Directive 1999/93/CE – Considérant 25

Il convient que les dispositions relatives à l'utilisation de pseudonymes dans des certificats n'empêchent pas les États membres de réclamer l'identification des personnes conformément au droit communautaire ou national.

Une fois le cadre juridique de la signature électronique ainsi défini, penchons-nous sur les aspects techniques liés à sa mise en œuvre.

Copyright © 2012 Eyrolles.

Copyright © 2012 Eyrolles.

Chapitre 8

La signature électronique : un objet technique

La réalisation technique d'une signature électronique

Les aspects cryptographiques de la signature électronique

Réaliser une signature électronique : un mécanisme de scellement cryptographique

Nous avons vu dans le chapitre 2, à la section dédiée à la cryptographie, que la signature électronique consiste à effectuer un calcul RSA à l'aide de la clé privée sur le document à signer.

Mais nous avons vu dans un second temps que cela n'était possible que si le document comportait moins de 256 caractères (pour une bi-clé de 2 048 bits) – ce qui est notoirement insuffisant.

Le rôle de la signature électronique étant de marquer son engagement sur les termes d'un document, il est fondamental que le calcul RSA, qui lie le document au signataire, porte bien sur l'intégralité du contenu du document signé. Pour ramener un document de 200 kilo-octets ou plus à moins de 256 octets, on utilise une fonction de hash, par exemple SHA256.

Le déroulement d'une signature électronique, du strict point de vue cryptographique, est donc le suivant (figure 8-1) :

- le document est condensé à l'aide d'une fonction de hash, par exemple SHA256 ;
- le hash du document est soumis à un calcul RSA à l'aide de la clé privée du signataire (cette opération nécessite la saisie du code PIN du signataire si le certificat est sur un support physique) ;

Copyright © 2012 Eyrolles.

- le résultat de ce calcul est, au sens technique, un scellement garantissant l'intégrité du document et réalisé par un acteur identifié, le signataire.

Lorsqu'on est dans le cadre juridique de l'engagement d'une personne sur le contenu d'un document, on appelle ce scellement une « signature électronique », et c'est le terme générique retenu abusivement pour décrire l'opération technique décrite ici. Nous verrons plus loin que, dans certains contextes, cette même procédure technique peut donner naissance à un cachet, à un jeton d'horodatage, à un certificat…

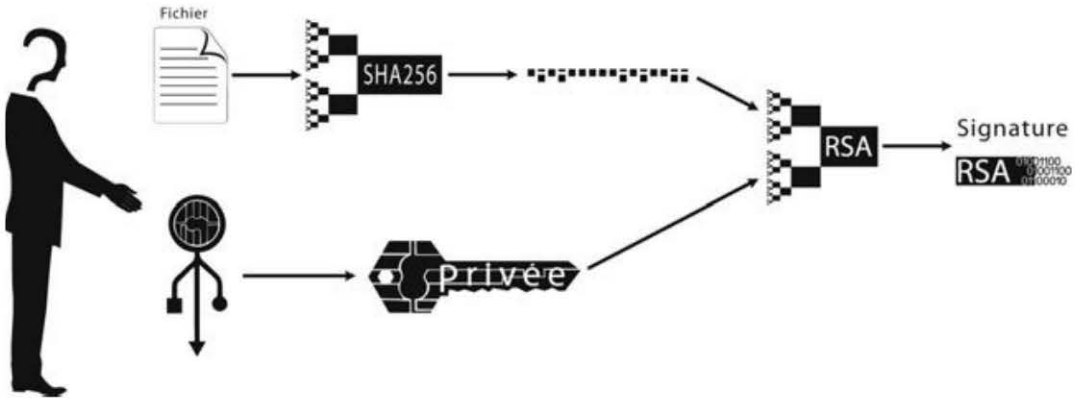


Figure 8-1 : La réalisation cryptographique d'une signature électronique

Le contenu des signatures électroniques

Une fois le calcul décrit précédemment réalisé, la signature électronique doit être complétée par les éléments nécessaires à sa vérification par le destinataire, et mise en forme à l'aide de l'un des formats standards que nous évoquerons à la section suivante.

Les éléments complémentaires à ajouter dans une signature électronique sont au nombre de trois :

- le certificat du signataire et la chaîne de certification correspondante ;
- un jeton d'horodatage permettant de connaître avec certitude le moment de réalisation de la signature, et ainsi de vérifier la validité du certificat du signataire ;
- une preuve de non-révocation du certificat du signataire.

Le contenu d'une signature électronique est alors résumé dans la figure 8-2.

Copyright © 2012 Eyrolles.

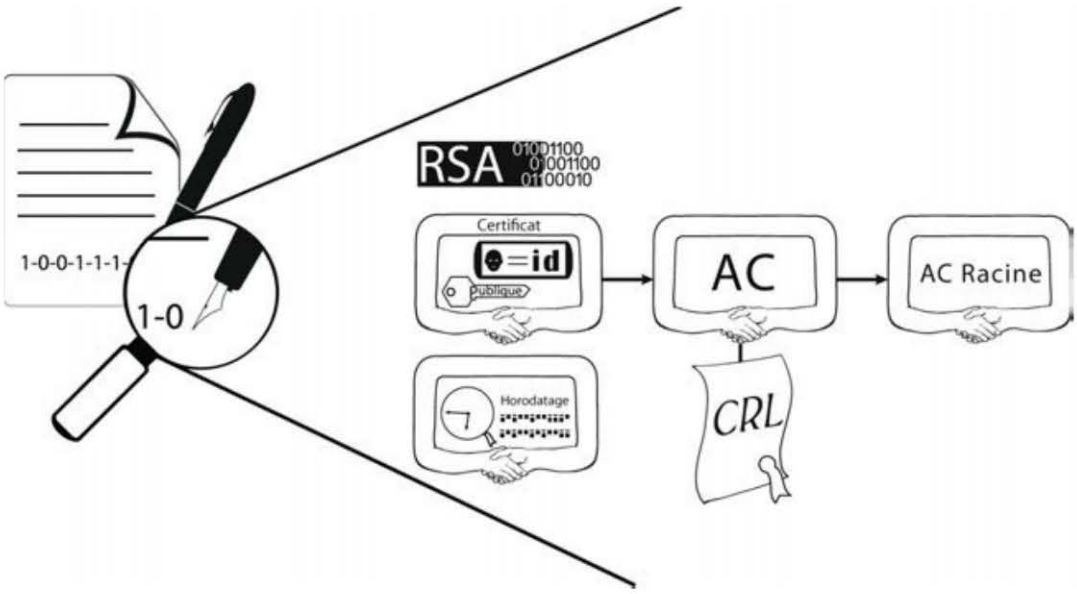


Figure 8-2 : Le contenu d'une signature électronique

Les formats de signatures électroniques

Les différents standards

Les formats de signatures électroniques sont nommés de manière homogène « AdES » pour *Advanced Electronic Signature*. Il en existe trois familles principales :

- le format XML, connu sous le terme générique de XAdES ;
- le format PKCS#7/CMS, connu sous le terme de CAdES ;
- le format PDF, connu sous le terme de PAdES.

Chacune de ces familles se décline en six sous-formats, classés par ordre croissant de fonctionnalités pour offrir des niveaux de sécurité successifs :

- AdES-BES (*Basic Electronic Signature*) correspond aux exigences minimales requises pour la réalisation de signatures électroniques sécurisées ;
- AdES-T (*Timestamp*) permet d'inclure dans la signature un jeton d'horodatage ;
- AdES-C (*Complete*) permet d'inclure des références à la chaîne de certification et à la liste de révocation ;
- AdES-X (*Extended*) permet d'inclure un horodatage des références incluses dans AdES-C pour éviter leur modification ;
- AdES-X-L (*Long-term*) permet d'inclure les certificats et la liste de révocation au lieu de simples références à ces éléments ;
- AdES-A (*Archiving*) permet de renouveler périodiquement les horodatages afin de garantir une certitude d'intégrité au fil du temps.

Copyright © 2012 Eyrolles.

Nous allons détailler les trois formats afin d'en présenter les caractéristiques et les avantages.

Le format XAdES

Le format XAdES (XML *Advanced Electronic Signature*) est une extension du format préexistant de signature XML, XMLDSig.

Il s'agit d'un format de stockage des signatures électroniques qui peut être indépendant des données signées (la signature constitue alors un fichier XML séparé du document signé, qui peut être à n'importe quel format), ou inclus dans le document signé si ce document est lui-même au format XML.

Aucun élément graphique ne permet d'identifier la présence d'une signature.

Le format CAdES

Le format CAdES (CMS *Advanced Electronic Signature*) permet de former des signatures détachées (la signature est dans un fichier à part, à transmettre en même temps que le document signé) ou opaque, c'est-à-dire que le document est inclus dans une « enveloppe » qui comporte aussi la signature.

Les deux options comportent des avantages et des inconvénients :

- dans le cas des signatures détachées, pour transmettre un document signé, il faut envoyer les deux fichiers simultanément ; le document initial est lisible avec le logiciel qui lui est nativement associé sans aucune manipulation ;
- dans le cas des signatures opaques, il faut disposer d'un outil pour extraire de l'enveloppe le document lorsque l'on souhaite le lire : faute de cet outil, l'enveloppe n'est pas exploitable directement, par exemple par un logiciel bureautique.

Le format CAdES permet la signature multiple du même document par plusieurs signataires.

Aucun élément graphique ne permet d'identifier la présence d'une signature.

Le format PAdES

Le format PAdES (PDF *Advanced Electronic Signature*) est le format des signatures électroniques incluses dans les documents PDF. Le format PAdES s'appuie sur le format CAdES.

Il permet la signature multiple du même document par plusieurs signataires, sous la forme de sursignatures : chaque signataire signe non seulement le document, mais aussi les signatures déjà apposées par les signataires précédents.

Copyright © 2012 Eyrolles.

Il existe deux natures de signatures : la « certification », qui correspond à un cachet apposé, par exemple, par l'application qui a généré le document, et la signature à proprement parler, qui correspond à l'approbation par un signataire.

La signature peut optionnellement apparaître graphiquement dans le document lorsqu'on le visualise avec le logiciel Adobe Reader. En cliquant sur cet élément graphique entièrement personnalisable, on affiche une fenêtre de vérification technique de la signature. Les informations à afficher dans un cartouche de signature informatif et les informations à afficher lors de la vérification de la signature sont normalisées par l'ETSI.

Quels types de données peut-on signer électroniquement ?

Il n'existe pas de restriction technique quant aux types de données que l'on peut signer électroniquement : la signature peut aussi bien porter sur un document bureautique (traitement de texte, tableur, présentation, PDF) que sur une image, sur des données informatiques (XML, extraction de base de données…), sur des plans d'architecte, sur des données d'information géographique, du son, des vidéos…

Bien entendu, il existe une limitation liée au format de la signature : une signature PAdES ne pourra porter que sur un document PDF. En revanche, les formats XAdES et CAdES permettent de signer tous les documents, quel que soit leur format.

Cependant, du point de vue juridique, la signature électronique doit porter sur des données intelligibles par un être humain, puisqu'il s'agit du consentement d'une personne physique au contenu d'un document. Il convient donc, dans la pratique, de ne faire signer par des utilisateurs que des documents dont ils peuvent visualiser et approuver le contenu, et dont la signature est rendue nécessaire par le contexte juridique.

Deux cas particuliers méritent d'être développés : les signatures apposées sur des fichiers ZIP et les e-mails.

La signature électronique apposée sur une enveloppe ZIP contenant un ou plusieurs documents ne vaut pas signature de chacun des documents contenus dans le fichier ZIP ! Signer l'enveloppe ne revient pas à signer le contenu de l'enveloppe.

Une jurisprudence a confirmé ce fait à l'occasion du rejet par une personne publique d'une offre à un marché public constituée d'un fichier ZIP signé sans que les fichiers inclus le soient eux-mêmes. Pour envoyer un ensemble de documents signés électroniquement, il convient de signer individuellement chacun des fichiers, puis de constituer l'enveloppe ZIP contenant les fichiers et, si elles sont en mode détaché, les signatures électroniques correspondantes.

Copyright © 2012 Eyrolles.

Le format standard de signature des courriers électroniques, S/MIME, fait porter la signature électronique sur le corps de l'e-mail et les pièces jointes. L'émetteur, le ou les destinataires et l'objet de l'e-mail sont exclus du champ de la signature, et leur intégrité n'est donc pas garantie.

Comme pour la signature de fichier ZIP, le format S/MIME consiste en la création d'une enveloppe contenant plusieurs éléments (le corps de l'e-mail et les pièces jointes éventuelles). Là encore, envoyer un e-mail signé contenant une pièce jointe n'équivaut pas à envoyer un e-mail contenant une pièce jointe signée.

La vérification d'une signature électronique

La vérification d'une signature électronique comporte trois étapes :

- la vérification technique, qui consiste à contrôler que la signature est bien formée techniquement et correspond bien au document signé ;
- la vérification de la chaîne de la confiance, qui consiste à contrôler que le certificat du signataire est bien émis par une autorité de certification fiable ;
- la vérification juridique, qui consiste à s'assurer que, dans le contexte précis de l'application, la signature est bien recevable.

Détaillons maintenant ces étapes.

La vérification technique de la signature électronique

La vérification technique de la signature électronique est réalisée automatiquement par le logiciel de vérification de signature.

Elle est effectuée selon les étapes suivantes, reprises dans la figure 8-3 :

1. extraire de l'enveloppe de signature le certificat du signataire ;
2. extraire du certificat la clé publique du signataire ;
3. effectuer sur la signature un calcul RSA à l'aide de cette clé publique : le résultat de ce calcul est le hash du document qui a été initialement signé ;
4. calculer le hash du document reçu ;
5. comparer ce hash avec celui qui provient du calcul RSA :
   - si les deux sont identiques, alors la signature porte bien sur le document reçu : elle est techniquement valide ;
   - dans le cas contraire, le document a été modifié depuis le moment où il a été signé, ou la signature portait sur un autre document : la signature est invalide.

Copyright © 2012 Eyrolles.

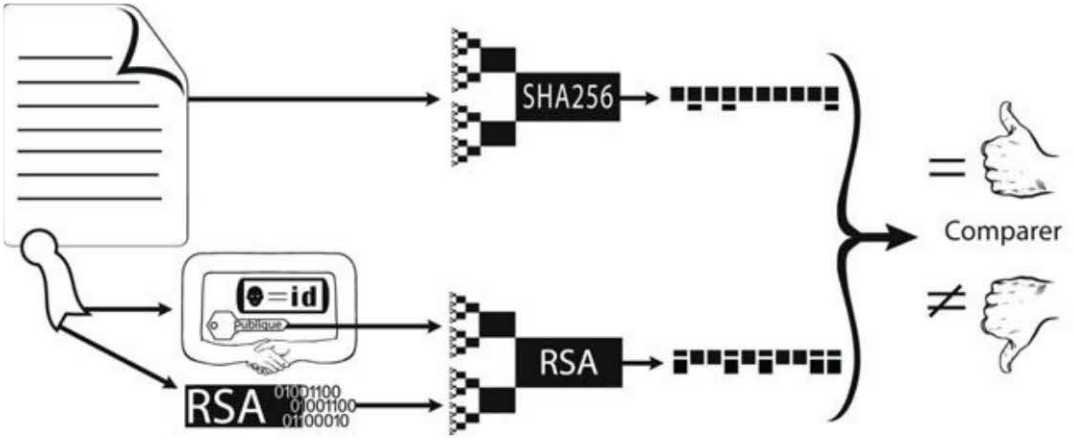


Figure 8-3 : La vérification technique d'une signature électronique

À l'issue de cette vérification, un résultat valide donne la certitude que le signataire est bien le porteur du certificat qui a été transmis avec la signature.

La deuxième étape consiste à vérifier si l'on peut faire confiance à ce certificat.

La vérification du certificat et l'héritage de la confiance

L'enveloppe de signature comprend l'ensemble de la « chaîne de la certification », c'est-à-dire le certificat du signataire, le certificat de l'autorité de certification qui l'a émis et les certificats des AC successives éventuelles au-dessus de celle-ci.

Une fois que l'on a vérifié que la signature était techniquement valide, il convient de s'assurer que :

- le certificat du signataire est valide ;
- l'un des certificats de cette chaîne a été défini comme digne de confiance dans le cadre de l'application concernée.

Vérifions le certificat du signataire

La vérification du certificat du signataire comporte plusieurs étapes, que nous développons maintenant.

Les première et deuxième étapes portent sur le certificat lui-même.

1. Il faut tout d'abord vérifier que ce certificat est bien formé et qu'il est intègre : l'outil de vérification de signature procède automatiquement à cette vérification de format et à la vérification du scellement du certificat par son autorité de certification émettrice, qui garantit son intégrité.
2. Il s'agit ensuite de s'assurer que le certificat est bien dédié à l'usage qui en a été fait : s'il ne contient pas les extensions correspondant à la fonctionnalité de signature électronique, il ne faut pas l'accepter. Par

Copyright © 2012 Eyrolles.

exemple, rien n'empêche techniquement d'utiliser un certificat de chiffrement pour réaliser une signature électronique ; mais comme nous l'avons vu au chapitre 5 consacré au cycle de vie des certificats, la clé privée d'un certificat de chiffrement est séquestrée pour éviter les pertes de données, alors que la clé privée d'un certificat de signature ne doit impérativement exister qu'en un seul exemplaire.

Les troisième et quatrième étapes portent sur la validité du certificat au moment où la signature a été réalisée.

En effet, la date à laquelle la vérification de signature est effectuée peut être très éloignée de sa date de réalisation, et il est possible que le certificat du signataire ne soit plus valide au moment de la vérification : cela ne doit pas porter préjudice à la validité de la signature. Ce qui compte, c'est que ce certificat ait été valide au moment où son porteur s'en est servi pour signer.

Il est donc fondamental de disposer dans la signature de la date de sa réalisation. Il existe deux façons d'inclure une date dans une signature électronique.

- Par défaut, les outils de signature électronique incluent la date et l'heure du poste de travail sur lequel la signature est en cours de réalisation : cette date n'est pas fiable puisqu'il suffit de modifier l'horloge de son ordinateur pour inclure dans la signature la date de son choix.
- Il est possible d'inclure un jeton d'horodatage certifié, émis par une autorité d'horodatage, qui garantit l'exactitude de la date et son intégrité. Nous verrons au chapitre 11 consacré à la traçabilité comment sont constitués ces jetons d'horadotage. C'est bien entendu la méthode recommandée pour garantir la capacité de vérification de la validité du certificat du signataire. Elle comporte l'inconvénient de nécessiter que le poste du signataire soit connecté à Internet afin d'accéder au service de l'autorité d'horodatage. Il est également possible de compléter la signature électronique avec l'horodatage *a posteriori*, de préférence « au plus près » du moment de la signature, l'essentiel étant que le certificat ne soit pas devenu invalide entre le moment de la réalisation de la signature et celui de l'inclusion de l'horodatage, sans quoi la signature serait rejetée lors de sa vérification.

3. La troisième étape consiste à vérifier si le certificat était bien en cours de validité au moment où la signature a été réalisée, en comparant la date de la signature aux dates de début et de fin de validité du certificat.
4. Il faut enfin examiner le statut de révocation du certificat au moment de la signature. Cela peut se faire de deux manières : en utilisant la liste de certificats révoqués (LCR) publiée par l'autorité de certification émettrice du certificat du signataire, ou en faisant appel au protocole OCSP, comme nous l'avons vu au chapitre 5 sur le cycle de vie du certificat.

Copyright © 2012 Eyrolles.

Il est possible d'inclure dans la signature électronique la LCR en cours de validité au moment de la réalisation de la signature, ou un jeton de vérification de validité OCSP attestant de la validité du certificat à ce même moment. On appelle ces éléments les « preuves de validité du certificat ».

Si elle inclut un horodatage certifié et une preuve de validité du certificat, la signature pourra être vérifiée techniquement de manière autonome même plusieurs années après sa réalisation.

Dans le cas contraire, il faudra accéder à la liste de certificats révoqués correspondante pour la contrôler. Il est alors prudent de l'archiver en même temps que la signature, car on peut difficilement se contenter d'espérer qu'elle soit encore en ligne le jour où un contrôle s'avérera nécessaire !

Vérifions la chaîne de confiance

Les autorités de certification « de confiance » sont celles qui ont été recensées au sein du magasin de certificats, comme nous l'avons vu au chapitre 5 consacré aux certificats. Une AC pourra être inscrite dans ce magasin pour plusieurs raisons différentes :

- il s'agit de l'AC interne de l'entreprise ;
- il s'agit d'une AC qualifiée à un niveau suffisant du RGS, par exemple (**) ;
- il s'agit d'une AC figurant sur la liste officielle d'un autre pays de l'Union européenne…

Le logiciel de vérification de signature va donc confirmer, à chaque niveau de la chaîne de certification, que le certificat est correct du point de vue technique, et qu'il a été valablement scellé par l'AC du niveau supérieur.

Il cherche ensuite si, dans le magasin de certificats, une des AC figure comme étant digne de confiance. Dans le cas inverse, un message d'alerte sera affiché à l'utilisateur.

La figure 8-4 illustre ce mécanisme : la confiance dans le signataire dépend donc de la confiance dans l'autorité de certification, qui découle elle-même, par exemple, de la confiance que l'on peut placer dans le processus d'évaluation des prestataires de services de certification électronique mis en œuvre par l'ANSSI.

Cette étape de vérification, réalisée automatiquement, permet de s'assurer que le nom figurant dans le certificat est bien celui du signataire. Toutefois, cela n'est pas toujours suffisant pour valider la signature juridiquement, il faut aussi vérifier si ce signataire est bien légitime.

Copyright © 2012 Eyrolles.

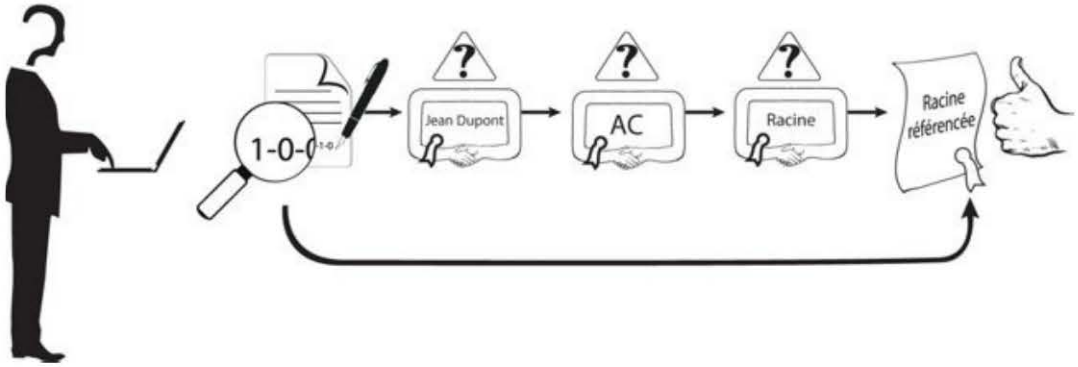


Figure 8-4 : La chaîne de confiance

La vérification juridique

La vérification juridique de la signature électronique est malheureusement souvent oubliée dans les processus de vérification de signature, pour une raison simple : elle dépend entièrement du contexte de l'application et doit donc être effectuée par un être humain ; elle peut difficilement être automatisée.

Cette vérification permet de s'assurer que le signataire est bien habilité à signer le document. Par exemple, s'agissant de la signature d'une offre à un marché public, il faut vérifier que :

- le signataire fait partie de l'entreprise ;
- le signataire est habilité à engager l'entreprise, soit parce qu'il figure sur le K-bis de celle-ci, soit parce qu'il a reçu un mandat de délégation de signature de la part d'un responsable lui-même habilité ;
- le mandat de délégation est bien conforme avec le contexte du marché, car une délégation de signature peut être limitée non seulement dans le temps, mais aussi en termes de montants.

Jurisprudence : l'importance de l'identité du signataire

Lors de la passation d'un marché d'infogérance par une caisse de Sécurité sociale, un candidat, SSII importante et titulaire de nombreux certificats, a transmis des pièces signées électroniquement par un employé ayant quitté la société. Son offre a été rejetée.

Lors de la commission d'ouverture des plis, le président de la commission a constaté que le nom indiqué dans certificat électronique, le nom indiqué sur l'acte d'engagement et les noms des personnes habilitées à engager la société sur le K-bis étaient différents. La caisse a donc demandé à la société, *via* un imprimé OUV 7, de bien vouloir compléter sa candidature en fournissant une attestation établissant que le signataire titulaire du certificat électronique a qualité pour engager l'entreprise.

Copyright © 2012 Eyrolles.

L'entreprise a répondu en indiquant que la personne titulaire du certificat électronique pour la succursale avait quitté la société pendant la période précédant la remise des offres. Le candidat a donc été rejeté.

Suite à ces actions, le candidat évincé a saisi le tribunal de grande instance (TGI) de Paris, compétent pour juger de la bonne application du Code des marchés publics en l'espèce. Le TGI a confirmé la caisse dans sa décision, en indiquant qu'elle n'avait commis aucune irrégularité de nature à entraîner l'annulation des actes de procédure, et en rappelant que le titulaire du certificat électronique utilisé lors de l'offre de la société n'avait plus aucun mandat pour signer en son nom et l'engager.

Penchons-nous sur l'opinion d'un praticien de la commande publique concernant la signature électronique des marchés publics.

Parole d'expert

Philippe Maraval, directeur des achats de Pôle Emploi

En quoi la signature apposée par les candidats aux marchés publics est-elle essentielle ?

Le Code des marchés publics impose la signature de la lettre de candidature et de l'acte d'engagement, que la réponse soit déposée sous forme papier ou électronique.

L'exigence d'une signature électronique a trois buts : tout d'abord, marquer l'engagement du signataire, pour éviter tout risque de rétractation. Ensuite, prouver l'intégrité des documents transmis et, grâce à l'horodatage, la date et l'heure de la transmission des pièces, afin de garantir le respect des conditions cardinales de l'égalité de traitement des candidats. Enfin, réduire le risque de contentieux lié au déroulement de la procédure, le respect des textes étant à ce titre primordial.

Dans les marchés publics, la signature va au-delà du seul engagement de l'entreprise : les procédures de contrôle internes ou externes à la personne publique requièrent souvent que les agents qui procèdent au dépouillement des offres signent eux-mêmes les pièces qu'ils ont reçues, afin d'assurer une traçabilité de la procédure d'analyse et d'attribution des marchés.

Par ailleurs, la dématérialisation, en offrant une immédiateté et une traçabilité parfaite de la transmission des dossiers de consultation des entreprises (DCE), a eu un impact majeur sur la passation des marchés en rendant obsolète la signature par le candidat du CCTP et du CCAP, dont l'exemplaire conservé par la personne publique fait foi : aucun débat sur le contenu objectif de ces pièces n'est plus possible, on est là dans le domaine du contrat d'adhésion, et tout rejet d'une clause par un candidat entraîne l'irrégularité de son offre.

Ainsi, seule la signature par le candidat de l'acte d'engagement et du bordereau de prix unitaires est essentielle.

Pour les marchés de faible montant, les exigences imposées par le législateur sont moins importantes. Il s'agit de mettre en adéquation les moyens de sécurisation mis en œuvre avec les enjeux réels. Les coûts de gestion des marchés doivent rester proportionnés aux dépenses. Que ce soit sur la mise en concurrence, la sécurisation

Copyright © 2012 Eyrolles.

des offres (notamment *via* leur signature) ou la collégialité et la transparence de la prise de décision, les choix sont libres au sein de la collectivité pour les petits marchés, en fonction de sa politique de gestion du risque. Le législateur a tout de même, depuis 2001, ajouté une sécurité : les contraintes de formalisation sont liées non au montant de chaque marché, mais à l'ensemble des dépenses annuelles sur chaque famille d'achat. Reste que, s'agissant de la gestion des deniers publics, les aspects économiques ne peuvent pas faire oublier le point de vue éthique.

Quelle est la validité d'une offre présentée sous la forme d'un fichier ZIP signé électroniquement, en l'absence de signature électronique individuelle des documents compressés ?

Une jurisprudence du tribunal administratif de Toulouse de mars 2011 a établi que la signature d'un fichier ZIP n'était pas suffisante.

Du point de vue du manifestement du consentement, il semble difficile de douter que l'entreprise ait souhaité s'engager sur l'offre incluse dans le fichier ZIP, le contenu de cette enveloppe étant entièrement sous son contrôle.

Néanmoins, du point de vue prudentiel, le risque portant sur le formalisme de la procédure m'amènerait à rejeter une telle offre.

Pourquoi de nombreux marchés publics sont-ils encore rematérialisés, et donnent-ils lieu *in fine* à une signature manuscrite malgré l'obligation de remise électronique des offres inscrite dans l'article 56 du Code des marchés publics ?

La chaîne de passation du marché ne s'arrête pas à la signature de l'acte d'engagement par le représentant du pouvoir adjudicateur : il existe de nombreux contrôles, différents selon les collectivités, en amont et en aval de cet acte : visa préalable du contrôleur financier, contrôle de légalité, comptabilité publique... La mise en œuvre d'une chaîne entièrement dématérialisée passe par la signature d'accords multipartites avec l'ensemble des acteurs de manière locale, aucun cadre général n'étant en place au niveau national. Il s'agit donc d'une démarche complexe, dont le coût est à mettre en balance avec les apports.

En effet, l'obligation de remise dématérialisée des offres (pour les marchés informatiques) est extrêmement récente, et jusqu'alors, le taux de réponse électronique des entreprises était resté marginal. L'effort à faire pour éviter la rematérialisation était donc disproportionné par rapport aux gains réels à en attendre.

En outre, l'usage de la signature électronique, pour se justifier, devrait être étendu aux autres actes signés par la personne publique (contrats de travail, engagement de dépense, liquidation de factures...). Or, il existe aujourd'hui des processus plutôt fondés sur des *workflows* d'approbation que sur la signature électronique, ce qui, en termes de conduite du changement, ne permet pas d'amortir sur plusieurs usages l'investissement lié au déploiement de cet outil.

Reste que l'apport fondamental de la dématérialisation des marchés publics a été l'économie et le gain d'efficacité liés à la diffusion électronique des DCE : quasiment toutes les personnes publiques ont adopté cette pratique extrêmement rapidement. Lorsque la rentabilité de l'investissement est assurée, l'administration met en œuvre les innovations de manière très efficace. Reste à développer les usages de la signature électronique pour en justifier le déploiement à grande échelle.

Copyright © 2012 Eyrolles.

Un élément facilitateur de l'appropriation du processus de signature électronique par les signataires consiste à rapprocher ce processus des habitudes du monde matériel. Voyons maintenant comment des outils innovants peuvent y aider.

Biométrie et signature électronique

La réalisation et la vérification d'une signature manuscrite sont des procédés de nature biométrique : le graphologue compare le signe tracé sur le papier avec une référence, et examine les aspects de pression et de vitesse du stylo pour estimer si les deux ont été réalisés par la même personne.

La signature électronique, quant à elle, repose sur un principe purement technique, mathématique, très éloigné de l'habitude que l'on a du fait de signer. En effet, l'absence de visualisation graphique directement liée au signataire dans une signature électronique, la ressemblance avec le procédé de paiement par carte bancaire (saisie du code PIN), la méthode de vérification comportant des termes complexes (« certificat », « confiance », « autorité de certification »…) font que la signature électronique reste mystérieuse pour le grand public.

L'article 1316-4 du Code civil définissant la signature électronique comme « l'usage d'un procédé fiable d'identification garantissant son lien avec l'acte auquel elle s'attache », il est dès lors tentant d'envisager la réalisation de signatures électroniques de manière biométrique afin de rendre l'opération plus facile d'accès.

Il existe de nombreux cas d'usage de tablettes graphiques, sur lesquelles l'utilisateur est invité à saisir sa signature manuscrite : ce procédé tend à se généraliser pour la remise d'un colis, par exemple. Toutefois, bien que mis en œuvre de manière assez répandue dans d'autres pays d'Europe, ce procédé ne correspond pas à la définition française de la signature électronique, puisque l'identification du signataire n'est pas fiable, et que ce geste n'est pas lié de manière garantie avec le document (en l'occurrence l'accusé de remise du colis).

Une solution peut être mise en œuvre pour lier l'habitude de la signature manuscrite avec la valeur juridique de la signature électronique : elle consiste à faire saisir par le signataire sa signature manuscrite sur une tablette graphique, à l'inclure dans le document, puis à apposer sur le document une signature électronique à l'aide d'un certificat au nom du signataire. Cela se pratique de plus en plus pour des souscriptions de contrats en agence : le vendeur tient lieu d'autorité d'enregistrement, vérifiant les papiers du client avant de déclencher l'émission automatique d'un certificat à son nom.

Copyright © 2012 Eyrolles.

Il est alors possible d'imprimer une copie du document électroniquement signé, et cette copie comporte une image de la signature manuscrite « rassurante » pour le client. La version imprimée n'est évidemment pas un original du contrat, puisque celui-ci est sous forme électronique, mais la ressemblance de cette copie avec les documents « habituels » est de nature à favoriser la confiance et donc l'adhésion des utilisateurs au processus. Il est bien entendu possible de remettre également l'original électronique du contrat signé au client, sur une clé mémoire ou en le lui envoyant par e-mail.

Si cette façon de signer est très intéressante du point de vue des usages, elle n'exploite pas du tout la biométrie puisque l'image de la signature manuscrite ne confère aucune valeur juridique au document : ce qui constitue la preuve, c'est exclusivement la signature électronique réalisée après inclusion de l'image dans le document.

Les nouvelles générations de tablettes graphiques permettent, outre la capture du dessin réalisé, d'effectuer des mesures biométriques sur le geste du signataire, qui peuvent être vérifiées de deux manières :

- soit au moment de la réalisation de la signature, par comparaison avec une base préétablie de signatures « dynamiques » ;
- soit, *a posteriori*, en comparant avec un nouvel acte de signature provenant du même signataire.

Ces éléments biométriques peuvent concourir à l'établissement de la fiabilité du procédé d'identification du signataire, et ainsi venir renforcer la qualité de la signature électronique réalisée. Toutefois, ils ne sont pas encore suffisants aujourd'hui en France pour constituer à eux seuls une signature électronique, faute de savoir établir un « lien garanti » avec le document signé.

Mais bien entendu, la recherche sur ce sujet est loin d'être close !

Laissons un fournisseur de solutions préciser quelques cas d'usage de la signature sur tablette graphique, en particulier dans d'autres pays européens.

Parole d'expert

Thomas Kaeb, directeur du développement Europe du Sud, Wacom Europe GmbH

Pour la capture de signatures biométriques, quelles sont les fonctions des tablettes Wacom ?

Depuis 2008, Wacom évolue sur le marché de la signature électronique manuscrite, devenant le premier fabricant de tablettes de signature au monde. En incorporant des données biométriques dans les signatures, nous avons fait progresser la technologie d'un cran, fournissant aux utilisateurs de nos produits une défense

Copyright © 2012 Eyrolles.

optimale et efficace contre la fraude. Plus de 100 000 tablettes de signature de la gamme STU vendues au cours des trois derniers trimestres 2011 assurent la position de premier plan de Wacom sur le marché de la signature électronique. Des organisations comme IKEA, Banca Intesa Sanpaolo, presque toutes les banques d'épargne espagnoles, Lloyds TSB, O2, T-Mobile, Hilton et l'autorité berlinoise chargée de la citoyenneté et des affaires réglementaires, utilisent maintenant les solutions de capture de signature de Wacom pour des flux de travail sans papier.

Basées sur la technologie de résonance électromagnétique (EMR), les tablettes de signature de Wacom sont capables de capturer les signaux statiques et biométriques des signatures individuelles, rendant la falsification extrêmement difficile. Quand un utilisateur signe sur l'écran, toutes les tablettes signature Wacom enregistrent la pression, la vitesse, l'accélération, le rythme et le mouvement lors du processus de signature, ainsi que la position XY physique du stylet. Ces paramètres serviront à créer un profil biométrique individuel de chaque signataire. Même si de temps en temps l'image d'une signature peut changer légèrement, le profil de signature biométrique reste le même. Il en résulte une caractéristique unique qui permet d'identifier et d'authentifier clairement les signatures.

Quel avenir prévoyez-vous pour la signature électronique biométrique ?

Nous évaluons le marché depuis un bon moment déjà, et nous avons l'impression que la signature électronique manuscrite devient monnaie courante en Europe. La principale raison pour l'implémentation d'une nouvelle technologie est l'amélioration du traitement des documents pour gagner du temps et faire des économies, en réduisant les documents papier. Nous constatons déjà que l'acceptation de la signature électronique augmente rapidement, au niveau professionnel comme au niveau de la clientèle. Cependant, les sociétés et établissements intégrant une tablette de signature Wacom dans leur flux de travail ne font pas tous usage de la possibilité de capturer également des données biométriques.

Mais dans le secteur de la banque et de la finance en particulier, où il est crucial d'avoir un niveau élevé d'efficience et de sécurité, la signature biométrique devient presque la norme en Europe. Lors de la signature sur une tablette de signature Wacom, un enregistrement de données biométriques individuelles et uniques est généré pour la signature, contenant bien plus d'informations qu'une signature analogique. Le profil biométrique peut servir à identifier clairement un signataire, car désormais l'immuabilité d'un document signé peut être garantie par logiciel. Ainsi, la signature biométrique est utilisable lors d'activités professionnelles dans de nombreux cas et pour un grand nombre de transactions différentes. La vision de Wacom est de développer de nouvelles technologies pour répondre aux besoins changeants du plus grand nombre d'applications possible, en considérant la signature biométrique comme une caractéristique importante et nécessaire de nos produits dans le proche avenir. Ce n'est qu'un début.

Copyright © 2012 Eyrolles.

Copyright © 2012 Eyrolles.

Chapitre 9

Le cachet et les autres formes de signatures

L'ambiguïté du terme « signature électronique »

Dans le présent ouvrage, nous avons systématiquement limité l'usage du terme « signature électronique » à son sens juridique français : consentement d'une personne physique aux termes d'un document.

Toutefois, le même mécanisme technique (calcul de hash, puis calcul RSA à l'aide de la clé privée) est couramment appelé « signature électronique », même lorsqu'il est utilisé dans d'autres contextes : nous avons préféré employer dans ces cas le terme de « scellement ».

Nous allons développer dans ce chapitre les autres usages du mécanisme technique de signature/scellement afin d'évoquer des cas d'utilisation très répandus de la cryptographie asymétrique.

La signature de personne morale : le cachet

La signature électronique d'une personne morale, si elle est possible au sens de la directive européenne de 1999, est explicitement exclue dans le droit français par le décret du 30 mars 2001.

De ce fait, et parce qu'elle est très fréquemment nécessaire dans les services dématérialisés, le RGS a introduit la notion de « cachet ». Il s'agit, du point de vue technique, de la même chose que la signature électronique, mais le cachet s'appuie sur un certificat qui désigne une personne morale (l'entreprise, la collectivité publique…), ou, de manière plus restrictive, un serveur applicatif particulier exploité par cette personne morale : dans ce cas, on parle parfois de « cachet serveur » .

Copyright © 2012 Eyrolles.

Le cachet est souvent apposé sur les documents de manière automatique, dans le cadre de l'exécution d'un service. Voyons un exemple d'utilisation du cachet dans un téléservice de l'administration.

Le téléservice Réseaux et canalisations de l'Ineris

Dans le cadre de ce téléservice, les exploitants de réseaux terrestres, aériens et subaquatiques ont l'obligation de déclarer leurs ouvrages auprès de l'Ineris afin de simplifier les déclarations préalables aux travaux.

La déclaration d'un ouvrage donne lieu à la signature d'un procès-verbal attestant de la bonne prise en compte de la déclaration par le téléservice. Le procès-verbal est généré automatiquement par la plate-forme au format PDF. La plate-forme y appose tout d'abord un cachet serveur, sous la forme d'une signature de « certification » selon la norme PAdES. Le document ainsi certifié est ensuite présenté à l'exploitant de réseau, qui y appose à son tour sa signature électronique, à l'aide d'un certificat de signature de niveau RGS (**) ou supérieur.

Ainsi, le procès-verbal est synallagmatique : les deux parties s'engagent simultanément sur les mêmes termes. L'engagement du téléservice est de mettre en ligne les données remises par l'exploitant de réseau ; l'engagement de l'exploitant de réseau est d'avoir vérifié que les données qu'il avait remises, et qui ont été retraitées par le téléservice, sont bien conformes à ce qu'il souhaitait déclarer.

Un autre exemple d'usage du cachet est la dématérialisation des factures. Dans ce cas d'usage particulier, il est précisé par le Code général des impôts que la signature est destinée non à un engagement du signataire (d'ailleurs, les factures papier ne sont pas signées), mais à garantir l'origine et l'intégrité du contenu de la facture. Il s'agit donc d'un usage du mécanisme technique de signature à des fins fonctionnelles, qui sera avantageusement réalisé sous la forme d'un cachet.

Code général des impôts – Article 289 V

Les factures peuvent, sous réserve de l'acceptation du destinataire, être transmises par voie électronique dès lors que l'authenticité de leur origine et l'intégrité de leur contenu sont garanties au moyen d'une signature électronique.

De nombreux acteurs du marché envoient donc des factures dématérialisées sous la forme d'un fichier PDF comprenant une signature au format PAdES, ce qui est tout à fait conforme au CGI.

Au-delà des exigences juridiques, dans un but d'interopérabilité des opérateurs de dématérialisation de facture, GSI FRANCE a publié des « Recommandations pour l'échange de factures dématérialisées fiscalement » et un cahier des charges correspondant, en vue de l'attribution d'un label. Ce référentiel est beaucoup plus exigeant que le CGI :

- les factures doivent être au format PDF/A-1 ;
- les données de facturation doivent y être jointes en XML ;

Copyright © 2012 Eyrolles.

- le cachet réalisé doit être de type XAdES-BES enveloppante (c'est-à-dire que le PDF et le XML des données de facturation sont inclus dans le fichier de signature, et que l'horodatage et l'inclusion d'une preuve de validité du certificat sont optionnels).

Les autres usages du mécanisme technique de « signature »

Le mécanisme technique de signature électronique offre plusieurs propriétés intéressantes du point de vue fonctionnel :

- il garantit l'intégrité des données signées : toute modification ultérieure de ces données rend la signature invalide ;
- il garantit la provenance des données, grâce à l'identité contenue dans le certificat.

Nous allons maintenant évoquer plusieurs cas d'usage de ce mécanisme.

Le scellement de code exécutable

Afin de réduire le risque lié à l'exécution de certains programmes sur les ordinateurs des utilisateurs, il est possible de les sceller à l'aide d'une « signature » de l'éditeur afin de garantir leur provenance et leur intégrité.

Ainsi, les applets Java, qui sont téléchargées *via* Internet dans le but de s'exécuter sur le poste de l'internaute, ont des possibilités très limitées quand elles ne sont pas scellées. Elles ne peuvent s'exécuter que dans le « bac à sable », c'est-à-dire qu'elles ne disposent pas de la possibilité d'accéder au disque dur en lecture ni en écriture, ni de la possibilité de déclencher l'exécution d'autres programmes sur l'ordinateur.

En revanche, si elles sont scellées à l'aide d'une signature valide, réalisée par un certificat « de confiance » au sens du magasin de certificats de Java, elles disposent alors de capacités bien plus étendues. Par exemple, elles sont fréquemment utilisées, pour réaliser des signatures électroniques dans le cadre des téléservices ! Au lieu d'exiger de l'utilisateur qu'il dispose d'un logiciel de signature électronique, le service inclut cet outil sous la forme d'une applet Java scellée, qui a tout loisir d'accéder aux fichiers à signer et de faire appel au support cryptographique du certificat.

Nous avons déjà vu dans le chapitre 5 abordant la chaîne des modules cryptographiques (voir figure 5-8) que les logiciels de sécurité appelés « CSP », ou *Cryptographic Service Providers*, doivent être scellés par Microsoft pour pouvoir être employés dans les environnements Windows : cette précaution évite les risques d'attaque de type *man in the middle* que nous avons décrites pour le standard alternatif, PKCS#11.

Copyright © 2012 Eyrolles.

Le scellement d'un certificat

Nous avons décrit la chaîne de la certification comme une série de certificats, chacun étant scellé par celui du niveau supérieur. Ce scellement est, du point de vue technique, une signature électronique qui permet de garantir la provenance du certificat (il est émis par l'autorité de certification qui l'a signé) et son intégrité. Ainsi, les certificats racine, qui réalisent leur propre scellement, sont appelés « autosignés ».

Le scellement des éléments techniques de preuve : horodatage, LCR, OCSP

De la même manière qu'elle scelle les certificats qu'elle émet, l'autorité de certification scelle la liste de certificats révoqués qu'elle publie. Il est ainsi impossible d'ajouter, de retirer ou de modifier les numéros de série inclus dans cette liste ou les dates de révocation correspondantes.

Il en va de même des réponses données par l'autorité de validation au travers du protocole de contrôle de validité de certificat OCSP : le jeton envoyé en réponse, qu'il atteste de la validité du certificat ou de son invalidité, comporte un scellement sous la forme technique d'une signature électronique.

Enfin, les autorités d'horodatage procèdent de manière identique au scellement des jetons d'horodatage (ou « contremarques de temps ») qui attestent de l'existence d'une donnée à un moment précis. Nous détaillerons ce format dans le chapitre 11 consacré à la traçabilité.

Le scellement des traces applicatives

Nous verrons dans le chapitre 11 sur la traçabilité qu'il peut être nécessaire de garantir l'intégrité des traces réalisées par une application, de manière à leur donner une force probante, dans le respect de l'article 1316-1 du Code civil qui dispose que « l'écrit sous forme électronique est admis en preuve au même titre que l'écrit sur support papier, sous réserve que puisse être dûment identifiée la personne dont il émane et qu'il soit établi et conservé dans des conditions de nature à en garantir l'intégrité ».

Le scellement offert par une signature technique, de type cachet, réalisé à l'aide d'un certificat au nom d'une machine ou d'une application, permet de garantir la provenance et l'intégrité de la trace réalisée, dès sa création et au fil du temps.

Le mécanisme technique de signature électronique est donc un outil fondamental de la traçabilité.

Copyright © 2012 Eyrolles.

L'authentification forte

Nous avons vu au chapitre 4 traitant de l'authentification par certificat que son fonctionnement est analogue à celui de la signature électronique : l'utilisateur reçoit un « défi », c'est-à-dire une valeur aléatoire, en réalise le hash et effectue un calcul RSA sur ce hash à l'aide de sa clé privée.

Ainsi, une authentification forte est l'équivalent technique d'une signature – mais pas son équivalent juridique, puisque l'objectif n'est que de prouver son identité pour gagner le droit d'accès à un service, et non de s'engager sur les termes d'un document.

Il convient d'ailleurs d'être prudent dans la mise en œuvre de l'authentification par certificat : si l'aléa était remplacé par un document, il y aurait un risque de signer à son insu ledit document !

C'est pourquoi il est souhaitable de dissocier les fonctions de signature électronique et d'authentification dans deux certificats différents.

Copyright © 2012 Eyrolles.

Copyright © 2012 Eyrolles.

Chapitre 10

Définir son besoin et choisir un outil de signature électronique

Déterminer le contexte du service

Lorsque l'on conçoit un service dématérialisé qui nécessite la génération et/ou l'échange de documents signés, il convient de bien choisir le mode de réalisation des signatures électroniques en fonction du contexte du service.

Ce mode de réalisation concerne deux éléments, qu'il est important de dissocier, et qui sont tous deux indispensables à la réalisation d'une signature électronique :

- **le certificat et la clé privée associée,** et leur procédure de distribution au signataire ;
- **le logiciel employé pour réaliser la signature :** c'est lui qui réalise le calcul du hash, l'algorithme RSA (sauf s'il est effectué directement dans la puce), la mise en forme de la signature (format PAdES, XAdES ou CAdES), et l'inclusion de l'horodatage et de la preuve de validité du certificat obtenus auprès des tiers de confiance.

Pour réaliser une signature électronique, le signataire doit disposer de sa clé privée, de son certificat et d'un logiciel de signature qui fait appel à ces éléments.

La détermination de ces éléments dépend de plusieurs critères.

- Existe-t-il des dispositions légales contraignantes ?
- Qui sont les signataires ? Y a-t-il vis-à-vis d'eux des contraintes budgétaires, organisationnelles, techniques ?
- Les documents à signer proviennent-ils du service même ou de l'extérieur ?

Il est important de noter que la signature électronique ne comporte pas l'indication de l'outil qui a été utilisé pour la réaliser, mais seulement celle du certificat à employer pour la vérifier.

Copyright © 2012 Eyrolles.

Nous allons maintenant décrire différentes solutions, en présentant leurs avantages et leurs contraintes afin de déterminer leur contexte d'utilisation optimal, et en les illustrant avec des exemples concrets de projets dans lesquels elles ont été choisies.

Les différentes façons de réaliser des signatures électroniques

L'outil autonome de signature électronique

La première solution pour faire réaliser des signatures électroniques à des utilisateurs consiste à ce que chacun des signataires potentiels installe sur son poste de travail un logiciel de signature électronique, et acquière un certificat, soit qu'il l'achète auprès d'un prestataire de services de certification électronique, soit qu'il le génère lui-même, si le contexte juridique du service permet un niveau de sécurité très faible sur la vérification de l'identité du signataire.

La figure 10-1 représente ce cas d'usage : tout le nécessaire à la réalisation de la signature (logiciel et certificat) se trouve sur le poste du signataire, la plate-forme ne comprenant que les outils de vérification de signature.

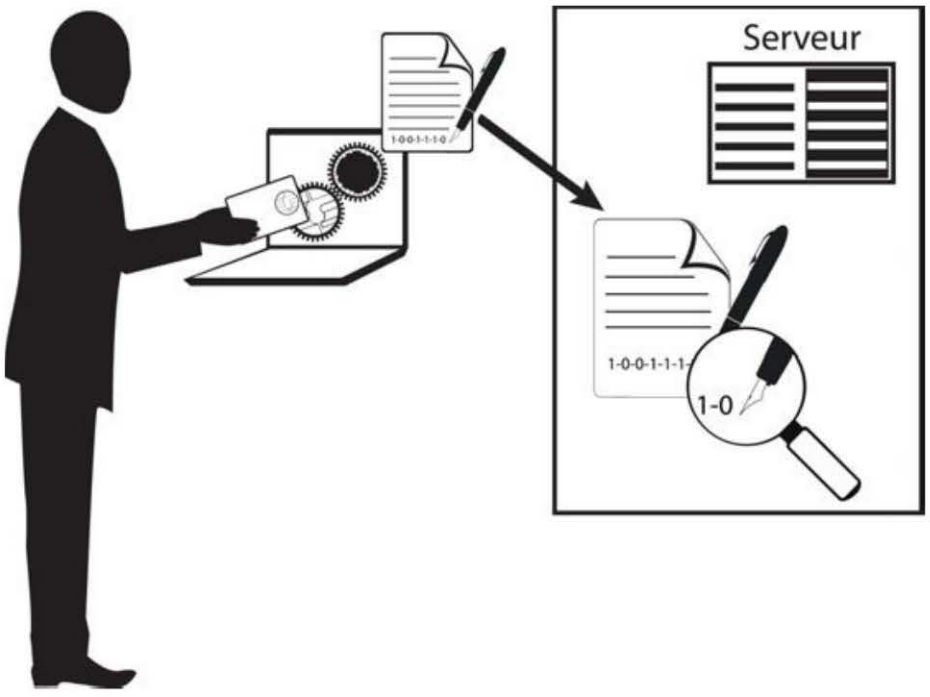


Figure 10-1 : L'outil autonome de signature électronique

Copyright © 2012 Eyrolles.

Cette solution nécessite soit des utilisateurs aguerris et capables de se procurer par eux-mêmes un outil de signature électronique, soit un contexte contrôlé, dans lequel l'entreprise installe ce logiciel sur le poste de ses collaborateurs.

Les documents signés par l'utilisateur de manière autonome sont, dans le processus métier, transmis à la plate-forme pour y être vérifiés, stockés, réacheminés… Se pose alors la question du format de signature électronique. Lorsqu'un service dématérialisé laisse aux utilisateurs le soin de choisir un outil, il doit :

- soit imposer un ou plusieurs formats de signature, les utilisateurs ayant la responsabilité de choisir un outil capable de produire le format demandé ;
- soit être capable de vérifier et d'accepter tous les formats de signature. La question de l'horodatage des signatures et de l'inclusion d'une preuve de validité du certificat se posera alors également.

Ce modèle est donc plus aisé à mettre en œuvre dans un contexte maîtrisé que dans un contexte de liberté de choix. Illustrons-le par trois cas pratiques.

Exemple 1

Un premier exemple est la signature électronique des experts-comptables : Signexpert. Le Conseil supérieur de l'ordre des experts-comptables a mis à disposition de l'ensemble de la profession non seulement des certificats de signature électronique, permettant l'authentification forte pour accéder aux services qui leur sont utiles, mais également un outil de signature électronique à installer sur leur poste de travail. Ainsi, bien que l'on soit dans un modèle de complète autonomie du signataire, les formats et la chaîne de la confiance sont sous contrôle.

Exemple 2

Un deuxième exemple d'outil correspondant à ce modèle est la suite bureautique Microsoft Office : ces logiciels incluent nativement une fonction de signature électronique et permettent même à l'utilisateur de se fabriquer un certificat de signature autosigné. Nous sommes là dans un exemple d'usage entièrement libre par l'utilisateur. Toutefois, le certificat généré ainsi est purement déclaratif, et ne correspond à aucune politique de certification (l'utilisateur a bien entendu la possibilité d'employer un certificat acheté auprès d'un PSCE).

Toutefois, lorsque le document Word signé est ouvert avec un autre logiciel « compatible » tel que OpenOffice.org, ce dernier, bien qu'il inclue lui aussi des fonctions de signature électronique, ne sait pas interpréter les signatures apposées par Word : le document apparaît alors comme non signé. Il y a donc un réel risque d'interopérabilité sur ces signatures.

Copyright © 2012 Eyrolles.

Exemple 3

Enfin, un troisième exemple porte sur le format PDF : bien que le logiciel Adobe Reader, installé sur la plupart des ordinateurs pour visualiser les PDF, n'offre pas par défaut la possibilité de signer des documents, cette faculté existe à condition que le droit en ait été donné par la personne qui a généré le document. Si le service dématérialisé génère des documents PDF en activant l'option de signature, les utilisateurs du service pourront, sans autre outil qu'Adobe Reader, apposer leur signature dans le champ prévu à cet effet. Ils devront pour cela disposer d'un certificat acheté auprès d'un PSCE.

Nous allons maintenant voir comment permettre à un utilisateur de réaliser une signature sans disposer sur son poste d'un outil de signature.

La signature par applet Java

Dans le but de simplifier l'usage de la signature électronique aux utilisateurs d'un service et de contrôler le contexte de sa réalisation, il est pratique d'inclure dans le service l'outil de signature électronique.

Toutefois, pour que le signataire conserve son moyen de signature sous son contrôle exclusif, il est préférable que le logiciel de signature, qui fait appel au support cryptographique, s'exécute sur le poste du signataire.

La façon de réaliser cela consiste à inclure dans les pages du service un programme exécutable qui se télécharge et s'exécute automatiquement sur le poste des utilisateurs : c'est ce que l'on appelle une « applet ». Le langage le plus fréquemment employé pour développer des applets est Java, d'où le terme fréquent d'« applet Java ».

Le fonctionnement est alors le suivant, illustré par la figure 10-2.

- Lorsque, dans le processus métier, l'utilisateur doit réaliser une signature électronique, l'applet est automatiquement téléchargée depuis le serveur et s'exécute sur son poste.
- L'applet accède automatiquement au certificat de l'utilisateur et peut même, s'il en a plusieurs, sélectionner celui ou ceux qui sont acceptés dans la politique de signature électronique du service.
- L'applet offre en général la possibilité de visualiser le ou les documents à signer.
- Lorsqu'il confirme sa volonté de signer, l'utilisateur est invité à saisir son code PIN, ce qui permet à l'applet de faire appel au support cryptographique contenant la clé privée de l'utilisateur.

Dans notre description, nous avons supposé que le signataire disposait d'un certificat acheté auprès d'un PSCE.

Copyright © 2012 Eyrolles.

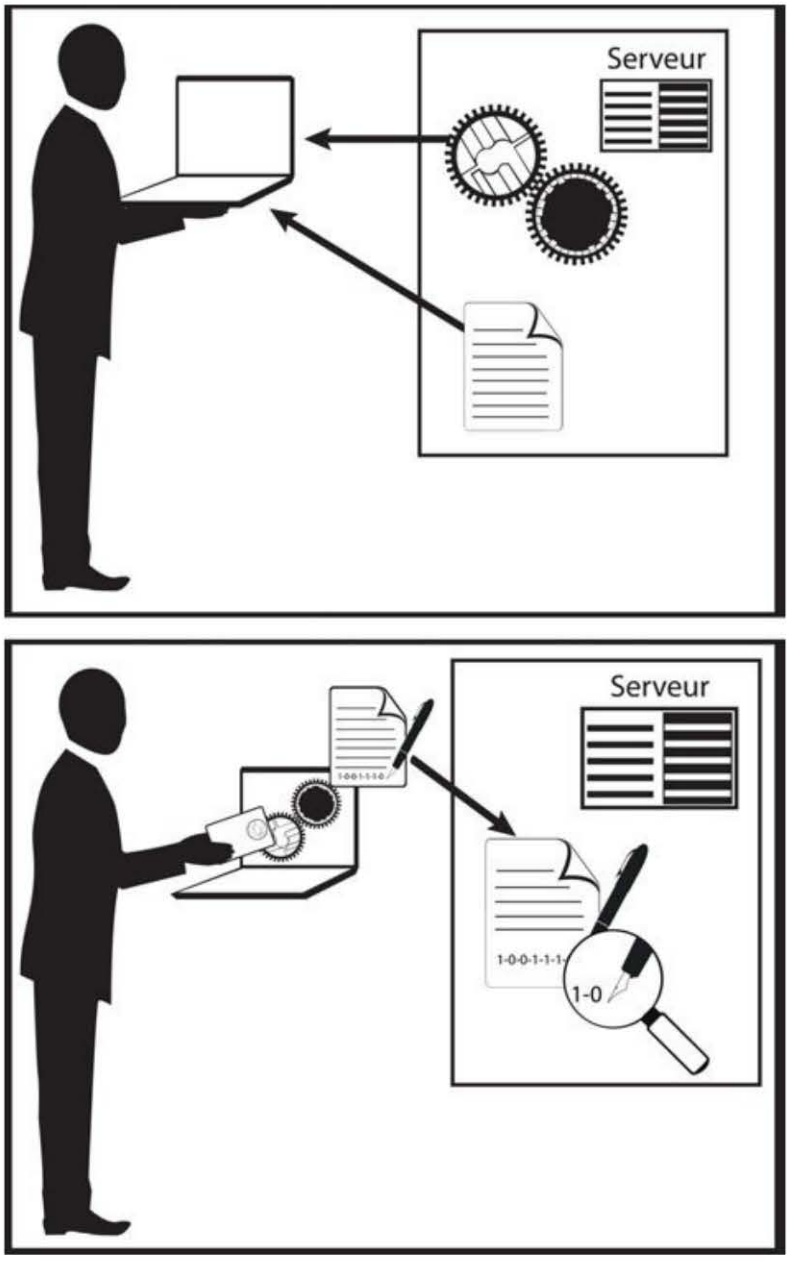


Figure 10-2 : La signature électronique par applet Java

Nous pouvons citer de nombreux exemples de plates-formes de dématérialisation offrant la signature électronique sous cette forme.

Exemple 1

La plate-forme Achatpublic.com de dématérialisation des marchés publics : le soumissionnaire constitue ses enveloppes à partir des fichiers qu'il a créés sur son poste de travail, et choisit ceux qu'il souhaite signer,

Copyright © 2012 Eyrolles.

quel que soit leur format. Le soumissionnaire achète auprès d'un PSCE un certificat référencé par l'administration. L'applet inclut automatiquement dans la signature électronique un jeton d'horodatage et une preuve de validité du certificat OCSP. Les signatures sont au format CAdES.

Exemple 2

Le téléservice Réseaux et canalisations de l'Ineris : l'exploitant de réseau qui déclare ses ouvrages doit signer un procès-verbal qui est automatiquement généré par l'application au format PDF avant de lui être présenté. Il emploie un certificat acheté auprès d'un PSCE référencé par l'Ineris. L'applet inclut automatiquement dans la signature électronique un jeton d'horodatage et la LCR correspondant au certificat. Les signatures sont au format PAdES.

Exemple 3

Le parapheur électronique de la région Limousin : lorsqu'une application dématérialisée de la région a besoin de faire signer un document par un agent de la région (par exemple, le président), elle dépose ce document dans le parapheur. Le signataire en est averti. Il accède alors au parapheur au moment où cela lui convient, et effectue au travers de l'applet du parapheur la visualisation des documents qui lui sont soumis, puis leur signature à l'aide de son certificat acquis auprès d'un PSCE, ou leur rejet s'il décide de ne pas signer.

Dans certains cas, il serait difficile d'exiger des utilisateurs qu'ils achètent dans le commerce un certificat de signature, pour des raisons de coût, de délai d'obtention ou de complexité de la procédure. Nous allons citer deux exemples de services qui ont opté pour la signature électronique par applet, tout en fournissant préalablement aux utilisateurs un certificat de signature.

Exemple 4

La première version du service de télédéclaration de l'impôt sur le revenu, Télé IR, pour établir le parallèle avec une déclaration papier, exigeait une signature électronique de la part du déclarant. Il aurait été irréaliste de faire acheter à chaque citoyen un certificat de signature pour ce seul usage. C'est pourquoi la Direction générale des finances publiques a opté pour la remise gratuite d'un certificat, sous forme logicielle, à chaque télédéclarant. La première étape de la procédure consistait donc à obtenir son certificat, en indiquant son revenu fiscal de référence de l'année précédente pour prouver son identité. Puis, une fois le certificat obtenu, il était utilisé pour signer la déclaration de revenus au travers d'une applet.

Copyright © 2012 Eyrolles.

Exemple 5

La Banque Casino a réalisé un essai de souscription de crédit à la consommation entièrement dématérialisé. Dans ce service, les prospects souhaitant souscrire le crédit fournissaient, outre leurs justificatifs financiers, un scan de leurs papiers d'identité qui permettait, après vérification par un agent, de leur délivrer, entièrement à distance, un certificat sous forme logicielle. (Ce processus correspond à la classe 2 que nous avons vue dans le chapitre 5 sur les certificats.) Le prospect pouvait alors signer son contrat de crédit à la consommation au travers d'une applet, et devenir client sans avoir eu à se déplacer ou à échanger du papier avec la banque.

Nous allons maintenant voir comment permettre à un utilisateur de réaliser une signature électronique sans disposer d'un outil de signature… et sans disposer d'un certificat !

La signature électronique « à la volée »

Ce troisième procédé de signature électronique, que l'on pourrait appeler aussi « signature avec un moyen d'authentification », permet à un service dématérialisé de réaliser une signature électronique au nom d'un utilisateur, à la demande de celui-ci, sans que le signataire ait besoin de disposer sur son poste de travail d'un certificat ou d'un logiciel.

Les étapes de réalisation d'une telle signature électronique, reprises dans la figure 10-3, sont les suivantes :

- l'utilisateur visualise le document et manifeste sa volonté de le signer ;
- il s'authentifie afin de valider sa demande de signature (il existe de nombreuses façons de réaliser cette authentification, au travers de ce que l'on appelle le « protocole de consentement ») ;
- le service génère une clé privée et un certificat au nom du signataire, réalise la signature électronique, puis efface la clé privée ;
- l'utilisateur est informé que sa signature a bien été réalisée et, si besoin, peut accéder au document signé.

La signature électronique étant définie par le Code civil comme « l'usage d'un procédé fiable d'authentification garantissant son lien avec l'acte auquel il s'attache », la valeur juridique des signatures électroniques réalisées selon le processus « à la volée » dépendra principalement de la fiabilité du protocole de consentement.

Il peut être suffisant de mettre en œuvre une authentification par un simple mot de passe, pourvu que celui-ci ait été choisi par l'utilisateur et placé explicitement sous son contrôle au sein de la convention de preuve, comme nous le verrons au chapitre 13.

Il est également possible de renforcer cette authentification en utilisant un second canal, comme l'envoi d'un code par SMS ou par e-mail.

Copyright © 2012 Eyrolles.

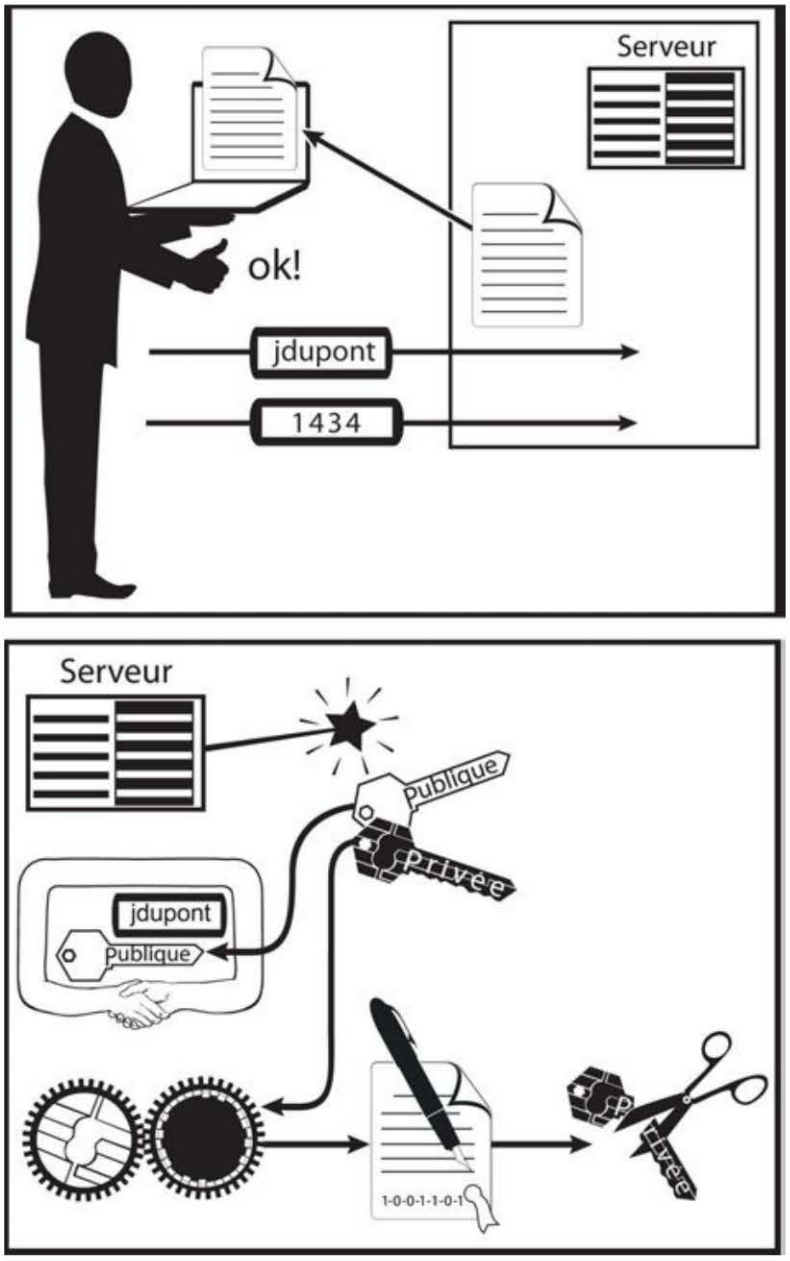


Figure 10-3 : La signature électronique à la volée

Nous allons illustrer les cas d'usage de la signature électronique « à la volée » par quelques cas pratiques d'utilisation dans des services dématérialisés.

Exemple 1

Nous avons déjà vu dans la section précédente sur la signature électronique par applet Java que la région Limousin a mis en œuvre un parapheur électronique pour son usage interne. Il n'était toutefois pas possible, dans le cadre des services dématérialisés (par exemple, les demandes d'aides à

Copyright © 2012 Eyrolles.

la région), de demander aux citoyens d'acheter un certificat de signature, car la complexité et le coût de l'opération les auraient conduits à effectuer leurs démarches par la voie papier. La région a donc opté pour la signature électronique à la volée des demandes d'aides : même si la création de compte est déclarative, le risque d'usurpation d'identité est très faible, puisque personne n'a intérêt à demander une aide financière pour un tiers.

Exemple 2

La société Sogelink exploite le service DICT.fr de dématérialisation des démarches déclaratives préalables aux chantiers. L'évolution de la législation ayant entraîné une obligation de signature des documents échangés par la plate-forme, Sogelink a fait le choix de se positionner en tant que tiers de confiance pour simplifier les procédures de ses clients. Le mot de passe qui servait auparavant à valider les déclarations peut maintenant également être employé pour réaliser une signature électronique à la volée. Le but recherché était d'une part la conformité à la législation, et d'autre part la fidélisation de la clientèle, grâce à un allègement des contraintes liées à l'acquisition des certificats.

Exemple 3

Le service e-attestations a pour fonction la dématérialisation des justificatifs dans le cadre de l'exécution des marchés, publics et privés. La société qui offre le service a fait le choix de s'appuyer sur un prestataire de services de confiance pour inclure dans e-attestations la signature à la volée. Ainsi, au lieu de vérifier elle-même le protocole de consentement, e-attestations a confié cette vérification au tiers de confiance, qui effectue également sur sa plate-forme la génération du certificat, la réalisation de la signature, puis l'effacement de la clé privée. L'objectif de ce choix était d'une part de simplifier les démarches des entreprises, et d'autre part de reporter la responsabilité juridique de la signature électronique sur un professionnel du domaine.

Exemple 4

Plusieurs opérateurs de télécommunication ont mis en œuvre un dispositif de signature en agence de contrats dématérialisés à l'aide d'un terminal muni d'une tablette graphique : le vendeur vérifie la carte d'identité du client et remplit un formulaire avec son identité (c'est la phase d'enregistrement du cycle de vie du certificat), puis le client effectue une signature manuscrite sur la tablette graphique. Cette signature est incluse dans le contrat, puis un certificat est généré au nom du client, téléchargé sur le terminal, et utilisé pour effectuer une signature électronique sur le contrat incluant la signature manuscrite. Ce certificat est créé avec une durée de vie courte, et la clé privée correspondante est effacée dès que la signature a été réalisée.

Copyright © 2012 Eyrolles.

Pour aller encore plus loin dans la simplification, nous allons maintenant voir comment recueillir l'assentiment d'un utilisateur sans avoir besoin de réaliser de signature électronique.

Une alternative à la signature électronique : la traçabilité

La signature a pour but de manifester le consentement du signataire aux termes du document qu'il signe.

Une autre façon de procéder pour recueillir ce consentement peut être la suivante :

- le service présente le document à l'utilisateur ;
- l'utilisateur indique son acceptation des termes du document, par exemple en cochant une case et en saisissant son mot de passe pour prouver son identité ;
- le service effectue alors une trace de l'action, comportant l'identité de l'utilisateur, le moment du consentement, le moyen employé pour s'authentifier et un scellement de l'ensemble de ces informations par un cachet.

Nous verrons dans le chapitre 11 consacré à la traçabilité que, moyennant la rédaction d'une convention de preuve adéquate, ce procédé, dénué de signature à proprement parler, peut offrir une preuve suffisante de l'engagement de l'utilisateur.

Illustrons cette procédure par deux cas pratiques.

Exemple 1

De nombreux services utilisent une traçabilité de ce type pour conserver la trace de la validation par les utilisateurs des conditions générales d'utilisation (CGU). Bien que cette étape soit souvent un passage obligé avant d'accéder au service, il importe d'en effectuer une traçabilité renforcée afin d'éviter toute contestation. Ainsi, la traçabilité comportera bien l'identification du signataire, la date et l'heure de l'action, le type d'action (validation des CGU), et les éléments d'identification du document de CGU qui a été présenté à l'utilisateur : titre, numéro de version, hash, voire identifiant unique au sein du système d'archivage électronique.

Exemple 2

Au sein du téléservice Réseaux et canalisations de l'Ineris, les collectivités publiques peuvent déclarer leurs réseaux (assainissement, éclairage public…) soit par voie dématérialisée, avec signature électronique, soit *via* un envoi papier, avec une signature manuscrite. En cas d'erreur dans leur déclaration, la possibilité d'annuler la mise à jour de la base de données leur est offerte. Les collectivités qui ont opté pour la voie dématérialisée peuvent ainsi signer de manière électronique un procès-verbal

Copyright © 2012 Eyrolles.

d'annulation. En revanche, pour celles qui ont choisi la voie papier, il serait trop long d'attendre la réception d'une annulation papier, car l'ouvrage erroné risquerait d'être mis en ligne avant le traitement du dossier. C'est pourquoi une procédure d'annulation dématérialisée a été mise en œuvre, avec un processus de traçabilité de l'annulation comme alternative à la signature électronique.

La quatrième partie de cet ouvrage, consacrée à la traçabilité, va nous permettre de détailler les mécanismes mis en œuvre pour constituer des traces, leur donner de la valeur et les utiliser à bon escient.

Copyright © 2012 Eyrolles.

Copyright © 2012 Eyrolles.

PARTIE 4

Tracer, conserver et certifier les données



Copyright © 2012 Eyrolles.

Copyright © 2012 Eyrolles.

Chapitre 11

La traçabilité

La traçabilité, définition et usages

Définition de la traçabilité

La traçabilité au sens des systèmes d'information

Lorsqu'on parle de traçabilité dans la vie courante, c'est en général pour évoquer le suivi de la chaîne de production, de transport et de distribution des produits agroalimentaires ou des médicaments, voire les flux migratoires des personnes.

Au sein d'un système d'information ou d'un service dématérialisé, ce n'est évidemment pas cette notion qui doit être entendue par le terme « traçabilité », mais plutôt le suivi du cycle de vie des informations et des actions effectuées par les utilisateurs.

La traçabilité au sein d'un système d'information sera ainsi la capacité à suivre ou à reconstruire un historique fidèle des événements qui se sont déroulés au sein de ce système.

Les traces seront structurées de manière à conserver les informations suivantes :

- Qui ?
- Quoi ?
- Quand ?

Le « Qui ? » désignera, selon les cas, un utilisateur humain ou un module technique constitutif du système.

Le triptyque « qui, quoi, quand » est le fondement de la traçabilité.

Le « Quoi ? » comportera les informations sur l'événement qui s'est déroulé : l'action en elle-même, mais aussi les éléments de contexte indispensables à l'interprétation ultérieure de la trace. Ainsi, l'action d'envoi d'un document devra inclure non seulement le type d'action « envoi de

Copyright © 2012 Eyrolles.

document », mais aussi les informations sur l'émetteur, le destinataire, le document envoyé, voire les modalités d'envoi (par e-mail, par mise à disposition sur une plate-forme de téléchargement, par fax, par courrier rematérialisé *via* un prestataire tiers…).

Le « Quand ? » désigne bien entendu la date de l'action. Nous verrons dans la section de ce chapitre consacrée à l'horodatage qu'il existe plusieurs solutions techniques pour fixer la date et l'heure des événements.

Que doit-on inclure dans la traçabilité ?

En fonction du service offert et de l'intérêt qu'il y a à conserver les traces des différents événements, la traçabilité pourra porter sur des événements de natures différentes, comme nous allons l'illustrer ici.

- **L'état d'un document** peut, par exemple, passer de la valeur « créé » ou « en cours de rédaction » à la valeur « à valider », puis lors d'étapes ultérieures à « rejeté » ou « validé », puis à « signé », « envoyé », « reçu », voire « non reçu » : la traçabilité sur le cycle de vie d'un document dépendra des étapes de sa constitution et de son échange.
- **Les actions d'un utilisateur** peuvent être tracées dans le but de suivre son activité sur un service : on pourra, par exemple, avoir des traces pour la création de compte, la validation des conditions générales d'utilisation, la souscription à tel ou tel service, une demande effectuée auprès du fournisseur de services, le dépôt d'un document, la réception d'une réponse, mais aussi le changement de mot de passe ou les évolutions des données personnelles.
- **Les actions automatiquement réalisées par le système**, comme la génération d'un document récapitulatif, l'envoi d'un accusé de réception, l'archivage d'un dossier, l'envoi d'un e-mail d'information, la vérification d'une donnée relative à l'utilisateur dans le but de lui accorder ou non un service (par exemple, le solde de son compte bancaire).
- **Les actions d'administration technique**, qui peuvent être considérées comme des actions d'utilisateurs ayant un statut particulier, mais aussi comme des procédures à part : mise à jour du système, sauvegarde, restauration, redémarrage, etc.

Cette liste n'est pas exhaustive ; en fonction du contexte, les éléments qui peuvent être tracés devront être déterminés en suivant la méthodologie que nous détaillerons plus loin dans la section « Inclure la traçabilité dans son projet ».

Traçabilité et données métier

Nous avons vu dans la liste précédente que certaines données de traçabilité sont en étroite corrélation avec les données « métier » gérées par la plate-forme : par exemple, sur un service de demande d'aides comme

Copyright © 2012 Eyrolles.

réalisé dans la plate-forme Planet Limousin, les états successifs d'un dossier seront constitués par les différentes actions des utilisateurs :

- lors de la constitution du dossier, il est à l'état « créé » ;
- lorsque les pièces justificatives à joindre ont été fournies, il est à l'état « complet » ;
- lorsqu'il a été instruit par un agent de la région, il est à l'état « instruit », ou éventuellement « en attente de compléments » ;
- lorsqu'il a été validé par un décideur, il passe à l'état « validé » ;
- lorsque le président de région l'a signé, il devient « attribué » ;
- et ainsi de suite au fur et à mesure de la libération des fonds d'aide, jusqu'à l'état « archivé » en fin de vie.

La traçabilité ne contiendra pas l'ensemble des données métier relatives au dossier. Le contenu des pièces jointes, le détail du projet, la justification des décisions pourront ne pas en faire partie.

En revanche, les éléments clés y figureront : l'identité du demandeur, le nom du projet qu'il présente, l'identité des agents qui ont réalisé les traitements, la liste des étapes…

Ce qui distinguera, au sein du service dématérialisé, les données métier des données de traçabilité, c'est l'usage auquel elles sont destinées.

Données métier ou données de traçabilité : la différence réside principalement dans l'usage qui en est fait.

Ainsi, la base de données métier contiendra les informations du service destinées à l'instruction des dossiers. L'agent en charge du dossier accédera à l'ensemble des pièces dans le but de réaliser l'activité de fond du service.

En revanche, la base de données de traçabilité contiendra les informations offrant une vision globale des actions successives effectuées sur le dossier. Cela permettra, par exemple, au service support de fournir au demandeur un récapitulatif de l'état du dossier, ou de faire des statistiques sur le temps de traitement des différents dossiers. Il s'agit là d'actions certes très importantes, mais annexes au cœur de métier.

D'un point de vue technique, la base de données contenant les informations métier et les informations de traçabilité pourra être la même ou non. Dans le cas où ces informations sont stockées en un seul endroit, c'est la « vue » qui est offerte aux différents utilisateurs qui distinguera la nature des données au moment où elles sont exploitées. Lors de la restitution, les dossiers pourront, par exemple, être rendus anonymes dans le cas de la traçabilité, si celle-ci est destinée à des partenaires externes au responsable du traitement, dans le but d'offrir une visibilité sur l'activité du service sans révéler d'information confidentielle.

Copyright © 2012 Eyrolles.

La traçabilité, une activité planifiée et organisée

Pour que la traçabilité remplisse son ou ses rôles (voir à ce sujet la section « La traçabilité, nécessité et opportunité » de ce chapitre), il est fondamental de la penser et de l'organiser en amont, au moment de la conception du service.

En effet, les données de traçabilité ont en général besoin d'être plus détaillées que les données métier. Prenons un exemple :

- lorsqu'un dossier passe de l'état « soumis » à l'état « instruit », du point de vue métier, son état change et l'ancien état disparaît au profit du nouveau ;
- en revanche, du point de vue de la traçabilité, il faut conserver la mémoire des états successifs, des dates des changements et des utilisateurs qui ont agi pour passer d'un état à l'autre.

Cette conception de la traçabilité permet de s'assurer de la pertinence et de la fidélité des traces qui sont conservées. Ainsi, dans un système de traçabilité, les traces individuelles et leurs relations entre elles doivent correspondre à un ensemble de règles sans lesquelles la traçabilité n'atteint pas son but.

Les règles suivantes s'appliquent aux traces prises individuellement :

- le contenu d'une trace doit correspondre à l'événement qu'elle représente, de manière exhaustive et certaine : le triptyque « Qui ? Quoi ? Quand ? » doit refléter la réalité de l'événement tracé ;
- par extension, la trace doit pouvoir être interprétée : sa syntaxe et sa sémantique (c'est-à-dire son format et son sens) doivent être définies en amont et systématiquement respectées ;
- afin de garantir sa fiabilité, la trace doit être intègre : il doit être possible de prouver qu'elle n'a pas été modifiée entre le moment de son établissement et celui de son interprétation ;
- chaque trace doit pouvoir être identifiée individuellement, par exemple à l'aide d'un numéro unique de trace.

Les règles suivantes s'appliquent aux traces prises dans leur ensemble :

- les traces doivent constituer un ensemble cohérent et exhaustif : il faut s'assurer que tous les événements qui nécessitent la traçabilité soient pris en compte ;
- aucune trace ne peut être ajoutée ou supprimée de l'ensemble : cela peut se faire *a minima* à l'aide d'une numérotation de chaque trace sous une forme croissante et sans interruption, mais on peut aller plus loin grâce au chaînage des traces, que nous détaillerons plus loin ;
- l'accès aux traces doit être prévu, de manière à pouvoir les consulter et les extraire autant que de besoin ;

Copyright © 2012 Eyrolles.

- l'accès aux traces doit être contrôlé et restreint aux seuls utilisateurs habilités à en prendre connaissance.

Certaines traces seront générées et conservées directement dans le service dématérialisé ; d'autres, en revanche, s'y rapportent mais ne peuvent pas être gérées par lui. C'est le cas en particulier des traces des opérations d'exploitation technique du service. Dans ce cas, on mettra en œuvre un système de traçabilité qui respectera les mêmes contraintes, mais géré séparément, par exemple sous la forme d'un « cahier d'exploitation ». Dans la suite de ce chapitre, nous restreindrons notre propos aux traces générées automatiquement au sein d'un service dématérialisé.

Voyons maintenant à quels usages les traces sont destinées, afin de mieux appréhender l'importance de la mise en œuvre d'un bon système de traçabilité.

La traçabilité, nécessité et opportunité

La nécessité de la traçabilité

Dans cette section, nous analyserons la nécessité de la traçabilité sous trois angles : les obligations sectorielles, l'utilité juridique et les besoins liés au métier de fournisseur de services dématérialisés.

Les obligations légales

Il existe de nombreux secteurs d'activités liés à la dématérialisation dans lesquels la traçabilité n'est pas une option mais bien une obligation, que ce soit du fait de la loi ou de contraintes sectorielles. Citons quelques exemples de ces obligations.

Dans le **secteur bancaire**, la traçabilité est indispensable d'une part pour réduire le risque opérationnel et d'autre part pour établir le contrôle interne des établissements bancaires. La dimension prudentielle de ce secteur aussi bien que la nécessité de lutte contre la fraude et le blanchiment d'argent rendent obligatoire une traçabilité totale des opérations réalisées, tant pour un usage interne que pour une possible divulgation aux autorités de contrôle.

Les opérateurs de **jeu d'argent et de hasard en ligne** opérant en France ou offrant un accès à des joueurs français ont l'obligation de déposer l'ensemble des traces des activités de jeu dans un coffre-fort électronique accessible en permanence par l'Autorité de régulation des jeux en ligne (Arjel), dont ils doivent obtenir un agrément (loi n° 2010-476 du 12 mai 2010). L'objectif de cette réglementation est triple : protection des joueurs par la détection de comportements addictifs, lutte contre le blanchiment d'argent et contrôle fiscal.

La loi pour la confiance dans l'économie numérique (LCEN) décrit les obligations qui s'imposent aux **fournisseurs d'accès à Internet et aux**

Copyright © 2012 Eyrolles.

fournisseurs d'hébergement de contenu en termes de conservation des traces, qui peuvent être requises par les autorités judiciaires. Les traces à conserver incluent les données sur les titulaires des comptes (nom, prénom, pseudonymes, identifiants de connexion, adresse postale, e-mail, numéro de téléphone, mot de passe…) ainsi que l'ensemble des opérations effectuées sur les contenus hébergés (identifiants de connexion, identifiant de contenu, nature de l'opération, date de l'opération…).

En règle générale, avant de se lancer dans une activité liée à la dématérialisation, il importe de bien analyser le contexte juridique applicable et de déterminer quelles obligations sont à prendre en compte. Ainsi, un cybercafé ou même une entreprise offrant un accès à Internet à ses employés à titre gratuit entrent dans la catégorie des « opérateurs de communications électroniques » et se voient donc *de facto* imposer les contraintes qui découlent de l'article L.34-1 du Code des postes et télécommunications. L'alinéa II oblige à l'anonymisation des données relatives au trafic, et l'alinéa III, par exception, demande la conservation des données de connexion, « pour les besoins de la recherche, de la constatation et de la poursuite des infractions pénales ou d'un manquement à l'obligation définie à l'article L.336-3 du Code de la propriété intellectuelle, et dans le seul but de permettre, en tant que de besoin, la mise à disposition de l'autorité judiciaire ou de la haute autorité mentionnée à l'article L.331-12 du Code de la propriété intellectuelle d'informations ».

Les traces à but juridique

Au-delà des obligations légales, la judiciarisation du domaine de la dématérialisation force les fournisseurs de services dématérialisés à se mettre en position de pouvoir prouver en cas de contentieux les opérations qui ont été réalisées au sein des services qu'ils offrent, que ce soit pour se protéger eux-mêmes ou pour offrir à leurs clients les moyens de faire la preuve de leur bonne foi. Citons deux exemples.

Le **Code des marchés publics** dispose, dans son article 56, que « dans toutes les procédures de passation des marchés publics et accords-cadres, les documents écrits […] peuvent être remplacés par un échange électronique ». Les modalités de transmission et de sécurisation des échanges sont à la charge de la personne publique, qui s'appuie sur une plate-forme de dématérialisation aussi appelée « profil d'acheteur » . Même si rien n'est précisé sur les obligations liées à la traçabilité, la conception d'un tel service nécessite de prendre en compte toutes les obligations qui découlent du Code des marchés publics en ce qui concerne les délais. Il sera ainsi utile de tracer de manière certaine et opposable la date d'envoi de l'avis d'appel public à la concurrence pour publication, la date de mise à disposition du dossier de consultation des entreprises, la date limite de remise des plis, la date de réponse aux questions des candidats, la date de réception des

Copyright © 2012 Eyrolles.

candidatures et des offres de chacun des candidats au marché, la date de notification des rejets, la date d'attribution du marché… Le non-respect de chacune des contraintes liées à ces éléments peut entraîner l'annulation de la procédure par le tribunal administratif en cas de référé.

Reprenons l'exemple du téléservice **Réseaux et canalisations** mis en œuvre par l'Ineris : ce service recense les coordonnées des ouvrages dans le but de permettre les déclarations préalables aux chantiers. Dans le cas d'un endommagement d'ouvrage qui résulterait d'une mauvaise tenue à jour du référentiel, il serait très important de pouvoir déterminer les responsabilités de chacun des acteurs. Est-ce l'exploitant de réseau qui a omis de déclarer son ouvrage ou qui s'est trompé sur sa localisation lors de sa déclaration ? Est-ce le service lui-même qui n'a pas reproduit fidèlement les informations de localisation et de nature de l'ouvrage, voire les coordonnées des contacts destinés à la déclaration ? Ou est-ce le responsable des travaux qui n'a pas respecté ses obligations de déclarations ou qui a mal interprété les réponses obtenues ? Les opérations de mise à jour du référentiel des ouvrages et les demandes des déclarants donnent systématiquement lieu à l'établissement d'un « dossier de preuve » regroupant l'ensemble des actions et des échanges réalisés, de manière à garantir la sécurité juridique tant du service que de ses utilisateurs.

Les traces au service du métier

La traçabilité n'a pas seulement une vocation juridique. Voyons maintenant comment elle peut souvent être mise au service du métier, au travers de trois exemples.

Les activités de **commerce en ligne**, dans lesquelles l'internaute passe commande d'un bien qui lui sera livré à domicile, peuvent aujourd'hui difficilement être imaginées sans un service de traçabilité de la commande mis à disposition du client. La commande est prise en compte, prête, expédiée, livrée, encaissée… Si cette fonction de traçabilité n'est pas le cœur du métier (qui consiste en l'achat et la livraison du bien), elle offre une valeur ajoutée de transparence qui contribue également à faire baisser le coût du service puisqu'elle évite des appels au service clients.

La **lettre recommandée électronique**, définie par l'article 1369-8 du Code civil et le décret n° 2011-144 du 2 février 2011, est un exemple type de service dans lequel la traçabilité est au cœur du métier. Ainsi, dans le cadre de la conclusion ou de l'exécution d'un contrat, la lettre recommandée électronique doit être acheminée par un tiers, selon un procédé permettant :

- d'identifier le tiers ;
- de désigner l'expéditeur ;
- de garantir l'identité du destinataire ;
- d'établir si la lettre a été remise ou non au destinataire.

Copyright © 2012 Eyrolles.

La traçabilité couvrira ainsi dans un tel service non seulement le cycle de vie du courrier (envoyé, présenté, remis, non remis), avec la gestion des délais, le destinataire ayant 15 jours pour procéder au retrait, mais également les moyens de garantie de l'identité de l'émetteur, du destinataire et du tiers d'acheminement.

Citons enfin le cas des **services publics dématérialisés** : l'ordonnance n° 2005-1516 du 8 décembre 2005 relative aux échanges électroniques entre les usagers et les autorités administratives, et entre les autorités administratives, dispose dans son article 5 que : « toute demande, déclaration ou production de documents adressée par un usager à une autorité administrative par voie électronique, ainsi que tout paiement opéré dans le cadre d'un téléservice, fait l'objet d'un accusé de réception électronique et, lorsque celui-ci n'est pas instantané, d'un accusé d'enregistrement électronique ». À la croisée de l'obligation légale et de l'utilité métier de la traçabilité, confortée par la mise en application de la charte Marianne destinée à améliorer la qualité du service public, cette disposition marque bien l'importance de la traçabilité dans la qualité de service, d'autant que les articles suivants du même texte établissent l'inapplicabilité des délais de recours en cas de non-envoi de l'accusé de réception par la personne publique.

Parole d'expert

Charles Du Boullay, président du Directoire de CDC Fast et directeur général de CDC Arkhinéo

CDC Fast et CDC Arkhinéo sont tiers de télétransmission et tiers archiveur, auprès des collectivités publiques et des entreprises privées. Quelle est l'apport d'un tiers de confiance pour l'établissement de la traçabilité des échanges ?

Le tiers de confiance est un intermédiaire indépendant entre les parties qui le reconnaissent simultanément et *a priori* comme garantie de neutralité et d'objectivité pour la bonne fin de leurs transactions. Le tiers de confiance est celui à qui les parties vont faire appel pour faire reconnaître leurs droits. Il est de plus en plus difficile de maîtriser les technologies et en particulier de les faire évoluer tant sur le plan matériel que logiciel. CDC Fast permet à ses clients de :

- reporter le risque sur un tiers ;
- ne pas être suspectés d'avoir pu modifier la donnée ;
- partager l'information en ligne ;
- limiter les investissements.

Quelles mesures spécifiques prenez-vous pour garantir la fiabilité et la conservation des données de traçabilité ?

CDC Fast, en tant que tiers de télétransmission, constitue une preuve de l'échange. Pour cela, il va associer à la trace de l'échange des éléments d'horodatage qui seront signés par le tiers de télétransmission, attestant la réalité de l'échange ainsi que sa date certaine. Cette preuve devra être conservée, pendant toute la durée légale, dans des conditions lui permettant d'être utilisée en cas de contestation.

Copyright © 2012 Eyrolles.

Pour cela, CDC Fast utilise le service de Coffre-fort électronique® de CDC Arkhinéo. CDC Arkhinéo, en tant que tiers archiveur, garantit l'intégrité, la sécurité et la disponibilité des fichiers de preuves. CDC Arkhinéo a été attesté conforme à la norme d'archivage Z42-013 (transposée en ISO 14641-1). Il a également été agréé par les Archives de France pour la conservation des archives publiques courantes et intermédiaires.

CDC Arkhinéo applique un processus d'archivage consistant à calculer des empreintes, sceller l'archive, l'indexer, la sécuriser en l'enregistrant en cinq exemplaires répartis sur trois sites distants dont un situé à plus de 450 km des deux autres. Grâce à sa plate-forme dont l'architecture logicielle est massivement répartie sur des serveurs distribués sur ces trois sites, CDC Arkhinéo offre un service sécurisé, accessible 24 heures sur 24 et 7 jours sur 7 en s'engageant sur un taux de disponibilité de 99,7 %. Le Coffre-fort électronique® conserve ainsi toute la valeur probante du fichier de preuve constitué par CDC Fast et le rend accessible pendant toute la durée de conservation.

Le coffre-fort électronique permet également la capture et la conservation des échanges de courriers électroniques : pourquoi appliquer la traçabilité à ce domaine spécifique ?

De plus en plus de transactions se font par e-mail sans aucune sécurité, il sera très difficile pour les parties de faire valoir leurs droits en cas de litige. S'appuyer sur un tiers tant pour la traçabilité que pour la conservation permet de donner aux échanges effectués par courriers électroniques la valeur probatoire qui leur manque. De plus, ces échanges contractuels sont soumis au Code du commerce en ce qui concerne la conservation des pièces (10 ans de durée de conservation). Une solution bureautique n'est pas adaptée à ce type de besoin, il est donc nécessaire d'en tenir compte et de mettre en place un dispositif pour faire face à ces obligations. Le coffre-fort électronique®, marque déposée en 2001 par CDC Arkhinéo, répond à ces exigences.

Les bénéfices secondaires de la traçabilité

Nous avons vu dans la section précédente que la traçabilité permettait de respecter la législation, d'apporter de la sécurité juridique aux services dématérialisés, et constituait également une dimension métier de certains services. Mais au-delà de ces aspects « obligatoires », l'établissement systématique de traces de l'activité constitue également une opportunité pour l'entreprise, tant sur la connaissance de ses clients que pour l'amélioration de sa qualité de service ou l'établissement de nouvelles offres.

Tout d'abord, la traçabilité permet de suivre la qualité de service offerte du point de vue technique (disponibilité du service, temps de réponse), mais également du point de vue métier, en permettant d'établir sur une base certaine les temps de traitement des dossiers instruits au sein du service. La traçabilité s'inscrit ainsi de manière naturelle dans une démarche qualité incluant un plan d'amélioration continue.

Copyright © 2012 Eyrolles.

Par extension, le système de traçabilité peut constituer la source de nombreuses mesures sur le fonctionnement du service. On peut en répartir les apports en deux catégories, selon qu'elles sont tournées vers l'extérieur ou vers l'intérieur.

Vis-à-vis de l'extérieur, les chiffres et informations qui en découlent peuvent servir de base au marketing par la connaissance qu'ils offrent des pratiques réelles des clients. Le *scoring* est une technique de hiérarchisation des traces qui permet de mieux définir et cibler son offre commerciale par rapport à l'activité constatée sur le service. La traçabilité devient ainsi un outil pour mieux définir ses services et pour mieux les vendre, et contribue à l'activité commerciale de l'entreprise.

Vis-à-vis de l'intérieur, les mesures issues de la traçabilité permettent d'adapter les ressources mises en œuvre et les procédures par rapport au fonctionnement du service. Elles permettent également de mesurer l'efficacité des agents affectés au traitement des dossiers, et ainsi d'attribuer les primes ou de déterminer les besoins de formations, mais aussi de faire ressortir les bonnes pratiques.

Enfin, la traçabilité, dans sa dimension de réduction du risque juridique lié à l'activité, permet également la création de nouveaux services. Ainsi, le secteur bancaire a pu créer de nouvelles offres, avec des seuils financiers plus importants, grâce à la traçabilité offerte par la banque en ligne garantissant l'opposabilité des actions des clients et donc baissant le coût assurantiel des services.

L'établissement d'un système fiable de traçabilité est donc, pour l'entreprise, un facteur d'amélioration et de productivité non négligeable, pourvu que soient mis en œuvre conjointement les outils d'analyse et de décision nécessaires à l'exploitation de la base de connaissances ainsi constituée.

Traçabilité et données personnelles

L'inclusion dans les traces de données à caractère personnel est encadrée par la loi Informatique et libertés du 6 janvier 1978.

Selon les cas, ces traitements pourront être soumis à une déclaration auprès de la CNIL, voire à une autorisation formelle de sa part. L'usage des données à caractère personnel force notamment à :

- établir la liste des données à caractère personnel employées ;
- établir la finalité du traitement ;
- justifier que les données à caractère personnel sont nécessaires au traitement envisagé ;
- établir la durée de conservation des traces nécessaire à la finalité, et supprimer les données personnelles à l'issue de ce délai.

Il est à noter que l'usage du numéro de Sécurité sociale dans les traces n'est pas autorisé, sauf exceptions spécifiques.

Copyright © 2012 Eyrolles.

Les différentes formes de traçabilité

Un outil au service de la traçabilité : l'horodatage

Une trace étant de manière générique constituée par le triptyque « Qui ? Quoi ? Quand ? », il est important de disposer de systèmes permettant d'établir la date et l'heure des événements, dans le but de les prouver *a posteriori*. C'est le rôle de l'« horodatage », que nous détaillerons ici en envisageant d'abord quelles sont les « sources de temps » qui peuvent être employées pour l'établir, puis en considérant deux façons de le réaliser : l'horodatage simple et l'horodatage certifié.

Les sources de temps

Les ordinateurs incluent des informations de date dans le cadre des processus dématérialisés sur la base de leur horloge interne. Or, la fiabilité de ces composants électroniques n'est pas suffisante pour offrir une qualité de service garantie contractuellement : il existe un risque important de dérive de l'horloge.

C'est pourquoi les serveurs devant offrir une heure fiable sont régulièrement synchronisés par rapport à des sources de temps. Le protocole utilisé pour la synchronisation des machines sur Internet s'appelle NTP (*Network Time Protocol*) et est normalisé dans la RFC 4330.

Le fonctionnement global du service de synchronisation est conçu sur la base de « strates », définissant la proximité de chaque serveur par rapport à une source de temps fiable. Ainsi, les serveurs de strate 0 sont directement connectés à telle source, comme une horloge atomique ou un récepteur GPS. Cette connexion ne passe pas par un réseau, mais par un lien physique direct. Les serveurs de strate 1 sont directement synchronisés sur une source fiable de la strate 0. Les serveurs de strate 2 sont synchronisés sur un serveur de strate 1, et ainsi de suite.

La synchronisation *via* le protocole NTP permet de garantir une fiabilité de la date et l'heure d'un ordinateur avec une précision de l'ordre du centième de seconde.

L'horodatage simple

La façon la plus simple de réaliser l'horodatage d'un événement consiste à enregistrer dans la base de traçabilité la date et l'heure du serveur au moment de l'événement.

La fiabilité de cet horodatage simple dépendra de plusieurs facteurs :

- la politique de synchronisation du serveur par rapport à des sources de temps et l'effectivité de sa mise en œuvre ;
- la synchronisation de l'événement et de la réalisation de sa trace ;

Copyright © 2012 Eyrolles.

- la conservation de la trace réalisée dans des conditions de nature à en garantir l'intégrité, afin de s'assurer que l'information de date enregistrée n'a pas pu être modifiée *a posteriori*.

Le lien entre l'horodatage simple et l'événement ou le document auquel il se rapporte est établi uniquement par l'enregistrement effectué dans la base de données et offre le niveau de confiance permis par cette base de données.

Lorsqu'il est réalisé au sein d'un service mettant en œuvre une politique de traçabilité offrant toutes les garanties de fiabilité, l'horodatage simple est satisfaisant dans bien des cas. Toutefois, il existe des situations où la fiabilité d'un tel horodatage n'est pas suffisante. Considérons, par exemple, la réalisation d'une signature électronique.

Nous avons vu que la date à laquelle la signature a été réalisée est un élément fondamental de la vérification de signature, puisqu'elle permet d'apprécier si le certificat était encore en cours de validité et non révoqué au moment de la signature. Le format CAdES de signature électronique inclut par défaut la date et l'heure du poste du signataire dans les données de signature. Toutefois, si le signataire est un usurpateur qui a volé la clé privée d'un tiers et veut réaliser de vraies fausses signatures à sa place, il n'aura qu'à reculer la date de son ordinateur pour faire croire que la signature a eu lieu avant le vol… Et lors de la vérification, la signature usurpée apparaîtra comme valide.

Un mécanisme permet de sécuriser l'horodatage et de le lier de manière fiable au contexte de son établissement : il s'agit de l'horodatage certifié.

L'horodatage certifié

La RFC 3161 (TSP, *Time Stamp Protocol*) définit le format des « jetons d'horodatage » ou « contremarques de temps » utilisés dans l'horodatage certifié.

Un jeton d'horodatage est émis par un tiers de confiance appelé « prestataire de services d'horodatage électronique » (PSHE), ou « autorité d'horodatage ». Il porte sur un document et est constitué des éléments suivants :

- un hash du document horodaté ;
- la date et l'heure provenant du serveur d'horodatage ;
- le scellement de ces informations par le PSHE sous la forme d'un cachet réalisé à l'aide de sa clé privée ;
- le certificat du PSHE permettant au destinataire du jeton d'en vérifier la provenance et l'intégrité.

Copyright © 2012 Eyrolles.

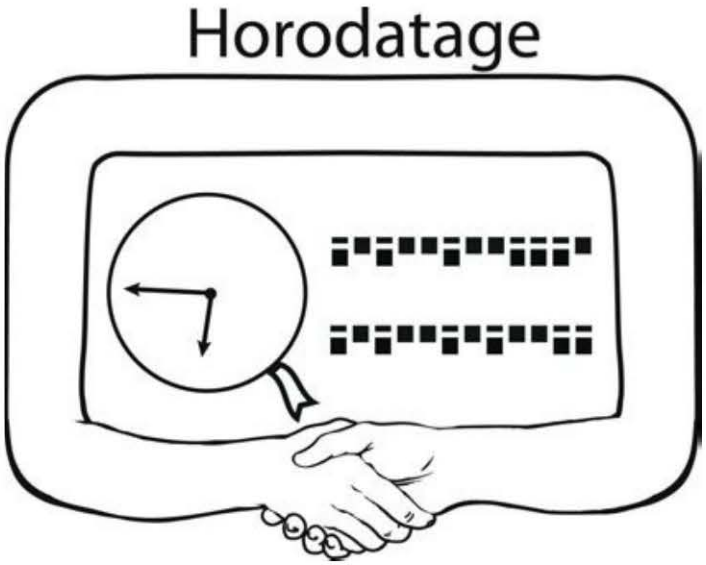


Figure 11-1 : Le jeton d'horodatage

Le jeton d'horodatage doit être interprété comme suit : à la date et l'heure certifiées dans le jeton, le document dont le hash est inclus dans le jeton existait. Le PSHE est le garant de ce fait, sur la base de la présentation du hash du document par le demandeur du jeton.

Il est à noter que le demandeur d'un jeton d'horodatage n'a pas à révéler au PSHE le contenu du document qu'il souhaite horodater : il se contente de lui en envoyer un hash. Toutefois, grâce aux propriétés du hash que nous avons vues dans le chapitre 2 sur la cryptographie, le cachet apposé par le PSHE garantit l'intégrité du document dans son ensemble.

Le PSHE décrit ses engagements, notamment en termes de précision de l'horodatage, dans une politique d'horodatage. Le Référentiel général de sécurité (RGS) fournit une politique d'horodatage type et décrit les contraintes à respecter pour faire qualifier un service d'horodatage. Il est en particulier demandé que la clé privée du PSHE soit générée et conservée dans un matériel cryptographique (HSM, *Hardware Security Module*).

Reprenons l'exemple de la signature électronique : l'horodatage certifié sera apposé sur le résultat du calcul RSA effectué par le signataire à l'aide de sa clé privée (la signature au sens technique du terme, comme décrite au chapitre 8). Le jeton d'horodatage sera inclus dans l'enveloppe de signature conformément à l'annexe A de la RFC 3161. Ainsi, le destinataire de la signature, lors de la vérification, aura la certitude qu'à la date incluse dans le jeton d'horodatage, la signature avait déjà été réalisée : toute expiration ou révocation du certificat du signataire postérieure à cette date n'invalidera pas la signature électronique.

Copyright © 2012 Eyrolles.

Parcourons maintenant les différentes formes que prennent les traces en fonction des usages auxquels elles sont destinées, et constatons dans chaque cas quelle est la forme d'horodatage la plus appropriée.

Les logs techniques

Les logs techniques sont les traces générées automatiquement par les applications informatiques pour faire foi du fonctionnement technique du système. Ils sont destinés aux concepteurs, aux développeurs et aux exploitants, qui s'en servent pour suivre la qualité de service et diagnostiquer les dysfonctionnements.

Ces logs ne sont en général pas rendus publics, et leur interprétation, faite par les techniciens, n'est documentée (au mieux) qu'au sein de la spécification technique ou des procédures d'exploitation. Ils comportent un horodatage simple.

Plusieurs niveaux de logs techniques sont en général disponibles, selon leur niveau de détail : du niveau « debug », principalement utilisé dans les phases de conception-réalisation, qui comprend le plus de détails, au niveau « erreurs seulement », dans lequel seuls les messages relatifs aux dysfonctionnements bloquants sont tracés.

Les logs techniques ne font en général pas partie des spécifications fonctionnelles du service, et sont conçus et mis en œuvre par les développeurs en fonction de leurs besoins. Il convient donc d'être attentif à ce que ces traces à vocation technique ne contiennent pas d'informations de nature à aller à l'encontre de la politique de sécurité globale du service, notamment en termes de confidentialité et de gestion des données à caractère personnel. Les logs techniques constituent une source classique de faille de sécurité des systèmes d'information : on y retrouve parfois les identifiants et mots de passe de connexion, voire des clés cryptographiques !

Les traces applicatives

Les traces applicatives sont destinées à la traçabilité fonctionnelle et juridique de la plate-forme.

Ces traces sont le cœur du système de traçabilité et doivent être conçues en même temps que le service, avec les interfaces de visualisation offrant à chaque acteur les possibilités de consultation et d'extraction nécessaires à son métier et restreintes à ses besoins.

Chaque événement utile pour l'un ou l'autre des acteurs du système doit faire l'objet d'une trace incluant l'ensemble des informations nécessaires à son exploitation.

Les traces doivent être conçues comme une base de données à part entière, sur laquelle il doit être possible de faire des recherches par filtrage.

Copyright © 2012 Eyrolles.

On pourra, par exemple, être intéressé par les traces d'une certaine période de temps, par les actions d'un certain utilisateur, par l'ensemble des traces correspondant à un certain type d'événement ou encore au cycle de vie d'un document particulier. Il sera très important, dans les interfaces de consultation des traces dédiées à chacun des rôles au sein du service dématérialisé, de permettre le filtrage sur les éléments pertinents en fonction du métier de chacun.

Pour que les traces soient opposables en cas de contentieux sans ambiguïté possible, leur contenu et leur interprétation doivent être documentés dans la politique de traçabilité du service. Pour chaque trace, il convient de décrire dans quel cas elle est produite, les éléments qui y figurent et le sens qu'ils ont.

Supposons que, dans le système de traçabilité, les utilisateurs soient représentés par leur identifiant stocké dans un champ « utilisateur ». Dans le cas d'un envoi de document d'un émetteur à un destinataire, la trace comprendrait deux champs « utilisateur » définissant ces deux personnes, ce qui crée une ambiguïté. On pourra concevoir la base avec un champ « émetteur » et un champ « destinataire », ce qui est très explicite mais moins générique, ou encore ajouter au champ « utilisateur » générique un attribut de qualification de l'utilisateur, renseigné dans ce cas d'usage avec la valeur « émetteur » ou « destinataire ».

Afin de renforcer la fiabilité et la valeur juridique des traces applicatives, on pourra mettre en œuvre un chaînage cryptographique, par exemple en incluant dans chacune le hash de la précédente. On pourra également, dans le but d'en garantir la provenance et l'intégrité, les sceller régulièrement par l'intermédiaire d'un cachet, et les extraire périodiquement afin de les déposer dans un coffre-fort électronique pour un archivage à vocation probatoire.

Certains des événements survenant au cours du processus dématérialisé peuvent revêtir une importance particulière du point de vue juridique. On pourra dans ce cas renforcer la valeur des traces en produisant des preuves certifiées, comme nous le détaillerons dans la section suivante.

Les preuves cryptographiques

Si le système de traçabilité applicative est conçu comme un tout cohérent sur lequel il est souhaitable de pouvoir faire des analyses et des extractions, il peut également être intéressant d'établir des éléments de traçabilité faisant foi de manière certaine d'un événement spécifique, indépendamment de son contexte : par exemple, la validation par un utilisateur des conditions générales d'utilisation, la réception d'un document, le changement de statut d'un dossier ouvrant des droits pour le demandeur…

Copyright © 2012 Eyrolles.

Dans ce cas, en plus de la génération d'une trace au sein de la traçabilité applicative, on générera, en même temps, une preuve autonome faisant foi du déroulement de l'événement, sous la forme :

- d'un fichier structuré (par exemple, XML) reprenant le contenu de la trace : acteurs, actions, éléments de contexte, documents ou processus concernés ;
- d'un scellement de ce fichier par un cachet afin de garantir la provenance et l'intégrité de la preuve ;
- d'un horodatage certifié faisant foi de la date et l'heure d'établissement de la preuve.

Les preuves cryptographiques ainsi générées seront conservées dans un système d'archivage électronique, et pourront être exhibées en cas de besoin. Elles pourront aussi être remises aux utilisateurs ayant effectué les actions concernées, dans le but d'offrir une égalité d'accès aux preuves et, ainsi, de rendre impossible la mauvaise foi des utilisateurs, ce qui réduit la possibilité de contentieux aux seuls aspects de fond et non de forme.

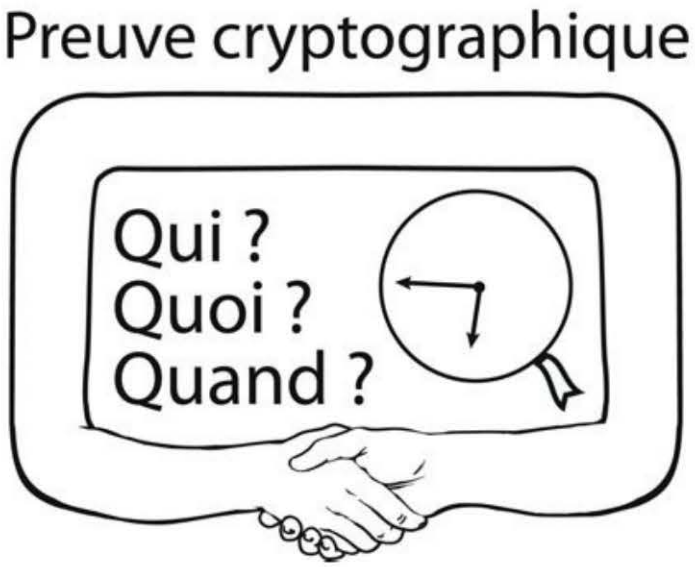


Figure 11-2 : La preuve cryptographique

La liste des preuves cryptographiques générées par le système, leur mode d'établissement, de conservation et d'accès, leur format, leur contenu et leur interprétation seront décrits dans la politique de gestion de preuves du service dématérialisé, qui doit être portée à la connaissance des utilisateurs et acceptée par eux.

L'accès aux preuves cryptographiques sera contrôlé et restreint aux seuls utilisateurs concernés par leur exploitation, pour des raisons de confidentialité et de présence éventuelle de données à caractère personnel.

Copyright © 2012 Eyrolles.

En poussant à l'extrême le principe de la preuve cryptographique, il est possible de générer un procès-verbal faisant foi d'une action ou d'une série d'actions, par exemple à un format directement lisible (PDF), scellé à l'aide d'un cachet du prestataire de service et d'un horodatage certifié. On peut aller jusqu'à faire signer électroniquement ce procès-verbal par l'utilisateur afin de lui en faire valider explicitement le contenu… Mais on sort de la pure « traçabilité » pour entrer dans le domaine des documents « métier » : l'établissement d'un tel procès-verbal correspondra en général à une exigence spécifique au contexte juridique du service.

Il existe une autre forme de traçabilité intermédiaire entre les traces et les données métier : il s'agit des accusés de réception, que nous aborderons dans la section suivante.

Les accusés de réception

Les accusés de réception sont en général des e-mails envoyés automatiquement aux utilisateurs pour faire foi de la bonne prise en compte d'une demande, d'une action ou d'un document transmis par voie électronique.

Comme nous l'avons vu, l'ordonnance du 8 décembre 2005 impose à tous les téléservices de l'administration de produire systématiquement des accusés de réception à destination des usagers.

Les accusés de réception étant bien souvent le seul élément de traçabilité mis à disposition de l'utilisateur des services dématérialisés, il convient d'y faire figurer l'ensemble des informations qui lui seront utiles.

Afin de garantir la provenance et l'intégrité de l'accusé de réception, il est possible de l'envoyer sous la forme d'un e-mail « signé », ou plutôt scellé par un cachet du serveur applicatif.

Après avoir établi la liste des types de traces à la disposition des concepteurs d'applications, développons maintenant les bonnes pratiques utiles pour l'inclusion de la traçabilité dans un projet de dématérialisation.

Inclure la traçabilité dans son projet

Le préalable indispensable : une analyse détaillée du contexte applicatif

L'analyse du contexte aura de préférence lieu au sein d'une étude de sécurité globale, comme nous le verrons au chapitre 14 consacré à la mise en œuvre de la dématérialisation.

Le besoin de traçabilité du service dématérialisé découle directement des aspects métier du service, mais aussi de son contexte juridique et des besoins internes de l'entreprise.

Copyright © 2012 Eyrolles.

L'analyse du contexte juridique recouvre deux dimensions :

- les obligations légales qui s'imposent du fait des textes en vigueur et du contexte sectoriel et/ou normatif ;
- la couverture par la traçabilité de tout ou partie du risque de contentieux lié à l'activité du service. Il s'agira alors de protéger les utilisateurs, mais aussi le fournisseur de services lui-même. Il pourra être utile d'envisager le recours à un tiers de confiance en vertu du principe qui stipule que « nul ne peut se constituer une preuve à lui-même ».

L'analyse du contexte métier déterminera les actions et les données qui ont du sens au sein du système de traçabilité, ainsi que les utilisateurs habilités à y accéder en fonction de leurs besoins. On prendra en compte les diverses catégories d'acteurs du système :

- les utilisateurs, pour leur permettre de suivre le déroulement de leurs procédures ;
- le service support, pour lui donner une vision d'ensemble des événements qui se sont déroulés dans le système ;
- le service marketing, à des fins de statistiques, de scoring ou de data mining ;
- le service qualité, dans un but d'analyse de qualité de service et d'amélioration continue ;
- la direction générale, pour le pilotage stratégique du développement des services ;
- la direction juridique, en cas de contentieux ;
- les organes de contrôle ou les autorités judiciaires…

Cette analyse prendra en compte le contexte technique du service, de manière à permettre également aux traces d'être un support utile pour la résolution d'éventuels incidents d'exploitation, le maintien en conditions opérationnelles du service et la mesure de performances en vue de la montée en charge de l'application.

Définir la forme et le contenu des traces

À l'issue de l'étape d'analyse du contexte, le concepteur de l'application dispose des éléments qui lui permettent de décider, pour chaque type de trace, des informations qu'elle contiendra et de la forme qu'elle prendra :

- les éléments purement techniques seront intégrés dans les logs applicatifs ;
- les événements de forte importance fonctionnelle seront inclus dans la traçabilité applicative ;
- les actions à connotation juridique donneront lieu à l'établissement d'une preuve cryptographique ;

Copyright © 2012 Eyrolles.

- les actions des utilisateurs seront confirmées par des accusés de réception.

Pour chacune de ces catégories, il est alors possible de déterminer le triptyque « Qui ? Quoi ? Quand ? » en gardant à l'esprit, pour chaque catégorie d'utilisateurs, quelles sont les informations pertinentes.

Il faut rester attentif, lors de cette étape, aux trois types de données :

- celles que l'on *doit* tracer du fait d'une obligation réglementaire ;
- celles que l'on *peut* tracer, en fonction de son besoin métier ;
- celles que l'on *ne doit pas* tracer du fait d'une interdiction.

Lorsque les données de traçabilité contiennent l'identité de personnes physiques, il importe d'être prudent en ce qui concerne la fiabilité de ces données. En effet, nous avons vu dans le chapitre 4 sur l'identité numérique que les référentiels d'utilisateurs étaient rarement fiables. Il s'agit aussi de prendre en compte l'existence d'homonymes, qui pourraient amener le système de traçabilité à imputer une action à un autre utilisateur, à refuser à un utilisateur la reconnaissance d'un droit, voire à dispenser un utilisateur du respect d'une obligation du fait de l'impossibilité de prouver qu'il s'agit bien de lui et non d'un homonyme. Le dédoublonnage des utilisateurs et l'utilisation d'identifiants en lieu et place des données d'état civil sont un début de solution au problème.

Pour déterminer avec précision le format des traces, et en particulier des preuves cryptographiques, on se conformera aux normes en vigueur applicables au contexte (standard XML, formats de cachet et d'horodatage, respect du RGS…).

Définir le cycle de vie des traces

L'étape suivante consiste à déterminer le cycle de vie des traces générées par le système. Cette activité passe par plusieurs étapes.

En premier lieu, il faut déterminer **le moment de la création des traces** : le plus fréquent est de les générer au moment où l'événement tracé survient, mais il convient de faire attention, pour les événements ayant une certaine durée, à la définition de ce moment. Par exemple, pour le téléchargement d'un document, en fonction de ce que la trace doit prouver, on la générera lors du début du téléchargement, ou à la fin. Il sera même envisageable de générer les deux traces (début et fin de téléchargement), ce qui permettra en outre de mesurer le temps de téléchargement.

Ce sera également le moment de déterminer si le système de traçabilité s'appuiera sur un ou plusieurs tiers de confiance, par exemple pour le scellement par un cachet, l'horodatage ou l'archivage des traces.

En deuxième lieu, on déterminera **le mode de conservation des traces** : selon les exigences de disponibilité et de performances, elles formeront

Copyright © 2012 Eyrolles.

un sous-ensemble de la base de données métier, ou une base de données indépendante. Les preuves cryptographiques pourront être stockées en base de données ou sur un système de fichiers.

L'opportunité et le moment de l'archivage des traces et des preuves seront déterminés. On pourra, par exemple, opter pour un archivage des preuves certifiées dès leur génération, et un archivage quotidien des traces consolidées de la veille.

Si les traces sont confiées à un tiers, les aspects contractuels de cette relation devront prendre en compte les aspects d'exploitation des traces et de confidentialité. On pourra ainsi demander la mise en place d'une traçabilité de l'accès aux traces par les personnels du tiers de confiance.

Enfin, les questions de confidentialité seront envisagées : si les traces comprennent des données à caractère personnel, une intrusion résultant en la divulgation de ces données peut être de nature à ternir durablement l'image de l'entreprise. Il est alors possible de mettre en œuvre le chiffrement de tout ou partie des données de traçabilité, de même qu'on le fera pour la base de données métier.

La troisième étape consiste à déterminer **les accès aux traces** : quelles données seront disponibles pour quels rôles ? Faut-il une anonymisation ? Par exemple, à des fins de traitement statistique, les exploitants système peuvent-ils accéder à la base de données de traçabilité, ou les contraintes de confidentialité imposent-elles une protection particulière (chiffrement ou contrôle d'accès plus restrictif) ?…

Dans un souci de transparence des services dématérialisés vis-à-vis des utilisateurs, et d'équilibre de l'établissement de la preuve, il est souhaitable de donner aux utilisateurs un accès aux traces qui les concernent directement, de manière à leur permettre de vérifier que leurs actions ont été prises en compte par le système et de suivre l'avancement de leurs dossiers.

Enfin, il est préférable d'anticiper **la fin de vie des traces** : la loi Informatique et libertés imposant, pour les données à caractère personnel, une conservation proportionnée au traitement effectué, il convient de définir et de justifier la durée de conservation des données de traçabilité, et de mettre effectivement en œuvre les mécanismes adéquats de destruction ou d'anonymisation de ces données à l'issue de la durée de conservation.

Outre cet impératif juridique, la suppression des traces correspond aussi à un souci de gain de place, les données de traçabilité pouvant représenter un volume de stockage important.

Établir et publier une politique de traçabilité

Une fois les spécifications de la traçabilité déterminées selon la méthodologie précédente, il est fondamental, pour conférer une valeur juridique

Copyright © 2012 Eyrolles.

aux traces, de les intégrer dans la convention de preuve globale du service. Nous détaillerons l'ensemble du dispositif de convention de preuve au chapitre 13.

La traçabilité donnera ainsi lieu à la rédaction d'une « politique de traçabilité et de gestion de preuves » décrivant :

- la liste des traces et preuves cryptographiques établies ;
- le contenu des traces et la sémantique associée en vue de leur interprétation ;
- les engagements du prestataire de services : établissement systématique et fidèle des traces, conservation dans des conditions de nature à garantir leur provenance et leur intégrité ;
- les engagements des utilisateurs du service : reconnaissance de la validité des traces en tant que preuves faisant foi des événements survenus dans le cycle de vie du service.

Outre l'apport de cette pratique en termes de transparence vis-à-vis des utilisateurs, et donc d'établissement de la confiance, la publication de cette politique et son acceptation par l'ensemble des utilisateurs constitue le pilier juridique qui confère leur valeur aux traces.

Quelques exemples de projets incluant la traçabilité

Le vote par Internet

Le vote par Internet est une forme de vote par correspondance, dans laquelle les votants sont invités à exprimer leur choix au travers d'une interface web. Ce type de vote est parfois couplé à d'autres modes de scrutin : vote à l'urne, vote par correspondance papier, vote par téléphone…

Deux préoccupations antagonistes régissent la traçabilité dans les applications de ce type, dans le cas du vote à bulletin secret :

- d'une part, la traçabilité la plus absolue est nécessaire pour confirmer la sincérité du scrutin, en garantissant à chaque électeur la prise en compte de son vote et l'intégrité de l'urne électronique, dans laquelle aucun bulletin ne doit pouvoir être retiré, modifié ou ajouté (mis à part par le mécanisme de vote nominal) ;
- d'autre part, la nécessité de l'anonymat du scrutin incite à se méfier de la traçabilité mise en œuvre, qui peut être soupçonnée de servir à lever l'anonymat du vote en établissant un lien entre l'identité de l'électeur et l'expression de son choix.

Copyright © 2012 Eyrolles.

La CNIL a déterminé en 2003 et mis à jour en 2010 les règles applicables aux systèmes de vote par Internet, dans sa délibération n° 2010-371 du 21 octobre 2010 adoptant une recommandation relative à la sécurité des systèmes de vote électronique. Selon les secteurs, des textes divers comportent également les règles applicables aux différents types de scrutins : Code électoral, Code du commerce, Code du travail, Code de la santé publique…

Afin de concilier le besoin de transparence de l'opération électorale et la contrainte de confidentialité, les règles de traçabilité fixées par la CNIL sont les suivantes :

- la solution de vote doit faire l'objet d'un audit indépendant par des experts formés par la CNIL, incluant une revue du code source, de l'infrastructure d'hébergement et de procédures mises en œuvre pour l'établissement des listes électorales et l'acheminement des codes de vote aux électeurs ;
- le système de vote doit faire l'objet d'un scellement logique, dont l'intégrité doit pouvoir être vérifiée par le bureau de vote et les représentants des candidats. Cela inclut non seulement le logiciel, mais également l'urne, la liste d'émargement, la liste des candidats et la configuration des serveurs ;
- la clé de déchiffrement des bulletins de vote doit être générée lors d'une cérémonie publique, et scindée en plusieurs fragments, dont au moins deux sont nécessaires pour réaliser le dépouillement ;
- tous les accès à la plate-forme de vote, par les électeurs, les membres du bureau de vote ou les exploitants techniques, doivent faire l'objet d'une traçabilité, renforcée par un mécanisme cryptographique (chaînage des traces, scellement), mais les traces ne doivent comporter aucune information de nature à permettre de lever l'anonymat du vote ;
- l'urne et la liste d'émargement doivent être séparées au moins logiquement ;
- l'émargement doit comporter un horodatage ;
- l'urne électronique ne doit pas comporter d'horodatage afin qu'aucun lien ne puisse être établi entre l'identité de l'électeur et l'expression de son vote : le principe d'une urne est en effet de mélanger les bulletins, et il ne faut pas que le système permette de les ranger dans l'ordre chronologique. Il s'agit là d'un contre-exemple à la constitution habituelle des traces par le triptyque « Qui ? Quoi ? Quand ? » : dans le cas particulier du vote par Internet, il est aussi important de tracer certaines informations que de ne pas tracer certaines autres !

Certaines solutions de vote par Internet permettent à l'électeur de vérifier la bonne prise en compte de leur vote. Il est important qu'un tel dispositif

Copyright © 2012 Eyrolles.

ne permette pas de retrouver la valeur de ce vote, afin d'éviter l'achat de vote ou la pression sur les électeurs.

On voit bien dans cet exemple que la mise en œuvre de la traçabilité ne repose pas seulement sur la base de données constituée, mais également dans toutes les mesures techniques et organisationnelles appliquées pour en garantir l'exactitude et l'intégrité. De ce point de vue, l'audit indépendant joue un rôle majeur. C'est le respect de l'ensemble de ces règles qui permet de garantir la sincérité du scrutin et d'établir la confiance dans le système mis en œuvre.

Les jeux d'argent et de hasard en ligne

L'ouverture à la concurrence et la régulation du secteur des jeux d'argent et de hasard en ligne a été l'occasion de la création de l'Autorité de régulation des jeux en ligne (Arjel), qui définit les règles applicables et attribue les agréments aux opérateurs.

La traçabilité du jeu en ligne a pour but principal de protéger les joueurs. L'Arjel a normalisé un frontal destiné à capter l'ensemble des flux de jeu en provenance du poste du joueur, et à les déposer en temps réel, sous un format normalisé, dans un coffre-fort électronique, qui en réalise un scellement cryptographique, et les met à disposition exclusive de l'Arjel pendant 12 mois.

Le scellement consiste en un cachet réalisé à l'aide d'un matériel cryptographique (HSM).

Le coffre-fort électronique doit avoir obtenu un certificat de sécurité de premier niveau (CSPN) délivré par l'ANSSI.

Les agents de l'Arjel se connectent au système *via* une authentification forte par certificat.

En cas d'indisponibilité du frontal de traçabilité, l'activité du site de jeu en ligne doit être interrompue.

Tout est donc mis en œuvre pour garantir une parfaite transparence des flux de jeu, la valeur probante des traces recueillies, ainsi qu'une parfaite disponibilité du service de traçabilité.

La dématérialisation des marchés publics

Les marchés publics sont un domaine juridique par essence, et objets de nombreux contentieux. Lorsqu'ils sont dématérialisés, la traçabilité joue donc un rôle primordial dans la sécurité juridique tant des acheteurs que des fournisseurs, chacun ayant besoin de faire la preuve de son respect des règles, en particulier en ce qui concerne les délais : durée allouée aux candidats pour prendre connaissance du dossier de consultation des entreprises et pour établir leur offre, date limite de remise des plis, date

Copyright © 2012 Eyrolles.

limite de remise des réponses aux questions par la personne publique… L'horodatage jouera donc un rôle essentiel dans l'exploitation des traces.

Le système de traçabilité mis en œuvre par une plate-forme de dématérialisation inclura la trace de l'ensemble des actions : l'envoi en publication de l'avis d'appel public à la concurrence, la mise en ligne des versions successives du cahier des charges, le dépôt des questions et l'envoi des réponses, le dépôt des candidatures et des offres.

Toutefois, selon la sensibilité de l'action effectuée, on pourra se contenter d'une traçabilité applicative en base de données, ou générer une preuve cryptographique faisant foi de l'événement.

Il est recommandé en particulier de générer une preuve cryptographique lors du dépôt de son pli par une entreprise, et de remettre à cette entreprise la preuve ainsi produite, de manière à lui permettre de disposer des éléments à valeur probatoire qui pourront être exhibés à l'appui de ses éventuelles revendications : de cette manière, la transparence garantit la confiance dans le système.

Le pli étant réputé avoir été déposé seulement quand le fichier a été entièrement reçu par la plate-forme, la preuve sera établie non au début du dépôt, mais à sa conclusion. C'est d'ailleurs indispensable pour inclure dans la preuve le hash du pli remis par le candidat.

Copyright © 2012 Eyrolles.

Chapitre 12

L'archivage électronique

Conserver à long terme les documents électroniques

Qu'est-ce que l'archivage ?

Avec la dématérialisation, la majeure partie des documents produits et échangés dans le cadre de l'activité des entreprises et des administrations sont nativement sous format électronique.

Le cycle de vie de ces documents inclut leur création, leurs évolutions, leur validation, éventuellement leur signature, leur envoi aux destinataires… mais ne s'arrête pas une fois le document transmis. La plupart d'entre eux revêtent une importance sur le long terme, de par :

- leur valeur juridique (contrats, commandes, factures, fiches de paie, ordres de mission, traces applicatives…) ;
- leur contenu technique et informationnel (spécifications, brevets…) ;
- leur valeur patrimoniale (articles, notes professionnelles…).

Ainsi, même à l'issue de son utilité immédiate au sein du projet qui a motivé sa création, un document doit être conservé dans des conditions qui permettront de le retrouver *a posteriori*, éventuellement de nombreuses années plus tard, dans le cadre de besoins qui sont ou non prévisibles lors de sa génération.

Prenons l'exemple de la construction d'un bâtiment : si, plusieurs années après l'inauguration, l'ouvrage se fissure du fait de la mauvaise qualité du béton employé, il sera important de pouvoir exhiber le cahier des charges initial pour vérifier les exigences du maître d'ouvrage en la matière et imputer la responsabilité au maître d'œuvre s'il n'a pas suivi les prescriptions, ou au donneur d'ordre si c'est lui qui s'est trompé dans le choix des matériaux.

Les enjeux économiques étant extrêmement importants dans cet exemple, il sera naturellement impossible de se contenter de retrouver sur le disque dur

Copyright © 2012 Eyrolles.

de l'acheteur un fichier datant de plusieurs années : il faudra faire la preuve que ce fichier est bien celui qui avait été transmis aux candidats au marché, et qu'il a été conservé dans des conditions de nature à en garantir l'intégrité.

À l'appui de l'authenticité du document, il sera possible de fournir également la traçabilité relative à la passation du marché, qui permettra de prouver qu'il s'agit bien de celui qui a été transmis, par exemple parce que son hash était présent dans la trace d'envoi aux candidats.

L'archivage est donc le mécanisme qui permet de garantir la pérennité des documents, tout en prouvant *a posteriori* leur authenticité et leur fidélité à l'original.

Il faut distinguer l'archivage de deux autres notions, tout aussi importantes dans le cycle de vie de l'information, mais qui n'ont pas la même finalité :

- le stockage des documents, pendant leur durée d'utilité « immédiate », dans le système de fichiers ou la GED (Gestion électronique de documents) : le but de ce dispositif est d'assurer une disponibilité rapide du document aux acteurs du processus dématérialisé, dans le contexte où il est encore « vivant » ;
- la sauvegarde des données du système d'information : l'objet de ce mécanisme est de garantir la capacité à restaurer le service avec une perte d'information minime en cas de sinistre (panne informatique ou vandalisme).

L'exemple précédent nous permet d'identifier les principaux points d'attention dans la mise en œuvre d'un système d'archivage électronique :

- les conditions de conservation doivent garantir la provenance, l'imputabilité et l'intégrité du document, mais aussi sa disponibilité permanente sur une longue période ;
- tous les documents ayant une valeur juridique, technique ou patrimoniale avérée ou potentielle doivent être archivés ;
- la durée de conservation des archives doit correspondre à la période pendant laquelle elles pourront être exploitées ;
- la recherche de documents dans les archives doit être possible même longtemps après et par quelqu'un qui n'a pas participé à la génération du document ;
- le contexte dans lequel le document a été élaboré initialement et déposé dans le système d'archivage électronique doit pouvoir être reconstitué également à partir des informations archivées ;
- les archives contenant potentiellement des données sensibles, les accès au système d'archivage électronique doivent être contrôlés de manière à garantir la confidentialité du contenu ;
- le système d'archivage électronique doit offrir la traçabilité de l'ensemble des actions effectuées sur les documents : dépôt, accès, destruction à l'issue de la période de conservation.

Copyright © 2012 Eyrolles.

Aurait-on l'idée de brûler les contrats papier dès leur signature réalisée, sous prétexte que l'acte de signature a permis de conclure la relation contractuelle ? Bien sûr que non : le contrat sera encore utile pour suivre l'exécution des obligations qui en découlent, et potentiellement au-delà en cas d'action en justice ou pour reconstituer l'historique des relations entre les parties, par exemple pour envisager un partenariat à long terme.

Dématérialiser sans archiver, c'est faire le pari que l'on n'aura plus jamais besoin de relire les documents produits. Sans un archivage bien conçu et mis en œuvre de manière systématique, la dématérialisation représente un risque démesuré pour le patrimoine informationnel de l'entreprise, et donc pour sa sécurité juridique et financière.

Une abondance de normes complémentaires

Le domaine de l'archivage électronique est normalisé par de très nombreux organismes. On peut citer, parmi les normes les plus importantes :

- la norme AFNOR NF Z42-013, mise à jour en mars 2009 sous le titre « Archivage électronique – Spécifications relatives à la conception et à l'exploitation de systèmes informatiques en vue d'assurer la conservation et l'intégrité des documents stockés dans ces systèmes », et sa transposition internationale, en 2012, sous la forme de la norme ISO 14641, « Spécifications relatives à la conception et au fonctionnement d'un système d'informations pour la conservation d'informations électroniques » ;
- le modèle OAIS (*Open Archival Information System*), normalisé sous la forme de la norme ISO 14721 ;
- le recueil d'exigences européen MoReq2010, *Model Requirements for the Management of Electronic Documents and Records*, qui se veut une déclinaison pratique de la norme ISO 15489, « Records management » ;
- le standard d'échange édité par la Direction générale de la modernisation de l'État et la Direction des archives de France, intitulé « Standard d'échange de données pour l'archivage : transfert – communication – élimination – restitution » –, et destiné à garantir l'interopérabilité des systèmes d'archivage électronique.

Par ailleurs, en France, la Fédération nationale des tiers de confiance a élaboré deux labels dans le but de certifier d'une part les tiers archiveurs, et d'autre part les solutions techniques de coffres-forts électroniques.

Qu'est-ce qu'un coffre-fort électronique ?

Le stockage des données sur un simple disque dur d'ordinateur personnel ou de serveur n'offre pas les garanties d'intégrité, de pérennité, de traçabilité et de confidentialité attendues d'un système d'archivage électronique.

Afin de satisfaire aux besoins du domaine de l'archivage, la notion rassurante de « coffre-fort électronique » a été créée pour désigner un système

Copyright © 2012 Eyrolles.

informatique garantissant, sur la base de spécifications précises et de manière certaine, l'ensemble des sécurités et des fonctionnalités nécessaires à la conservation, la recherche et la restauration à long terme des documents.

Un coffre-fort électronique est donc un système de stockage de fichiers garantissant :

- la conservation simultanée des documents et des données permettant de faire des recherches *a posteriori*, appelées « métadonnées » ou « index » ;
- l'intégrité des documents, grâce à une prise d'empreinte numérique systématique lors du dépôt ;
- leur pérennité, grâce à la redondance du stockage et à des contrôles périodiques ;
- leur confidentialité, à l'aide de mécanismes de chiffrement et de contrôle d'accès ;
- la traçabilité des accès.

La figure 12-1 reprend les différents types de données gérées au sein d'un coffre-fort électronique et montre qu'il s'agit de bien plus que d'un simple système de stockage.

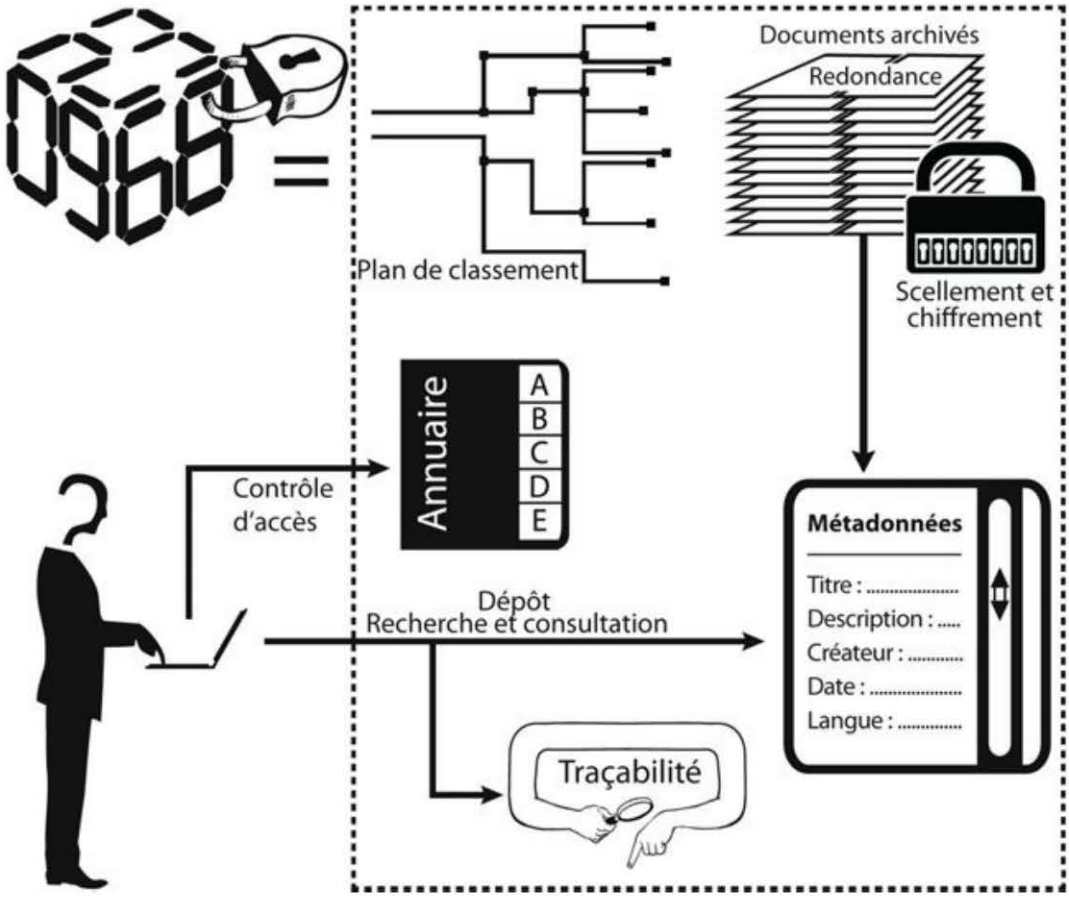


Figure 12-1 : Le coffre-fort électronique

Copyright © 2012 Eyrolles.

La conservation des documents dans un coffre-fort électronique permet de leur donner une valeur probatoire, en regard de l'article 1316-1 du Code civil qui dispose que « L'écrit sous forme électronique est admis en preuve au même titre que l'écrit sur support papier, sous réserve que puisse être dûment identifiée la personne dont il émane et qu'il soit établi et conservé dans des conditions de nature à en garantir l'intégrité. ». C'est pourquoi les termes d'« archivage légal » ou d'« archivage à valeur probatoire » sont souvent employés pour caractériser l'archivage électronique.

Parole d'expert

Alain Borghesi, PDG de Cecurity.com

Cecurity.com est l'éditeur du Coffre-fort électronique communicant (CFEC). Pourquoi parle-t-on dans l'archivage électronique de « coffre-fort électronique », alors que dans l'archivage papier, on se contente de simples boîtes d'archives ?

Il est important de se rappeler que le terme de « coffre-fort électronique » est apparu dans le débat public au début des années 2000 à propos d'un projet gouvernemental relatif à l'administration électronique. Il s'agissait de mettre à disposition des citoyens un dispositif technique leur permettant d'assurer la protection de leurs données à caractère personnel tout en leur donnant la possibilité d'autoriser les administrations à venir consulter les informations nécessaires à la réalisation des démarches administratives en ligne. Dès le départ, avant même qu'il ne soit question d'archivage, le concept de coffre-fort électronique était indissociablement lié à la confidentialité des informations et à la diffusion contrôlée de celles-ci par leur détenteur.

Parallèlement, à la faveur de la reconnaissance juridique de l'original électronique et avec l'essor des premières applications de dématérialisation, s'est posée la question de la conservation de ce nouveau type de preuve, qu'il fallait archiver dans la durée. L'usage du terme coffre-fort électronique s'est alors progressivement imposé. Il fallait rendre compte d'une réalité nouvelle : la dématérialisation des preuves rendait possible la production sans limite de copies électroniques conformes tout en faisant peser une incertitude sur la préservation de l'intégrité des documents numériques. C'est au coffre-fort électronique qu'il revient de garantir la préservation de l'intégrité des originaux électroniques.

Quelles mesures prenez-vous pour garantir aux utilisateurs du CFEC le respect des conditions de conservation des données imposées par la législation ?

Tout repose sur la mise en œuvre d'une technologie : la cryptographie, qui associe le chiffrement des données, les empreintes d'intégrité, la signature électronique ou encore les jetons d'horodatage. La mise en œuvre de cette technologie se fait dans le respect de normes relatives à l'archivage électronique à vocation probatoire, voire aux textes de référence spécifiquement consacrés au coffre-fort numérique.

Plutôt que d'autoproclamer la conformité à ces exigences normatives, nous nous efforçons d'apporter des garanties aux utilisateurs par les certifications ou les labels. C'est ainsi que les coffres-forts électroniques de Cecurity.com bénéficient du label « coffre-fort électronique » de la Fédération nationale des tiers de confiance (FNTC) ou de la Certification de sécurité de premier niveau (CSPN) délivrée par l'Agence nationale de la sécurité des systèmes d'information (ANSSI).

Copyright © 2012 Eyrolles.

Au-delà de l'archivage électronique, quelles sont les fonctions d'un coffre-fort électronique ?

Pour l'utilisateur, le coffre-fort électronique est non seulement un dispositif d'archivage électronique mais aussi une technologie de protection des données à caractère personnel, ce que les Anglo-Saxons désignent sous le terme de PET ou *Privacy Enhancing Technology*. Il permet également de donner à l'archivage une dimension active qu'il n'a pas avec le papier, en favorisant la diffusion maîtrisée par l'utilisateur de ses contenus numériques.

Pour les grandes institutions de confiance en relation avec le public, telles que les mutuelles et compagnies d'assurance, un service de coffre-fort numérique, au profit de leurs clients potentiels ou assurés, se traduit par la mise à disposition d'un service innovant qui favorise une relation dans la durée. Ces coffres-forts constituent alors le socle sur lequel se bâtiront les futures applications de dématérialisation qui seront des sources de création de valeur pour les utilisateurs et de réduction des coûts pour les entreprises proposant ce service.

Le rôle du tiers archiveur

La fonction d'archivage électronique pourra, selon le choix du propriétaire des données, être exploitée en interne ou confiée à un tiers de confiance, appelé « tiers archiveur ».

Le rôle du tiers archiveur consiste à garantir le respect de la politique d'archivage électronique, qui décrit les règles applicables au sein du système d'archivage électronique.

Des relations contractuelles précises permettront de garantir les éléments fondamentaux, en plus des propriétés fonctionnelles et techniques décrites dans la politique et les spécifications du système :

- la confidentialité doit être opposable aux personnels du tiers archiveur ;
- le tiers archiveur doit garantir à son client un accès direct au coffre-fort électronique ou un délai maximal de remise des archives demandées ;
- la réversibilité doit être prévue, c'est-à-dire que le tiers archiveur doit s'engager à remettre l'ensemble du contenu du système d'archivage électronique (documents, métadonnées, données d'intégrité et de traçabilité) à l'issue du contrat qui le lie à son client, dans un format garantissant l'interopérabilité avec d'autres systèmes techniques d'archivage électronique.

Que faut-il archiver ?

Le patrimoine informationnel de l'entreprise

Comme nous l'avons vu, l'archivage électronique a pour but la pérennisation du patrimoine informationnel de l'entreprise. Il constitue sa mémoire, mais aussi un des piliers de sa sécurité juridique.

Copyright © 2012 Eyrolles.

Lors de la conception d'un service dématérialisé, ou plus largement, du système d'information de l'entreprise, il est fondamental d'identifier tous les types de documents et de données qui ont ou auront une utilité potentielle pour l'entreprise au cours des années suivant leur création, et de les inclure dans le système d'archivage électronique.

Pour certains de ces documents, le choix est immédiat : conserver les documents RH, tels que les contrats de travail, les fiches de paie, les avenants, les ordres de mission, les demandes de congés, les courriers officiels envoyés aux employés, les comptes-rendus d'assemblées générales, est une évidence. Il en va de même pour tous les documents commerciaux générés sous forme électronique : contrats, factures, récépissés, procès-verbaux de réception et de validation, etc.

D'autres données sont tout aussi nécessaires à conserver bien que cela apparaisse moins clairement pour le novice : il s'agit des données de traçabilité provenant des différents processus dématérialisés de l'entreprise, qui ont une valeur juridique fondamentale et devront être présentés en cas de litige.

Le choix sera en revanche moins évident pour d'autres types de données. Prenons quelques exemples.

Les versions de travail des documents

Les versions successives d'un document, établies au cours de son cycle de vie, peuvent sembler moins importantes que la version finale, validée et diffusée. Pourtant, dans certains contextes, comme en Recherche et développement, ils peuvent revêtir une importance capitale : ils permettront, par exemple, de déterminer de qui provient une idée innovante au cours de l'élaboration commune d'une spécification par plusieurs partenaires. Il n'est donc pas utile de conserver les versions temporaires de documents dans le cas général, mais cela peut devenir important dans certains cas particuliers.

L'archivage des e-mails

Les e-mails entrants et sortants représentent un volume d'information très important. Si techniquement leur capture au niveau du serveur de messagerie pour stockage dans le système d'archivage électronique ne pose pas de difficulté particulière, il semble en revanche coûteux de les conserver dans leur ensemble, surtout du fait que :

- la plupart des e-mails ne contiennent pas ou peu d'information à véritable valeur ajoutée patrimoniale pour l'entreprise ;
- la recherche *a posteriori* dans une telle masse d'information relève de la métaphore de l'aiguille dans la botte de paille.

Il peut ainsi être préférable de filtrer les e-mails à archiver sur certains critères souvent complexes à définir : l'émetteur, les destinataires ou

Copyright © 2012 Eyrolles.

certains mots-clés. Il est également possible d'envisager une procédure d'archivage volontaire des messages importants par les utilisateurs, *via* un réacheminement à une adresse spécifique d'archivage.

Le code source des applications informatiques

Le code informatique est en général conservé dans un « gestionnaire de sources » qui a pour fonction d'en gérer les versions successives, et qui tient souvent lieu aux yeux des services de R&D informatique de système d'archivage, en s'appuyant sur un mécanisme de sauvegarde régulier. Il s'agit de contenus extrêmement mouvants, le code des applications restant en général vivant tant que le logiciel est exploité.

Ce code représente le fruit de l'investissement de l'entreprise : il est donc fondamental d'en réaliser un archivage périodique.

Nota Bene : dans un but de pérennisation des données, il est également possible de procéder à un dépôt du code source des applications auprès de l'Agence pour la protection des programmes. Cet « entiercement » offre en outre des garanties en termes de propriété intellectuelle.

Les types d'archives de la Direction des archives de France

Le décret n° 79-1037 du 3 décembre 1979 relatif à la compétence des services d'archives publics et à la coopération entre les administrations pour la collecte, la conservation et la communication des archives publiques, mis à jour le 27 mai 2011, définit le rôle de la Direction des archives de France dans l'archivage des données publiques, et définit dans ses articles 12 à 14 trois types d'archives et les conditions de leur conservation :

- les archives courantes ;
- les archives intermédiaires ;
- les archives définitives.

Sans constituer un standard absolu, ces notions sont intéressantes à prendre en compte dans la conception d'un système d'archivage électronique.

Décret n° 79-1037 du 3 décembre 1979

Article 12

Sont considérés comme archives courantes les documents qui sont d'utilisation habituelle pour l'activité des services, établissements et organismes qui les ont produits ou reçus.

La conservation des archives courantes incombe, sous le contrôle de la Direction des archives de France, aux services, établissements et organismes qui les ont produites ou reçues.

Copyright © 2012 Eyrolles.

Article 13

Sont considérés comme archives intermédiaires les documents qui :

a) ont cessé d'être considérés comme archives courantes ;

b) ne peuvent encore, en raison de leur intérêt administratif, faire l'objet de tri et d'élimination [...].

La conservation des archives intermédiaires peut être assurée dans des dépôts spéciaux, dits « dépôts de préarchivage », gérés par la Direction des archives de France ou placés sous son contrôle.

À défaut de préarchivage, les archives intermédiaires sont conservées soit dans les locaux de leur service, établissement ou organisme d'origine, sous le contrôle de la Direction des archives de France, soit dans les dépôts d'archives relevant de la Direction des archives de France.

Article 14

Sont considérés comme archives définitives les documents qui ont subi les tris et éliminations définis ci-dessous [...] et qui sont à conserver sans limitation de durée.

La conservation des archives définitives est assurée dans les dépôts d'archives relevant de la Direction des archives de France ou placés sous son contrôle.

Le format des documents

Il n'existe pas de restriction concernant les formats qu'un système d'archivage électronique peut conserver.

Afin de garantir l'intégrité et la fidélité des documents, il est fondamental de les archiver dans leur format d'origine : toute conversion entraîne nécessairement une perte d'intégrité. Ce fait est particulièrement sensible pour les documents comportant un scellement cryptographique ou une signature électronique : ces données seront invalidées par toute modification du document, y compris une conversion de format.

Toutefois, l'un des buts de l'archivage est de garantir la lisibilité des documents sur le long terme : si un document provient d'un logiciel peu usité, ou est généré à un format qui tombe en obsolescence, comment pourra-t-on le relire dans quinze ou vingt ans ?

Une solution consiste à archiver également le logiciel qui permet de relire les documents. Toutefois, il faut également envisager d'archiver le système d'exploitation qui permet d'exécuter ce logiciel… Qui peut ne plus pouvoir être exécuté sur des ordinateurs trop modernes !

Une seconde solution consiste à archiver, conjointement avec le document, une image fidèle de celui-ci dans un format considéré comme pérenne. C'est l'objectif qu'a poursuivi la société Adobe en normalisant le format PDF (*Portable Document Format*), en particulier dans sa version PDF/A dédiée à l'archivage électronique. La spécificité des documents PDF/A est de contenir l'ensemble des éléments nécessaires à leur affichage, notamment

Copyright © 2012 Eyrolles.

les polices de caractères. L'usage de la transparence y est interdit afin de ne pas avoir d'ambiguïté d'interprétation à l'affichage.

Attention : l'original du document restera la version archivée dans son format natif, et la sauvegarde sous un autre format (PDF, TIFF, TXT…) n'en constituera qu'une copie.

Examinons à titre d'exemples les choix effectués par deux professions réglementées : les huissiers de justice et les notaires.

Les huissiers de justice ont fait le choix de constituer les actes authentiques au format PDF/A. Le document PDF, signé électroniquement par l'huissier au format S/MIME à l'aide d'un certificat qualifié, est associé à un ensemble de métadonnées au format XML avant dépôt dans le système d'archivage électronique appelé le « minutier central des huissiers ».

Les notaires, quant à eux, ont fait le choix de conserver les actes authentiques d'une part sous un format PDF/A et d'autre part, dans un format texte, sans mise en forme. Le format TXT étant le plus simple possible, sa pérennité est absolument garantie. Les deux documents sont inclus dans un fichier au format XML qui contient également les annexes sous forme d'images, les métadonnées et la signature électronique réalisée avec un certificat qualifié. Ces données sont conservées 75 ans dans le minutier central des notaires.

À quel moment faut-il mettre en œuvre l'archivage électronique ?

Du fait de l'enjeu de conservation du patrimoine informationnel de l'entreprise et de la nécessité de pouvoir reconstituer le contexte global dans lequel les documents ont été constitués et archivés, l'archivage électronique constitue une problématique transverse au système d'information.

En principe, tout système d'information devrait disposer, dès sa conception, d'un système d'archivage électronique.

Dans la pratique, le besoin d'archivage électronique est le plus souvent identifié à l'occasion de l'inclusion dans le système d'information de procédures dématérialisées à forte connotation juridique, qu'elles soient internes (ressources humaines, par exemple), ou externes (dématérialisation fiscale des factures, dématérialisation des marchés ou des contrats, e-commerce…).

Dans le cadre de ces projets de dématérialisation, la gestion des coûts et des délais pousse souvent la maîtrise d'ouvrage à reléguer dans un lot tardif la mise en œuvre de l'archivage, qui arrive fonctionnellement en bout de chaîne, et dont l'utilité correspond à des cas d'usage de l'information souvent oubliés au cours de la conception fonctionnelle, puisque concernant en général des populations d'utilisateurs différentes de celles directement impliquées dans le « métier » du service dématérialisé.

Copyright © 2012 Eyrolles.

Il s'agit d'une erreur dans la conduite de projet ! De même que la traçabilité ou la sécurité de l'infrastructure technique, l'archivage doit être pensé et mis en œuvre dès les premières phases du projet, dans un esprit de mutualisation avec les autres applications du système d'information. Ouvrir le service dématérialisé sans la fonctionnalité d'archivage en se disant qu'« on l'ajoutera après » est systématiquement source de perte de données (fichiers, mais aussi métadonnées et éléments de contexte) et de constitution d'un référentiel d'archivage incohérent et incomplet, difficile à exploiter par la suite.

Définir un plan d'archivage

La nécessité du plan d'archivage

Du fait de la masse très importante de documents générés au sein du système d'information, et notamment des services dématérialisés, il serait vain de les stocker « en vrac » dans un espace d'archivage non structuré.

Le plan d'archivage a pour but de permettre aux utilisateurs du système d'archivage de procéder à des recherches au sein des archives, afin de retrouver les documents sur la base de plusieurs critères :

- un plan de classement, qui consiste à ranger les différents documents dans une arborescence qui reflète leur organisation logique ;
- des métadonnées, c'est-à-dire des « données relatives aux données », aussi appelées « index d'archivage ».

Outre ces éléments, le plan d'archivage définit également, pour chaque type de document, le moment de son dépôt dans le système d'archivage électronique, la durée de sa conservation et les conditions de sa suppression.

Il définit aussi les procédures d'accès aux archives.

Lorsque l'archivage est effectué pour une procédure dématérialisée ouverte sur l'extérieur, il est utile de publier les règles appliquées en déclinant le plan d'archivage sous la forme d'une politique d'archivage électronique, qui fait partie de la convention de preuve du service.

Nous allons maintenant détailler les différents aspects du plan d'archivage.

Le plan de classement

Le plan de classement est l'équivalent du rangement dans des répertoires au sein d'un système de fichiers. Il sert à regrouper les archives selon une logique qui peut être métier (documents de même nature), organisationnelle (documents de même provenance), technique (documents de même format)… La détermination du plan de classement découlera logiquement de l'étude menée sur la façon d'accéder aux données *a posteriori*.

Copyright © 2012 Eyrolles.

On pourra, par exemple, avoir au sein du coffre-fort d'archivage un dossier « ressources humaines » contenant des sous-dossiers « contrats de travail », « fiches de paie », « ordres de mission », « demandes de congés », etc.

À titre d'illustration, le téléservice Réseaux et canalisations de l'Ineris a opté pour un plan de classement en trois sous-parties distinguant :

- les documents métier ;
- les documents contractuels (incluant les politiques de sécurité et les conditions générales d'utilisation) ;
- les documents de traçabilité.

Les métadonnées

Les métadonnées sont les index à partir desquels il sera possible d'effectuer des recherches sur les documents archivés.

Il est important de les concevoir avec une grande richesse, de manière à s'assurer de pouvoir rechercher dans plusieurs années dans des contextes qu'il n'est pas nécessairement possible d'imaginer au moment de la conception du système d'archivage électronique.

Les métadonnées incluent :

- des valeurs (titre du document, montant d'un contrat…) ;
- des mots-clés ;
- des dates ;
- des identifiants de personnes ou d'entreprises…

Il peut être intéressant d'avoir la possibilité de multivaluer certains index. Ainsi, par exemple, si un document concerne plusieurs utilisateurs (par exemple, un contrat multipartite), il sera archivé avec les identifiants de tous ces utilisateurs, de manière à être retrouvé en cas de recherche concernant chacun d'entre eux. Selon l'implémentation choisie, on pourra mettre plusieurs données dans le même champ (un champ « signataires » comprendra les noms de tous les signataires), ou mettre autant de champs « signataire » qu'il y a de signataires, chacun ne comportant qu'un nom.

Reprenons l'exemple du système d'archivage « ressources humaines » : on pourra reconstituer la carrière d'un employé en recherchant dans l'ensemble du dossier « ressources humaines » les documents relatifs à cet employé sur la base de son matricule ou de son nom, à condition que le matricule et le nom du ou des agents concernés aient été systématiquement inclus dans les métadonnées pour tous les types de documents.

Dans le but de favoriser l'interopérabilité des systèmes de gestion électronique de documents, un ensemble de métadonnées a été standardisé dans la norme ISO 15836 sous le nom de « Dublin Core ». Orienté « propriété

Copyright © 2012 Eyrolles.

intellectuelle », il peut servir de base à la définition de l'indexation d'un système d'archivage électronique. Les éléments en sont les suivants :

- titre ;
- créateur ;
- sujet ;
- description ;
- éditeur ;
- contributeur ;
- date ;
- type de ressource ;
- format ;
- identifiant de ressource ;
- source ;
- langue ;
- relation ;
- couverture ;
- droits.

Définir le moment de l'archivage

Selon la nature des documents, le moment de leur archivage pourra être différent. L'important est que l'archivage soit systématique et conforme au plan d'archivage défini, afin de s'assurer de ne pas avoir de perte de données.

Prenons quelques exemples pour illustrer les différents moments d'archivage.

Un document généré automatiquement au cours d'un processus dématérialisé, puis signé électroniquement par un utilisateur pour être acheminé à un destinataire sera archivé dès que la signature y a été apposée. En effet, une fois signé, le document n'est plus susceptible d'être modifié. Cette version est figée, et peut être archivée immédiatement, même s'il reste « vivant » dans le processus puisqu'il donne encore lieu à des échanges, accusés de réception, etc.

Les traces applicatives générées par une application donneraient lieu à un très grand nombre d'enregistrements si l'on archivait chaque trace indépendamment. En général, on se contente donc de regrouper quotidiennement les traces réalisées la veille dans un seul fichier, qui donne lieu à un archivage unique. Nous avons évoqué dans le chapitre 11 sur la traçabilité un cas où ce regroupement n'est pas possible : les jeux d'argent et de hasard, dans lesquels la notion de temps réel est fondamentale pour

Copyright © 2012 Eyrolles.

permettre les contrôles au fil de l'eau. Chaque trace est alors déposée dès sa génération dans le coffre-fort électronique de l'Autorité de régulation des jeux en ligne. C'est également cette règle de simultanéité de la génération et de l'archivage qui sera appliquée pour les preuves cryptographiques.

Le code source des applications informatiques pourra, par exemple, être archivé sous la forme d'une archive globale une fois par mois, ou à une fréquence plus élevée, selon la volumétrie générée.

Le plan d'archivage décrira donc, pour chaque type de document, le lieu de son archivage (plan de classement), ses index (métadonnées) et le moment de son dépôt dans le système d'archivage électronique. Le dernier élément propre à chaque type de document, que nous abordons maintenant, est la durée de conservation de l'archive.

Prévoir la suppression des archives

La durée de conservation des archives dépend de plusieurs critères complémentaires :

- pour certaines activités, il existe un délai de conservation légal. Par exemple, les contrats conclus avec un particulier pour un montant supérieur à 120 euros sont conservés 10 ans, en respect de l'article L.134-2 du Code de la consommation, les factures 10 ans au titre de l'article L.123-22 du Code de commerce, etc. ;
- si les documents contiennent des données à caractère personnel (par exemple, les données de traçabilité), la durée de conservation doit être la durée nécessaire au traitement, justifiée par sa finalité ;
- les données patrimoniales, qui peuvent avoir un intérêt culturel, comme les plans des ouvrages d'art, sont conservées sans limitation de durée.

Lors de la définition du moment de suppression des archives, il faut être prudent car le délai de conservation ne commence pas nécessairement au moment de l'archivage. Ainsi, les données relatives au compte d'un utilisateur pourront être conservées un an à l'issue de la fin d'activité de ce compte, et non à compter de sa création.

La suppression des archives doit donc être prise en compte dès la conception du système d'archivage électronique, et répond à un double impératif de respect des obligations légales et de libération d'espace de stockage.

Définir les procédures d'accès aux archives

Le but premier de l'archivage est bien entendu de permettre à leur propriétaire de les retrouver. Il convient donc de définir avec attention les modalités d'accès, dans le souci de plusieurs critères complémentaires : permettre la recherche, garantir le restauration et respecter la confidentialité.

Copyright © 2012 Eyrolles.

Permettre la recherche

Le premier élément à prendre en compte est la capacité de recherche. La recherche ne s'effectue pas directement sur les documents, mais sur le plan de classement et les métadonnées. Si l'indexation a été conçue de manière riche, il sera nécessaire de disposer d'un moteur de recherche ou d'un requêteur sur la base de l'ensemble des index, permettant de faire des recherches croisées de manière à retrouver tous les éléments liés à un même contexte. Ainsi, la reconstitution du contexte de la génération et de la signature électronique d'un document au sein d'un processus dématérialisé pourra nécessiter de retrouver :

- le document signé ;
- les traces applicatives et preuves cryptographiques relatives aux actions ayant amené à son élaboration ;
- éventuellement, les traces relatives aux traitements ultérieurs (envoi, réception…) ;
- les conditions générales d'utilisation (CGU) du service en vigueur au moment de l'action ;
- la preuve de la validation de ces CGU par l'utilisateur concerné…

Ces différents éléments seront vraisemblablement archivés à des emplacements différents, selon le plan de classement.

La procédure de reconstitution d'un tel « dossier de preuves » peut passer par plusieurs recherches successives, mais elle ne sera en tout état de cause possible que si le plan d'indexation est suffisamment complet et cohérent, et si les interfaces de recherche offrent la souplesse nécessaire. Faute de quoi, la complémentarité des documents sera perdue, et le contexte d'origine ne pourra pas être reconstitué, ce qui induit une perte d'information et de valeur juridique importante.

Garantir la restauration

Une fois le ou les documents identifiés au sein du système d'archivage électronique, il est nécessaire de les en extraire pour les remettre à l'utilisateur qui les demande.

Cette extraction peut, selon les cas, être réalisée en temps réel par l'utilisateur lui-même, s'il en a les droits, ou en temps différé par le service des archives ou un tiers archiveur.

Le plan d'archivage prévoira les procédures d'extraction et de remise au demandeur, dans le respect des règles de confidentialité et de délais raisonnables tant du point de vue du service des archives que du point de vue du demandeur.

La restauration des fichiers devra conserver leur intégrité, en particulier en ce qui concerne le nom original du fichier, qui est parfois remplacé par

Copyright © 2012 Eyrolles.

un nom technique pour les besoins de conservation au sein du coffre-fort électronique.

Optionnellement, il sera possible d'extraire, en même temps que le document, l'ensemble des métadonnées qui lui sont attachées, qui seront, par exemple, remises au format XML.

Respecter la confidentialité

La confidentialité recouvre deux contraintes complémentaires.

Tout d'abord, les données archivées ne doivent pas être accessibles librement, et en interne, les accès doivent être limités aux personnels autorisés. Si l'archivage a été confié à un tiers archiveur, une clause de confidentialité doit être prévue, ainsi que des mesures techniques garantissant le respect de cette exigence.

On envisagera également la problématique de la confidentialité au cours du transfert des documents depuis le service des archives jusqu'à leur demandeur. L'emploi d'un moyen de transmission sécurisé est souhaitable pour éviter la divulgation de documents sensibles.

En second lieu, la demande de restauration d'une archive ne doit pouvoir être faite que par une personne habilitée à consulter le document. Un membre de la direction R&D, par exemple, ne sera pas habilité à consulter un contrat passé par l'entreprise avec un de ses clients. En revanche, il pourra consulter un contrat passé par l'entreprise avec un de ses fournisseurs si l'activité de ce fournisseur concerne la R&D.

La gestion des droits d'accès aux archives fait partie du plan d'archivage, et peut être effectuée soit par l'intermédiaire du plan de classement, en gérant des droits sur les différents répertoires comme on le fait sur un serveur, soit par l'intermédiaire de l'indexation, les droits d'accès étant une métadonnée du document. C'est d'ailleurs ce qui est prévu dans l'indexation Dublin Core.

Il convient, lors de la définition des droits d'accès, de les penser de manière générique, c'est-à-dire de les rattacher à des fonctions et non à des personnes, dont la pérennité et le rôle dans l'entreprise ne sont jamais certains.

Copyright © 2012 Eyrolles.

Chapitre 13

La convention de preuve

Une convention de preuve... Pour quoi faire ?

Le fondement juridique de la convention de preuve

La directive 1999/93/CE du Parlement européen et du Conseil du 13 décembre 1999, sur un cadre communautaire pour les signatures électroniques, introduit la notion de convention de preuve relative à la signature électronique.

Directive 1999/93/CE – Considérant 16

Un cadre réglementaire n'est pas nécessaire pour les signatures électroniques utilisées exclusivement à l'intérieur de systèmes résultant d'accords volontaires de droit privé entre un nombre défini de participants ; il est nécessaire que la liberté des parties de convenir entre elles des modalités et conditions dans lesquelles elles acceptent les données signées électroniquement soit respectée dans les limites autorisées par le droit national ; il convient de reconnaître l'efficacité juridique des signatures électroniques utilisées dans de tels systèmes et leur recevabilité comme preuves en justice.

Ainsi, en ce qui concerne la signature électronique, le droit européen met en avant la capacité des acteurs privés à établir des règles qui leur sont propres. Pourvu que ces règles respectent le droit national, les signatures électroniques réalisées selon la convention de preuve privée doivent disposer d'une valeur probatoire auprès des tribunaux.

Ce principe a été transposé dans le droit français par la loi du 13 mars 2000, qui a instauré l'article 1316-2 du Code civil.

Copyright © 2012 Eyrolles.

Code civil – Article 1316-2

Lorsque la loi n'a pas fixé d'autres principes, et à défaut de convention valable entre les parties, le juge règle les conflits de preuve littérale en déterminant par tous moyens le titre le plus vraisemblable, quel qu'en soit le support.

Cet article, qui s'inscrit dans le cadre global de la loi du 13 mars 2000, ne concerne pas seulement la signature électronique, mais plus largement les preuves par écrit, qu'elles soient sous forme papier ou sous forme électronique. Il s'applique donc à tous les domaines où l'établissement d'une preuve peut être nécessaire, ce qui en fait une base inévitable pour tous les projets de dématérialisation, aussi bien pour les questions de signature électronique que de traçabilité, d'imputabilité ou d'archivage des documents.

Le texte distingue deux cas :

- soit la loi fixe les principes (par exemple, pour les marchés publics, l'arrêté du 28 août 2006 précise quelles familles de certificats peuvent être employées pour signer l'acte d'engagement) ;
- soit la loi ne fixe pas de principe.

Dans le premier cas, il faut bien entendu suivre les prescriptions de la loi.

Dans le second cas, le concepteur d'un service dématérialisé a le choix :

- il pourra s'en remettre au juge pour trancher les cas de contentieux, ce dernier étant souverain pour décider, parmi les éléments à sa disposition, de ceux qui établissent la preuve la plus vraisemblable ;
- il peut établir une convention de preuve déterminant à l'avance les règles applicables en termes d'établissement, de gestion et d'interprétation des preuves littérales établies dans le cadre du service.

Parole d'expert

Me Éric Caprioli, avocat à la Cour de Paris, docteur en droit, membre de la délégation française aux Nations Unies sur le commerce électronique

Pourquoi est-il important de mettre en œuvre une convention de preuve lorsqu'on conçoit un service dématérialisé ?

La convention de preuve a pour but de prévoir juridiquement de quelle façon la preuve sera préconstituée et admissible en cas de litige. Elle décrit les modalités techniques à suivre afin d'établir, conserver et produire les preuves. La convention de preuve peut également permettre de renverser la charge de la preuve entre les deux parties. Elle constitue, lorsqu'elle est rédigée de manière juridiquement cohérente, un outil de sécurité juridique pour les professionnels (un élément de prévisibilité). De plus, après de nombreuses jurisprudences de la Cour de cassation depuis plusieurs décennies, la convention de preuve est consacrée par l'article 1316-2 du Code civil, avec la loi du 13 mars 2000, mais elle doit être valable.

Copyright © 2012 Eyrolles.

En d'autres termes, elle doit respecter les règles d'ordre public (ex : clauses abusives), elle doit également être précise, tout en restant suffisamment générale pour permettre d'admettre dans la durée de nouveaux moyens techniques.

En cas de contentieux, existe-t-il un risque que la convention de preuve ne soit pas suivie par le juge ?

Oui, il existe un risque. Ainsi, si le juge considère que la convention de preuve figurant dans un contrat entre un particulier et un professionnel constitue une clause abusive définie par l'article L.132-1 du Code de la consommation comme celle « qui a pour objet ou pour effet de créer, au détriment du non professionnel ou du consommateur, un déséquilibre significatif entre les droits et les obligations des parties au contrat », celle-ci pourra être réputée non écrite. La clause litigieuse (non valable) serait annulée par le juge. Le régime légal (et non contractuel) trouverait à s'appliquer et les preuves du professionnel ne seraient alors reçues qu'à titre d'éléments de preuve (au même titre que les preuves du consommateur). Il serait alors important, pour le professionnel, de démontrer la fiabilité technique du procédé de signature électronique et sa conformité juridique aux textes en vigueur (par une documentation exhaustive du processus de dématérialisation, la délivrance de certifications, labellisations, etc.), ce qui sera moins aisé sans cette convention de preuve.

Quels sont les éléments clés à prendre en compte pour garantir la validité d'une convention de preuve ?

Il est important que la rédaction des conventions de preuve soit proportionnée et équilibrée.

Dans les rapports entre particuliers et professionnels : outre les exigences du droit de la consommation, une convention de preuve doit prévoir de ne pas exclure les autres moyens de preuve. Le professionnel doit respecter le caractère contradictoire du débat probatoire : le consommateur doit pouvoir rapporter une preuve contraire. En effet, le nouvel article R132-2 du Code de la consommation énonce :

« Dans les contrats conclus entre des professionnels et des non-professionnels ou des consommateurs, sont présumées abusives au sens des dispositions du premier et du deuxième alinéas de l'article L.132-1, sauf au professionnel à rapporter la preuve contraire, les clauses ayant pour objet ou pour effet de : [...]

9° Limiter indûment les moyens de preuve à la disposition du non-professionnel ou du consommateur ».

En outre, la convention de preuve doit énoncer les éléments techniques qui vaudront preuve devant les tribunaux (certificats, signatures électroniques, enregistrements informatiques, jetons d'horodatage, données de connexion...).

Dans les rapports entre professionnels : la rédaction de la convention de preuve est plus libre étant donné que les règles protectrices des consommateurs ne trouveraient pas à s'appliquer. Cela ne signifie pas pour autant qu'il ne faut suivre aucune règle (ex : l'interdiction de ne pas pouvoir rapporter la preuve contraire). Pour bien faire, il faut prévoir que le processus du service dématérialisé puisse être audité par un tiers et que la convention de preuve repose sur des éléments techniques fiables. Mais entre commerçants, ce sont les parties qui sont libres de déterminer les preuves recevables, le plus souvent en fonction de leurs usages et de leurs besoins par rapport à la sensibilité de leurs échanges.

Copyright © 2012 Eyrolles.

Nous allons maintenant voir quelle est l'utilité pratique d'une convention de preuve.

Le but de la convention de preuve

Une convention de preuve est un ensemble de règles, sur lesquelles des parties à un contrat se mettent d'accord, dans le but d'organiser par avance la façon dont seront réglés, à l'amiable ou devant les tribunaux, d'éventuels conflits portant sur la valeur probatoire des écrits.

L'objectif de la convention de preuve est donc de réduire le risque juridique lié à la dématérialisation, de deux manières.

Tout d'abord, il s'agit de réduire le nombre de contentieux. L'établissement de règles claires permet de diminuer le nombre d'ambiguïtés, et de laisser le moins de place possible à l'interprétation… voire à la mauvaise foi.

En second lieu, la convention de preuve permet de réduire l'aléa juridique, donc économique, lié à la dématérialisation. En effet, si le traitement amiable d'un contentieux échoue et si le conflit est porté devant un tribunal, le juge prend sa décision de manière souveraine (dans la pratique, un expert judiciaire sera nommé et donnera son avis). La durée et l'issue d'un tel procès étant indécises, il est préférable de créer les conditions d'application d'une règle prédéfinie contractuellement, que le juge prendra en compte en vertu de l'article 1316-2 du Code civil, comme nous l'avons vu précédemment.

La convention de preuve est donc un outil juridique qui permet de lever le caractère arbitraire des preuves établies par l'une des parties, en définissant les conditions d'établissement et de conservation des preuves électroniques produites.

Dans le but de renforcer l'efficacité de la convention de preuve, il est souhaitable de prévoir un audit des conditions de sa mise en œuvre effective dans le service dématérialisé. Pour aller plus loin, il est possible de faire certifier ou qualifier le système de gestion de preuves afin d'accroître encore sa légitimité.

Constituer une convention de preuve

Bien rédiger la convention de preuve

Il est fondamental qu'une convention de preuve soit rédigée de manière très claire et précise : plus elle sera explicite, moins le risque d'ambiguïté ou d'interprétation sera élevé.

Bien que la dématérialisation soit un domaine technique, il convient de rendre les règles qui la régissent le plus facile d'accès possible pour les utilisateurs, en gardant en mémoire le fait que l'on ne pourra pas, en cas

Copyright © 2012 Eyrolles.

de contentieux, se camoufler derrière un galimatias technique pour « faire passer n'importe quoi ». Les deux articles suivants du Code civil permettent d'illustrer ce fait.

Code civil – Article 1156

On doit, dans les conventions, rechercher quelle a été la commune intention des parties contractantes, plutôt que de s'arrêter au sens littéral des termes.

Ainsi, si les notions techniques évoquées, éventuellement difficiles à comprendre pour un utilisateur, sont correctes, mais ne servent pas l'objet de la convention de preuve, par exemple dans son but d'équilibre de l'accès aux éléments probants pour les parties, le juge sera à même d'interpréter le texte selon son esprit et non selon la lettre.

Il convient d'être d'autant plus prudent que l'article 1162 du Code civil donne raison, en cas d'interprétation, à celui qui aura accepté la convention de preuve plutôt qu'à celui qui l'aura rédigée.

Code civil – Article 1162

Dans le doute, la convention s'interprète contre celui qui a stipulé et en faveur de celui qui a contracté l'obligation.

Afin de faciliter l'applicabilité de la convention de preuve, on fera attention dans sa rédaction aux éléments suivants :

- être extrêmement clair et explicite ;
- ne pas aller à l'encontre des règles de droit ;
- l'imposer à l'ensemble des parties au contrat, c'est-à-dire à tous les types d'utilisateurs du service dématérialisé et à celui qui le fournit ;
- la concevoir de manière équilibrée, afin de conférer à chacune des parties des moyens de défendre son point de vue : en particulier, faire attention aux clauses abusives.

Les clauses abusives concernent les relations entre professionnels et particuliers, comme l'indique le Code de la consommation.

Code de la consommation – Article L132-1

Dans les contrats conclus entre professionnels et non-professionnels ou consommateurs, sont abusives les clauses qui ont pour objet ou pour effet de créer, au détriment du non-professionnel ou du consommateur, un déséquilibre significatif entre les droits et obligations des parties au contrat.

L'établissement d'une convention de preuve ne permet donc pas d'imposer aux utilisateurs d'un service dématérialisé des règles d'établissement de la

Copyright © 2012 Eyrolles.

preuve qui donnent toute liberté au fournisseur du service, ou qui exonère le fournisseur de services de toute obligation.

Afin d'éviter tout soupçon d'arbitraire, la convention de preuve doit décrire de manière détaillée et précise le mode d'administration de la preuve, la façon dont les preuves électroniques sont générées, conservées, vérifiées et interprétées.

La sincérité et la crédibilité de la preuve résulteront d'une description des procédés mis en œuvre à la fois techniquement rigoureuse, et suffisamment vulgarisée pour être compréhensible pour l'ensemble des parties.

Où placer la convention de preuve ?

La convention de preuve a une nature contractuelle. S'il existe un contrat signé entre les parties, elle y trouvera naturellement sa place. Certains des éléments constitutifs de la convention de preuve, comme les politiques de sécurité, pourront être placés en annexes sous la forme de documents indépendants. Nous détaillerons ces éléments dans la section suivante « Que faut-il inclure dans la convention de preuve ? ».

Dans le cas où il n'existe pas de contrat signé entre les parties, par exemple pour un service grand public ou pour un service ouvert gratuitement à des utilisateurs professionnels, comme une plate-forme de dématérialisation des marchés publics, la convention de preuve peut être incluse dans les conditions générales d'utilisation (CGU) du service.

L'acceptation des CGU forme un contrat, même en l'absence de signature. On sera donc attentif à bien tracer l'acceptation des CGU par chaque utilisateur, de manière à pouvoir prouver l'établissement du contrat et donc l'applicabilité de la convention de preuve.

Il existe une exception, établie par l'ordonnance n° 2005-1516 du 8 décembre 2005, relative aux échanges électroniques entre les usagers et les autorités administratives, et entre les autorités administratives.

Ordonnance n° 2005-1516 – Article 4

Les autorités administratives peuvent créer [...] des téléservices. Lorsqu'elles mettent en place un tel service, les autorités administratives rendent accessibles depuis ce dernier la décision le créant ainsi que ses modalités d'utilisation, notamment les modes de communication possibles. Ces modalités s'imposent aux usagers.

Dans le cas des téléservices administratifs, l'usager n'a pas à « valider » les CGU, mais il doit en avoir connaissance. Il est souhaitable de lui faire confirmer le fait qu'il en ait pris connaissance, et de tracer cette confirmation.

En cas de modification substantielle de la convention de preuve, le fournisseur du service dématérialisé portera cette modification à la connaissance de l'ensemble des utilisateurs, par voie d'avenant au contrat ou d'une

Copyright © 2012 Eyrolles.

nouvelle validation des CGU, qui donnera bien entendu lieu à une traçabilité.

Dans tous les cas, une bonne pratique consiste, dans un but de transparence, à publier la convention de preuve soit dans un espace public du site, soit dans une zone accessible à l'ensemble des utilisateurs identifiés.

Les éléments constitutifs de la convention de preuve étant en eux-mêmes des éléments de preuve, il est recommandé de les sceller par un cachet et de les horodater, ainsi que de les conserver dans un coffre-fort électronique afin de pouvoir dûment identifier la personne dont elle émane, et prouver qu'elle a été conservée dans des conditions de nature à garantir son intégrité.

Que faut-il inclure dans la convention de preuve ?

Un dispositif à tiroirs

Une convention de preuve est classiquement constituée de plusieurs parties :

- la convention à proprement parler, qui détermine quelles sont les obligations de chacune des parties en matière de preuve : quels éléments générés dans le cadre du service font foi, dans quelles conditions ils sont produits, mis à disposition des autres parties et conservés ;
- pour chacun de ces éléments de preuve, selon sa nature, une politique décrivant les modalités précises de leur production et de leur interprétation ;
- pour chaque politique, une déclaration de pratiques pourra être rédigée afin de décrire précisément les mesures techniques mises en œuvre à l'appui de la politique.

Les politiques classiquement rédigées, et que nous détaillerons par la suite, sont les suivantes :

- politique d'horodatage ;
- politique de certification ;
- politique de signature électronique ;
- politique de cachet ;
- politique de traçabilité et de gestion de preuves ;
- politique d'archivage électronique.

Les politiques de sécurité qui constituent la convention de preuve doivent être conçues conjointement car elles sont fortement interdépendantes.

En règle générale, les politiques sont des documents de nature fonctionnelle, décrivant les engagements pris en termes métier, ainsi que les normes respectées dans le cadre du service.

Elles sont rendues publiques et incluses dans la convention de preuve sous forme d'annexes.

Copyright © 2012 Eyrolles.

En revanche, les déclarations de pratiques sont des documents techniques, conservés par le fournisseur du service, qui servent à l'appui des audits, et peuvent être remis aux parties sur demande motivée, de manière à garantir la confidentialité du savoir-faire du prestataire de services.

Les politiques seront des documents de nature assez différente selon qu'il s'agit de décrire des services de sécurité purement techniques, comme l'horodatage, ou les pratiques directement accessibles par l'utilisateur du service, comme la signature électronique.

Les services de sécurité mis en œuvre à l'appui de la convention de preuve sont souvent interdépendants. Ainsi, une signature électronique ou un cachet inclura un horodatage, une preuve, comportant un cachet et un horodatage, donnera lieu à un archivage électronique, qui lui-même pourra comporter un horodatage… Sans oublier qu'un jeton d'horodatage est lui-même scellé par un certificat émis en respect d'une politique de certification !

Il convient donc de concevoir l'ensemble des politiques de manière cohérente, avec des renvois explicites de l'une à l'autre. Afin de garantir l'intégrité de l'ensemble, il faut faire attention à ne pas reprendre les éléments d'une politique dans une autre, au risque d'introduire des incohérences en cas de modification des règles établies ou des pratiques.

Voyons maintenant les grandes lignes des différentes politiques à rédiger en fonction des besoins du projet.

La politique d'horodatage

La politique d'horodatage décrit les obligations qui résultent de la génération de jetons d'horodatage. On peut également rédiger une politique d'horodatage pour l'horodatage simple consistant à apposer une date sur un document ou dans une base de données.

Le RGS fournit une politique d'horodatage type, qui décrit les pratiques à adopter pour être conforme au niveau de sécurité (*).

Si le service dématérialisé s'appuie sur un prestataire de services d'horodatage électronique externe, la convention de preuve renverra à la politique d'horodatage de ce prestataire.

La politique d'horodatage doit inclure au moins les éléments suivants :

- la sémantique attachée à la production d'un jeton d'horodatage (situer dans le temps un événement, garantir l'antériorité d'un document…) ;
- les obligations du prestataire et des utilisateurs des jetons d'horodatage ;
- les règles de gestion des clés servant à produire les jetons d'horodatage, y compris leur fin de vie et la vérification de leur révocation ;
- le format des jetons d'horodatage, leur contenu, les algorithmes utilisés ;
- les conditions de production des jetons d'horodatage ;

Copyright © 2012 Eyrolles.

- les règles de vérification des jetons d'horodatage ;
- les garanties relatives à la fiabilité de la date et de l'heure des jetons d'horodatage ;
- les assurances ;
- les conditions éventuelles d'audit.

Cette liste n'est évidemment pas exhaustive. On adaptera le contenu de la politique d'horodatage en fonction de la réalité du service offert.

Il convient de conformer les engagements pris aux moyens effectivement mis en œuvre pour remplir ces obligations. Ainsi, un service d'horodatage qui a pour but de garantir une date à la journée près, pour des événements ne se produisant que pendant les heures ouvrables, ne nécessite pas une précision d'une milliseconde : il sera possible de se contenter d'un engagement de précision d'une minute et de préciser ce niveau de fiabilité dans la politique d'horodatage.

La politique de certification

La politique de certification décrit les obligations qui résultent de la génération de certificats.

Le RGS fournit des politiques de certification types, à appliquer en fonction des usages du certificat : authentification de serveur, authentification de personne physique, signature électronique, confidentialité, cachet, ou usage mixte (authentification et signature électronique). Chacune de ces politiques est déclinée en fonction des niveaux de sécurité admissibles, de (*) à (***).

Ces politiques de certification types ne s'appliquent pas à tous les usages possibles des certificats. Ainsi, la signature électronique « à la volée » n'est pas un usage prévu par le RGS.

La politique de certification est également normalisée dans la RFC 3647, publiée par l'IETF.

Si le service dématérialisé s'appuie sur un prestataire de services de certification électronique externe, la convention de preuve renverra à la politique de certification de ce prestataire.

La politique de certification doit inclure au moins les éléments suivants :

- l'infrastructure de gestion de clés (PKI, *Public Key Infrastructure*) mise en œuvre ;
- les usages autorisés des certificats et, éventuellement, les limitations applicables ;
- les obligations du prestataire, des titulaires et des utilisateurs des certificats ;

Copyright © 2012 Eyrolles.

- les règles de gestion des clés servant à produire les certificats, y compris leur fin de vie et la vérification de leur révocation ;
- les règles d'enregistrement des titulaires des certificats ;
- les règles relatives à la révocation des certificats ;
- les règles relatives au renouvellement des certificats ;
- le format des certificats, leur contenu, les algorithmes utilisés ;
- les conditions de production des certificats ;
- les règles de vérification des certificats ;
- le cas échéant, les conditions de séquestre et de recouvrement des clés privées ;
- les règles de gestion des données personnelles ;
- les conditions de conservation des éléments et dossiers liés à l'activité d'émission des certificats ;
- les assurances ;
- les conditions éventuelles d'audit.

Cette liste n'est évidemment pas exhaustive. On adaptera le contenu de la politique de certification en fonction de la réalité du service offert et de l'usage qui sera fait des certificats.

La politique de signature électronique et la politique de cachet

La politique de signature électronique et la politique de cachet ont pour but de décrire les pratiques mises en œuvre pour la réalisation de ces deux opérations.

Elles sont plus fonctionnelles que les politiques d'horodatage ou de certification. Elles décrivent en particulier dans quelles conditions les signatures et les cachets sont produits, et sur quels documents ils sont apposés.

Dans le cas de la signature électronique, la politique décrit les grandes lignes de l'interface offerte au signataire : la possibilité de visualiser le document avant de le signer, la possibilité de refuser de signer, la possibilité éventuelle de sélectionner plusieurs documents pour les signer simultanément, avec ou sans confirmation pour chacun.

Dans le cas de la signature électronique à la volée, la politique de signature électronique décrit le protocole de consentement et emporte l'adhésion du signataire à ses termes. Elle rappelle en outre le moyen d'authentification employé et s'attache à démontrer qu'il constitue un « procédé fiable d'identification » au sens de l'article 1316-4 du Code civil.

Il sera d'ailleurs très important, en cas de signature électronique à la volée, de placer explicitement le moyen d'authentification de l'utilisateur sous sa responsabilité et son contrôle exclusifs. Si ce moyen d'authentification est un mot de passe, cela peut être fait au choix directement dans les

Copyright © 2012 Eyrolles.

conditions générales d'utilisation, dans la politique de signature électronique, ou dans une politique de gestion des identités et d'authentification à part.

On veillera dans ce cas à ce que l'utilisateur choisisse lui-même son mot de passe dans le respect des règles garantissant sa robustesse, et à ce que le mot de passe en clair ne soit jamais conservé par la plate-forme, qui ne disposera que du hash.

L'engagement du service sera alors de ne jamais procéder à une signature au nom d'un utilisateur sans qu'il ait validé le protocole de consentement.

La politique de signature électronique décrit la liste des familles de certificats éligibles dans le cadre du service et invite, si nécessaire, le signataire à se procurer l'un de ces certificats auprès du prestataire de services de certification électronique de son choix. Il est souhaitable, par ailleurs, de publier cette liste sur une page en accès libre du site Internet, à des fins de transparence et de facilité d'accès.

La politique de cachet, quant à elle, décrit le certificat mis en œuvre par le service pour la réalisation des cachets, et précise la politique de certification applicable afin de permettre à l'utilisateur d'en prendre connaissance.

Ces deux politiques décrivent le format de signature ou de cachet réalisé (PAdES, XAdES ou CAdES, en général), ainsi que les options retenues. Si la signature inclut un horodatage, on renverra à la politique d'horodatage applicable.

Il sera possible d'inclure dans ces politiques, ou de placer dans des politiques à part, les deux compléments suivants :

- la politique de validation de certificat, qui décrit comment la validité des certificats des signataires est vérifiée (à partir de la liste de certificats révoqués ou d'un service de validation OCSP) ;
- la politique de vérification de signature électronique et de cachet, qui décrit l'ensemble des opérations réalisées pour la vérification, et qui positionne ainsi les bases de la validité ou de l'invalidité technique et juridique des signatures et des cachets.

La politique de traçabilité et de gestion de preuves

La politique de traçabilité et de gestion de preuves décrit les pratiques du service dématérialisé en termes de génération, de conservation, de protection, de partage et d'interprétation des traces produites.

Cette politique précise que chacune des parties accepte la validité en preuve des traces produites par le service dans les conditions décrites, et reconnaît leur prépondérance sur tout autre élément de preuve qui pourrait être produit par ailleurs.

Copyright © 2012 Eyrolles.

Elle décrit ensuite la liste des événements donnant lieu à la production d'une trace, ainsi que le contenu de chacune de ces traces et l'interprétation qu'il faut faire de chacun des champs qu'elle contient.

Pour les preuves certifiées, la politique décrit le format des preuves, y compris le cachet et l'horodatage éventuels qui y sont apposés, ainsi que les procédés à mettre en œuvre pour en vérifier la validité. À cette fin, la politique de gestion de preuves pourra renvoyer vers la politique de cachet et/ou la politique d'horodatage.

La politique de traçabilité doit garantir la cohérence et l'exhaustivité de la traçabilité : tracer l'envoi d'un document et non sa réception peut, par exemple, être source de litige ; il en va de même si l'on trace l'envoi d'un document sans garder trace de l'émetteur et du destinataire.

Le principal engagement du fournisseur de services consiste à produire systématiquement et automatiquement toutes les traces décrites par la politique, et à ne pas produire de traces ne correspondant pas à des événements effectivement survenus au sein du système : l'existence de « vraies fausses » traces entraînerait évidemment la remise en cause de l'ensemble de la traçabilité du service.

Les procédés appliqués pour garantir cette intégrité du système global de traçabilité doivent être décrits : numérotation séquentielle, chaînage cryptographique, etc.

La politique de traçabilité décrit les conditions de conservation des traces et des preuves, ainsi que les dispositions prises pour en garantir l'intégrité. Là encore, un renvoi à la politique de cachet et à la politique d'archivage électronique seront nécessaires.

Enfin, la politique précise les conditions de fourniture des traces et des preuves, ainsi que les garanties de confidentialité offertes.

La politique d'archivage électronique

Si le service dématérialisé fait appel à un tiers archiveur, la convention de preuve renverra à la politique d'archivage électronique de ce tiers pour les aspects de conditions de conservation et éventuellement de recherche et de restitution d'archives, ainsi que de confidentialité.

Toutefois, l'initiative du dépôt des archives reste en règle générale de la responsabilité du service, ainsi que la définition du plan d'archivage et de l'indexation.

Si le plan d'archivage est un document à usage interne qui doit être extrêmement détaillé en ce qui concerne le plan de classement et les métadonnées, il n'est pas indispensable d'en donner le détail dans la politique d'archivage.

Copyright © 2012 Eyrolles.

En revanche, on y indiquera :

- les documents concernés par l'archivage ;
- les garanties de conservation : moment de leur dépôt dans le système d'archivage électronique, durée de conservation, garanties de confidentialité, garanties d'intégrité ;
- les conditions techniques de l'archivage électronique, en particulier le respect des normes, en renvoyant éventuellement à la politique d'archivage du tiers archiveur ou à la documentation du coffre-fort électronique employé ;
- les engagements en termes de restitution des archives.

Ces éléments ne sont pas exhaustifs et pourront être complétés et adaptés en fonction des besoins précis du projet.

Les autres politiques

Toute fonction de sécurité mise en œuvre au sein du service dématérialisé peut donner lieu, en fonction des besoins, à une politique, si la convention de preuve l'exige, ou si c'est utile pour d'autres aspects du projet, par exemple pour l'établissement de la confiance.

Ainsi, si un service implique de fortes contraintes de confidentialité des données, comme une plate-forme d'échange de documents en vue de la rédaction de brevets, il sera utile de préciser les engagements pris dans une politique de confidentialité, qui décrira le contrôle des accès et le chiffrement appliqués aux données.

À l'appui d'une telle politique de confidentialité, il pourra être intéressant de décrire les rôles et profils ainsi que les méthodes d'identification et d'authentification mises en œuvre au sein d'une politique de gestion des identités et d'authentification, qui décrira les procédures de création de compte, les certificats autorisés pour l'authentification, les contraintes de sécurité sur les mots de passe, etc.

Copyright © 2012 Eyrolles.

Copyright © 2012 Eyrolles.

PARTIE 5

Organiser la dématérialisation et mener son projet



Copyright © 2012 Eyrolles.

Copyright © 2012 Eyrolles.

Chapitre 14

Mener un projet de dématérialisation

Les méthodologies normalisées

Comme nous l'avons vu au chapitre 1 sur la dématérialisation, un projet de dématérialisation est avant tout un projet informatique. Depuis l'avènement du « génie logiciel », il existe de nombreuses méthodologies normalisées pour mener de tels projets.

Certaines se contentent de décrire des modes de conception et de réalisation de logiciels, comme la très souple méthode agile, l'*extreme programming* ou les méthodes « en V » comme 2TUP ; d'autres vont bien au-delà et incluent l'ensemble du management de projet, notamment le schéma informatique global et la conduite du changement, comme la pionnière française Merise ou la très exhaustive méthode ITIL. Les pratiques empiriques et approximatives malheureusement très répandues ont même été formalisées par l'IILaR sous la forme de la méthodologie de la RACHE (*Rapid Application Conception and Heuristic Extreme-programming*).

L'objet de ce chapitre n'est pas de faire une liste des méthodes applicables à la dématérialisation, ni d'en décrire une nouvelle, mais, dans un premier temps, de faire ressortir les spécificités d'un projet de dématérialisation sous la forme de cinq axes d'approche pour la phase initiale du projet (prise de décision et conception) et, dans un second temps, des éléments clés de chacune des grandes étapes du projet, de l'expression du besoin au maintien en conditions opérationnelles.

Copyright © 2012 Eyrolles.

Les cinq axes d'approche décisionnels

Le démarrage d'un projet de dématérialisation passe nécessairement par l'expression du besoin ou de l'idée du service à mettre en œuvre, et par une prise de décision sur l'opportunité du projet.

À l'appui de ces deux étapes essentielles, cinq axes d'approche complémentaires permettent de former une vision globale en prenant en compte les compétences nécessaires à la réussite du projet. Nous allons aborder successivement les approches fonctionnelle, juridique, organisationnelle, technique et financière du projet, et développer ce que chacune apporte au porteur du projet et au décideur.

Bien entendu, dans la pratique, ces axes d'approche seront abordés en parallèle, et de manière interactive, les apports de chacun ayant des incidences sur les autres.

L'approche fonctionnelle

L'approche fonctionnelle consiste à définir le service dématérialisé du point de vue métier. Que doit-il faire ? Quels services doit-il rendre à chacune des populations d'utilisateurs ? Elle prend en compte l'existant, interne comme externe, anticipe les risques de blocage, et prévoit le phasage du projet.

Identifier les acteurs et les besoins

La première étape consiste à identifier les utilisateurs du service.

Parmi ces utilisateurs, on distinguera cinq catégories principales :

- les utilisateurs externes (demandeurs, clients, usagers du service) ;
- les utilisateurs internes (services métier traitant les demandes) ;
- le service support, qui répond aux questions des utilisateurs et dispose pour cela d'un vue sur les données métier ;
- les administrateurs fonctionnels, qui procèdent au paramétrage du service ;
- les administrateurs techniques, qui procèdent à l'exploitation du service en vue de son maintien en conditions opérationnelles.

Pour chacune de ces catégories d'utilisateurs, il convient de déterminer :

- les actions offertes ;
- les informations disponibles ;
- les documents produits et échangés.

Copyright © 2012 Eyrolles.

Analyser l'existant

Si l'approche fonctionnelle est une projection dans l'avenir, elle part avant tout de l'analyse de l'existant : si un service équivalent existe, par exemple sous la forme d'échanges de papier, *via* des appels téléphoniques ou au travers d'un guichet physique, la procédure dématérialisée devra reprendre les grandes lignes de ce service.

Toutefois, calquer fidèlement le service dématérialisé sur le service préexistant permet rarement de tirer tous les bénéfices de la dématérialisation : c'est par les simplifications et par l'enrichissement que le passage à l'électronique permet de dégager des gains.

Un outil intéressant pour l'approche fonctionnelle est le benchmarking de solutions existantes :

- en interne : analyser les autres services dématérialisés déjà mis en œuvre, et en tirer les enseignements ;
- en externe : étudier les services offerts par les concurrents ou par d'autres entreprises.

Prendre en compte les risques de blocage

L'analyse fonctionnelle inclut les solutions de secours : quel plan de continuité d'activité sera activé au cas où le service ne fonctionne pas, soit au cours de la phase de lancement, soit en cas de panne temporaire survenant ultérieurement ?

Prévoir une solution dégradée en cas d'indisponibilité du service est une précaution indispensable !

Il existe en effet plusieurs causes possibles à un blocage du processus dans le cadre de la dématérialisation :

- d'une part, la fiabilité du service dépendra de l'infrastructure et des procédures d'exploitation mises en œuvre. Tous les services dématérialisés ne justifient pas une architecture coûteuse de haute disponibilité, et tous n'ont pas le même niveau de priorité en termes d'attribution de ressources, ce qui ne signifie pas qu'une interruption du service rendu soit acceptable ;
- d'autre part, même une conception fonctionnelle minutieuse peut omettre certaines exceptions ou certains cas limites, qui se présentent rarement.

Il est donc prudent, dans l'approche fonctionnelle du service, de prévoir la solution de déblocage en cas d'indisponibilité du service ou d'exception non prévue.

Prévoir le phasage du projet

Lors de la mise en œuvre de la dématérialisation, il n'est pas toujours possible ou souhaitable de traiter d'emblée 100 % des cas d'usage de la procédure papier existante. Si le coût de conception et de réalisation correspondant aux cas d'usage rares représente une proportion

Copyright © 2012 Eyrolles.

La théorie du « tout ou rien » conduit souvent à des blocages : phaser le projet est un gage de succès.

trop importante du coût de mise en œuvre du service, il est préférable d'adopter une démarche pragmatique consistant à traiter le cas général et à conserver un traitement parallèle pour les exceptions.

Une approche trop intransigeante sur l'exhaustivité du service entraîne dans bien des cas des retards importants, des situations de blocage, voire l'abandon du projet. Il sera préférable d'envisager une réalisation itérative, permettant d'atteindre la cible en plusieurs étapes prédéfinies, qui offriront chacune un service cohérent à l'ensemble des utilisateurs, par exemple en dématérialisant d'abord les premières phases du processus, puis les phases aval.

Si le service dématérialisé est un service innovant, il est nécessaire d'en cadrer les contours successifs, en envisageant d'abord une première version permettant de tester le concept (*proof of concept*) sur une population cible spécifique ou une partie restreinte du service, avant de généraliser.

Une fois la conception purement fonctionnelle du service réalisée, il convient de l'analyser du point de vue juridique. Cette étape permettra de préciser certains aspects de la conception métier, mais aussi le phasage du projet, de par la nécessité de mettre en œuvre l'infrastructure de sécurité technique et juridique nécessaire à la validité des documents produits dans le cadre du service.

L'approche juridique

L'approche juridique du projet consiste à étudier le contexte de droit dans lequel il s'inscrit, de manière à en valider la faisabilité et à prévoir en amont les mécanismes de sécurité et de confiance utiles et nécessaires.

Analyser le contexte juridique global

En fonction de la nature du service dématérialisé qui doit être réalisé, il existe cinq situations distinctes qu'il convient d'identifier :

- le droit ne mentionne pas explicitement les aspects de dématérialisation du service concerné ;
- le droit interdit la dématérialisation (par exemple, l'article 1108-2 du Code civil interdit notamment la dématérialisation des actes sous seing privé relatifs au droit de la famille et des successions) ;
- il existe une autorisation explicite à dématérialiser ce service (par exemple, le bulletin de paie peut être dématérialisé depuis la loi du 12 mai 2009) ;
- il existe une incitation à dématérialiser ce service (par exemple, l'article 57 du Code des marchés publics réduit le délai de réception des offres de 7 jours si l'avis d'appel public à la concurrence est envoyé par voie électronique et de 5 jours si les documents de la consultation sont rendus accessibles par voie électronique) ;

Copyright © 2012 Eyrolles.

- il existe une obligation à dématérialiser ce service (par exemple, l'article 56 du Code des marchés publics dispose que « pour les achats de fournitures de matériel informatique et de services informatiques d'un montant supérieur à 90 000 euros HT, les candidatures et les offres sont transmises par voie électronique »).

Si la loi fixe les conditions applicables, il faudra alors s'appuyer sur les textes pour déterminer les fonctions de sécurité à inclure dans le service. Les contraintes imposées par le droit peuvent aller des conditions d'authentification des utilisateurs à l'archivage électronique des documents, en passant par la traçabilité de certaines données et la nécessité de signature électronique portant sur certains documents. Mais elles déterminent aussi les conditions d'applicabilité de la dématérialisation, et ont donc des impacts forts sur les aspects fonctionnels et organisationnels, comme nous le verrons dans l'exemple suivant relatif à la dématérialisation des factures.

Cas d'usage : la dématérialisation de facture

La dématérialisation des factures est prévue par le Code général des impôts sous trois formes :

- la conservation électronique du double des factures envoyées en papier ;
- la dématérialisation des factures sous forme d'un flux structuré ;
- la dématérialisation des factures sous forme de fichiers.

Nous allons nous intéresser ici à ce troisième cas.

Code général des impôts – Article 289 V

Les factures peuvent, sous réserve de l'acceptation du destinataire, être transmises par voie électronique dès lors que l'authenticité de leur origine et l'intégrité de leur contenu sont garanties au moyen d'une signature électronique.

Les impacts de ce texte sont multiples.

- Il constitue une autorisation explicite de dématérialiser la facturation : cela lève le risque quant à la faisabilité.
- Il conditionne cette faculté à l'acceptation du processus par le destinataire de la facture, ce qui a un fort impact contractuel et organisationnel, puisqu'il faut prévoir dans le projet de recueillir l'assentiment du destinataire de la facture, et de pouvoir en faire la preuve.
- Il fixe la nécessité de garantir leur origine et leur intégrité (ce qui reprend les conditions de validité en preuve d'un écrit électronique mentionnées dans l'article 1316-1 du Code civil, mais sans le citer), au moyen d'une signature électronique. Cela conditionne les fonctions de sécurité à mettre en œuvre, la signature électronique est incontournable.

Copyright © 2012 Eyrolles.

Mais avant de se précipiter sur les textes qui définissent la signature électronique (article 1316-4 du Code civil et décret du 30 mars 2001), une analyse plus poussée permet d'obtenir des précisions.

Code général des impôts – Annexe 3 – Article 96 F

Le signataire est celui qui détient et met en œuvre le moyen de création de la signature électronique. Il peut s'agir d'une personne morale, auquel cas la signature électronique est produite automatiquement lors de l'envoi des factures, ou d'une personne physique émettant les factures après les avoir signées en son nom pour le compte de l'entreprise.

Cet article précise que le signataire peut être une personne morale, on ne se trouve donc pas dans le contexte juridique du décret du 30 mars 2001, qui définissait le signataire comme une personne physique !

Le même article définit par la suite avec beaucoup de précision la forme que doit prendre la signature électronique mentionnée à l'article 289 V, et indique notamment que le certificat du signataire doit être délivré par un prestataire de services de certification (contrainte technique et organisationnelle sur le service), et que le destinataire de la facture a l'obligation d'en vérifier la signature (contrainte fonctionnelle sur le service).

La définition donnée de la signature électronique, et sa portée juridique, dépendent donc fortement du contexte de droit dans lequel on se trouve. Faute de l'analyse juridique appropriée, le concepteur du service doté uniquement de compétences techniques pourrait être amené à mettre en œuvre des solutions inadaptées – entraînant un risque financier très important en cas d'invalidité des factures produites.

Déterminer les contraintes et les opportunités juridiques

En complément de l'analyse du contexte, l'étude juridique permet de se pencher sur l'opportunité de la mise en œuvre de certains mécanismes de sécurité.

Prenons deux exemples dans lesquels l'analyse juridique pourra avoir un impact fort sur la conception du service : la traçabilité et la signature électronique.

Premier exemple : traçabilité et données à caractère personnel

En matière de traçabilité, l'analyse fonctionnelle aura déterminé les usages qui seront faits des traces : par exemple, établissement de la preuve des échanges, suivi des actions des clients, et data mining dans un but marketing, cette action étant confiée à un prestataire tiers.

L'étude juridique permettra alors de fixer les règles relatives à cette dernière activité. En respect de la loi Informatique et libertés, les données de traçabilité seront anonymisées avant de les fournir au prestataire qui les analysera.

Copyright © 2012 Eyrolles.

Mais en allant plus loin, cette contrainte pourra être déterminante lors de la conception technique du service. Ainsi, on pourra, par exemple, envisager que les traces ne contiennent nativement que des identifiants anonymes des utilisateurs, et que le lien avec les personnes physiques et morales ne soit reconstitué qu'à partir du croisement avec une autre base de données. Les besoins d'établissement de la preuve amèneront alors à prévoir les mécanismes nécessaires pour garantir l'intégrité et la fiabilité de cette base d'identifiants.

Ainsi, l'approche juridique a un impact important au niveau de la conception technique du service, et même de son mode d'exploitation si l'on veut garantir que les administrateurs n'aient pas la possibilité de recouper les données de traçabilité avec les données d'identification.

Deuxième exemple : signature électronique et engagement

Nous avons vu dans le chapitre 7 sur la signature électronique que ce mécanisme offre deux propriétés techniques intéressantes : garantir la provenance d'un document (il est lié à l'identité du signataire) et garantir son intégrité (toute modification ultérieure est détectable).

Il peut donc être tentant d'un point de vue technique de signer systématiquement tous les documents transmis *via* une plate-forme dématérialisée.

Toutefois, la signature électronique emporte également le consentement du signataire, c'est là son objet principal au titre de l'article 1316-4 du Code civil. L'analyse juridique amènera donc à n'apposer de signature électronique que sur les documents finaux, sur lesquels l'engagement du signataire est requis.

Une version temporaire d'un document ne sera pas signée : on garantira sa provenance et son intégrité d'une autre manière, par exemple *via* la traçabilité ou en lui apposant un cachet.

De même, un document qui n'a pas vocation à engager son auteur ne sera pas signé électroniquement. Par exemple, une notice explicative, un mode d'emploi ou une spécification technique dans le cadre d'un processus R&D dématérialisé peuvent ne pas nécessiter une signature.

L'approche juridique sera l'occasion d'interroger les pratiques habituelles mises en œuvre en papier au regard des obligations légales, et éventuellement de les simplifier à l'occasion de la dématérialisation. Elle servira à proposer les mécanismes de sécurité les mieux adaptés.

Déterminer les niveaux de sécurité applicables

L'approche juridique est également le moment de la détermination des niveaux de sécurité à appliquer, d'une part à chacun des utilisateurs du service, en matière d'authentification ou de signature électronique,

Copyright © 2012 Eyrolles.

par exemple, et d'autre part, au service lui-même, par exemple pour l'horodatage ou le cachet.

Cela est particulièrement important dans le secteur public, qui est soumis réglementairement au RGS. Le choix du niveau de sécurité applicable dépend de l'analyse de risque, qui est à la fois organisationnelle, technique et juridique.

Ainsi, sur un téléservice d'une collectivité locale, un citoyen qui peut, à partir de son compte, effectuer des demandes de subventions et en suivre l'avancement sera authentifié par un simple mot de passe puisque aucune conséquence juridique ne peut résulter d'une usurpation d'identité. En effet, personne n'a d'intérêt à demander une subvention pour un tiers.

En revanche, les conséquences du piratage du compte d'un agent de la collectivité pouvant entraîner l'attribution indue d'une subvention à un citoyen, il conviendra de mettre en place une authentification forte, par exemple à l'aide d'un certificat RGS (**).

Les choix effectués en vertu des approches fonctionnelle et juridique vont s'imposer aux utilisateurs et aux administrateurs du service. L'impact opérationnel de ces deux étapes de conception doit donc être pris en compte dans une approche organisationnelle du projet.

L'approche organisationnelle

L'approche organisationnelle de la conception est une anticipation de la phase de conduite du changement qui devra être menée au cours du projet. Les trois règles d'or sont :

- avoir une vision globale ;
- prendre en compte l'existant sans en faire un référentiel absolu ;
- être pragmatique.

La nécessité d'une vision globale

La dématérialisation entraîne une modification profonde des modes de travail et des modes d'accès aux services.

Elle touche directement ou indirectement la plupart des métiers de l'entreprise : les services métier, bien entendu, mais aussi le marketing et la vente, pour prendre en compte les nouveaux produits ou l'évolution des modes de distribution. Le support aux utilisateurs sera un facteur essentiel de réussite du projet, modifiant ou créant un nouveau métier dans l'entreprise. Le service des archives sera concerné au premier plan si les documents originaux électroniques donnent lieu à un nouveau mode de conservation. Enfin, la direction informatique sera aux premières loges de par la nécessité de gérer de nouveaux logiciels, de nouveaux matériels, de nouveaux flux de données et de nouvelles procédures.

Copyright © 2012 Eyrolles.

Mais la dématérialisation s'imposera également aux partenaires avec lesquels l'entreprise travaille au quotidien : eux aussi devront s'adapter aux nouvelles modalités d'échange de données et de fichiers.

Enfin, les utilisateurs des services dématérialisés se voient proposer de nouvelles pratiques, qui peuvent entraîner pour eux des conséquences importantes en termes de bénéfices, mais aussi de contraintes.

Il est impossible de concevoir un service dématérialisé sans prendre en compte l'ensemble de la chaîne des acteurs concernés, et les modifications organisationnelles induites pour chacun d'entre eux.

Mais la conception globale de la dématérialisation va au-delà de ce simple panorama du contexte : elle doit également se pencher sur les ouvertures possibles de la dématérialisation à d'autres processus, proches ou non, qui peuvent en être des bénéficiaires ou des facilitateurs.

Prenons deux exemples : la distribution au personnel de l'entreprise de cartes à puce et la mise en œuvre de l'archivage.

Lorsqu'une entreprise déploie des supports cryptographiques, par exemple pour sécuriser l'accès au poste de travail et le courrier électronique, la carte qui sert de support à cette sécurisation peut être simplement « une carte de plus », que les employés risquent d'oublier chez eux ou, pour éviter justement les conséquences fâcheuses de cet oubli, de laisser dans le tiroir de leur bureau. On perd alors une grande partie de l'intérêt du déploiement ! Dans une vision globale, on pourra envisager de transformer la carte d'authentification en badge multi-usage, qui servira également à contrôler l'accès au bureau grâce à une puce sans contact, à régler les consommations à la machine à café, à payer la cantine, voire, à l'aide d'une personnalisation graphique, à remplacer le badge professionnel identifiant la personne lors de ses déplacements dans les locaux. Le risque d'oubli est alors réduit, et l'outil est plus facilement approprié par les employés du fait de la multitude d'utilités complémentaires que revêt la carte. La gestion du parc de cartes sera alors facilitée par le déploiement d'un système de gestion des cartes (CMS, *Card Management System*), qui permettra de gérer automatiquement la mise à jour des droits, le renouvellement des certificats et l'émission d'un badge temporaire en cas d'oubli ou de perte.

Dans le même esprit, lorsque la mise en œuvre d'un service dématérialisé entraîne le déploiement de l'archivage électronique, ce serait une erreur de cantonner l'usage de ce nouveau dispositif au seul projet qui en a été à l'origine : ce sera alors l'occasion de faire un point transversal sur l'ensemble des documents électroniques gérés par l'entreprise de manière à les intégrer dans le coffre-fort d'archivage. Si l'ampleur du projet qui découle de cette étude est telle qu'il ne puisse être envisagé immédiatement, il faudra au moins concevoir le plan d'archivage de telle manière que l'inclusion de ces nouveaux documents soit aisée dans l'avenir.

Copyright © 2012 Eyrolles.

Ainsi, l'analyse de l'existant, dans une vision globale, ne se limite pas à la procédure en cours de dématérialisation. Approfondissons ce concept.

L'analyse de l'existant… en vue de sa modification

Un service dématérialisé est rarement entièrement nouveau : soit il est la transcription dans le mode immatériel d'un processus qui donnait jusqu'ici lieu à des échanges papier, soit il se fonde sur une possibilité ou une obligation offerte par les textes législatifs, soit il s'agit d'un service répondant à un besoin des utilisateurs, qui avaient préalablement, en général, une autre pratique.

Dans tous les cas, l'étude attentive de l'existant fonctionnel est un point essentiel du projet. Mais cette étape comporte un piège, il faut donc être très vigilant : le fait de décrire l'existant ne doit pas figer *a priori* le contour du nouveau service. En effet, les bénéfices ne sont tirés de la dématérialisation que si elle est l'occasion d'une modification des pratiques : amélioration, fluidification, simplification… Il importe d'identifier, avec les étapes du processus existant, les raisons d'être de ces étapes. On se rend compte ainsi que de nombreuses lourdeurs sont intégrées aux processus métier par le simple fait d'habitudes obsolètes qui n'ont jamais été remises en cause. Ainsi, l'existant doit être un référentiel de travail, mais en aucun cas le référentiel absolu.

De même, les différentes étapes d'un processus renvoient, en filigrane, à l'organisation mise en place pour son déroulement. La remise à plat d'un processus métier peut entraîner la modification en profondeur d'une structure d'entreprise et des modes de travail. L'étude ne saurait ignorer ce fait, car il peut être un facteur d'échec du projet si les mesures adéquates d'accompagnement au changement ne sont pas mises en œuvre suffisamment tôt – ou si le projet remet en cause le positionnement de décideurs ayant le pouvoir de s'y opposer !

Enfin, l'existant technique de l'entreprise est un élément fondamental qu'il ne faut pas oublier. Nous l'aborderons plus précisément dans la section dédiée à l'approche technique du projet.

L'analyse de l'existant et son pendant, la conception des évolutions, doivent ainsi alimenter dès l'amont du projet le plan global de conduite du changement, que nous détaillerons plus loin.

Le pragmatisme : un garde-fou contre l'échec

L'approche organisationnelle du projet de dématérialisation doit toujours prendre en compte cette question fondamentale : qu'est-ce qui a le plus de chances de fonctionner ?

Une solution parfaitement sécurisée mais trop contraignante pour les utilisateurs sera systématiquement rejetée. Une solution techniquement

Copyright © 2012 Eyrolles.

parfaite mais nécessitant des compétences dont l'entreprise ne dispose pas aura du mal à être déployée. Un nouvel usage sans l'accompagnement nécessaire ne sera pas facilement adopté…

La prise en compte du facteur humain dans le projet de dématérialisation est sans doute le facteur de réussite le plus important. Le concepteur doit systématiquement se mettre à la place de l'utilisateur, en « candide », et se demander comment il réagirait aux modifications envisagées sur ses conditions de travail.

L'approche technique

L'approche technique du projet comporte de nombreuses dimensions complémentaires, dont certaines ont trait au choix de réalisation de la solution dématérialisée, et d'autres à son exploitation.

La conception du service

Dans le projet de dématérialisation, l'approche technique commence par la prise en compte du SI existant.

L'homogénéité technologique du parc d'applications de l'entreprise est un facteur de qualité de service important pour la direction informatique. Les règles de sécurité du SI peuvent imposer des restrictions, par exemple sur l'appel à des services externalisés, ou sur l'accès des utilisateurs internes à Internet. Et certaines des briques techniques nécessaires au projet sont peut-être déjà présentes dans le SI, pour avoir été mises en œuvre dans d'autres projets. Ces éléments doivent être pris en compte en amont lors de la conception technique du service afin de ne pas risquer de se heurter à des impossibilités au moment du déploiement.

La réalisation du service dématérialisé pourra être, selon les ressources disponibles dans l'entreprise, effectuée en interne ou sous-traitée à une SSII. Dans le cas d'une sous-traitance, les contraintes techniques liées au SI doivent figurer au cahier des charges au même titre que la description fonctionnelle du service attendu.

De même, les performances attendues du système sont un élément clé qui déterminera le choix des technologies mises en œuvre aussi bien que du dimensionnement des serveurs hébergeant l'application.

Enfin, la question de l'utilisation de solutions open source se pose très fréquemment lors des phases amont des projets. Plusieurs critères doivent entrer en jeu dans ce choix.

Le premier est la robustesse de la solution : a-t-elle fait l'objet d'une évaluation de sécurité et de performances ? Les patchs de sécurité sont-ils réguliers ?

Ensuite, se pose la question de la réalité de son caractère open source : la solution dispose-t-elle d'une communauté nombreuse et active, ou

Copyright © 2012 Eyrolles.

s'agit-il d'un argument marketing mis en avant par une seule entreprise ? Le code source est-il effectivement disponible ? S'agit-il bien de la dernière version ? En choisissant une solution « ouverte » dépendant d'un seul contributeur, on court un fort risque d'être pieds et poings liés face au fournisseur de la solution.

La maîtrise effective du code source de l'application est également un point fondamental : ce n'est pas parce qu'on a la capacité théorique à reprendre le code source qu'on en a effectivement la capacité technique ou les moyens humains. Ainsi, cet argument de l'open source est à mettre en regard avec les besoins effectifs en termes de réversibilité par rapport au prestataire de réalisation ou d'intégration. Dans bien des cas, il peut être préférable d'avoir un bon contrat de service avec un éditeur pour bénéficier d'une solution propriétaire, que de compter sur une licence open source pour garantir une indépendance qui sera en fait toute théorique.

Cet axe d'approche est indissociable de la réflexion sur la sécurité, puisqu'il peut avoir des influences sur la disponibilité du service et la capacité de l'entreprise à le faire évoluer. La sécurité contractuelle garantira la souveraineté de l'entreprise sur son SI.

L'exploitation du service

De même que pour le développement, l'exploitation du service dématérialisé peut être internalisée ou externalisée *via* un contrat de service. Les compétences disponibles en interne, les coûts liés et les aspects de sécurité (en particulier de confidentialité) seront mis en balance pour faire un choix pertinent.

Lorsque l'exploitation est effectuée en interne, un contrat de service plus ou moins formel pourra également être conclu entre la direction informatique et la direction conceptrice ou utilisatrice du service, de manière à garantir le respect des performances et de la disponibilité nécessaires.

La sécurité de l'exploitation comporte plusieurs aspects, qui couvrent la sécurité technique, la sécurité organisationnelle et la sécurité comportementale.

Au titre de la sécurité technique, outre la capacité de sécurisation classique (pare-feu, détection d'intrusion, disponibilité…), on prendra en compte la nécessité d'ouverture vers l'extérieur de services web, ou d'accès distants pour les partenaires ou les utilisateurs en situation de mobilité : ces ouvertures ne doivent pas faire naître de risques d'attaque, notamment par injection de code.

Les procédures organisationnelles liées à l'exploitation de nouveaux services, tels que l'horodatage ou le cachet, nécessiteront une attention particulière si elles sont mises en œuvre pour la première fois.

Copyright © 2012 Eyrolles.

Enfin, les personnels doivent être sensibilisés à la portée juridique des éléments qu'ils gèrent au sein de l'application dématérialisée, afin d'adapter si nécessaire leur niveau de vigilance à l'importance des risques encourus en cas de défaillance.

L'approche financière

L'approche financière du projet de dématérialisation comporte deux dimensions : les coûts liés au projet et les gains qui en sont attendus.

L'étude des coûts

Les coûts d'un projet de dématérialisation sont trop souvent calculés en prenant en compte uniquement le prix des développements informatiques correspondants.

Pour un calcul objectif du coût global d'un projet, il convient d'y inclure également les éléments suivants :

- le coût des ressources humaines consacrées au projet, dans les phases amont (cycle de décision), les phases de réalisation (spécification, recette) et les phases aval ;
- les coûts d'exploitation de la solution, qui incluent non seulement son hébergement, mais aussi le monitoring et le support aux utilisateurs, sans oublier les frais liés à la location de licences des logiciels inclus dans la solution, ou le coût récurrent lié à l'archivage électronique, dont le volume est en général croissant dans le temps ;
- les coûts de maintenance, qui incluent les éventuelles corrections techniques et fonctionnelles mais également les évolutions à venir du service, pour prendre en compte les changements de réglementation, la progression du marché, les inflexions de la stratégie ou de l'organisation de l'entreprise ;
- les coûts liés à l'accompagnement du projet : formation, communication, publicité ;
- et surtout, le coût de la conduite du changement, notamment les réorganisations qu'induit l'évolution des processus internes, les nouveaux métiers qui peuvent apparaître pour prendre en compte les évolutions des modes de travail ou du SI.

La prise en compte de l'ensemble de ces éléments est indispensable pour avoir une vision objective des dépenses globales occasionnées par le projet, dans le cadre d'une étude d'opportunité.

On sera également prudent en ce qui concerne le calendrier du projet : un *time to market* serré ne permet pas les dérapages du planning, et les coûts engendrés par des retards sont à la fois directs (allongement de la mobilisation des personnels sur le projet) et indirects (image de marque en cas

Copyright © 2012 Eyrolles.

d'annonces non tenues, retard par rapport à la concurrence, déception des clients).

L'étude des gains

Le retour sur investissement d'un projet de dématérialisation comporte, lui aussi, de nombreux éléments.

Pour un service commercial dématérialisé, le premier élément à prendre en compte est évidemment l'accroissement du chiffre d'affaires généré par le nouveau service ou le nouveau processus de commercialisation.

Pour un service administratif, le point le plus facile à mesurer est le gain direct, par exemple sous forme d'économies de papier et d'affranchissement. Ainsi, le projet « J'entreprends en Bourgogne », qui gère au sein du portail e-bourgogne les aides de la région Bourgogne aux entrepreneurs, affiche une économie de 10 millions de feuilles de papier par an.

Toutefois, ce n'est pas là que se situe la plus grande partie des gains. Il faut chercher le véritable apport de la dématérialisation dans les gains indirects.

En effet, la dématérialisation induit une hausse de la qualité des dossiers reçus : le nombre d'allers-retours entre les demandeurs et le service de traitement est drastiquement réduit par les contrôles automatiques de cohérence et de complétude qui peuvent être réalisés automatiquement par la plate-forme. Une étude menée sur le projet Planet Limousin a montré un taux de dossiers papier incomplets ou erronés de 26 %. La suppression quasiment complète des tâches liées au traitement de ces dossiers en erreur représente un gain très important en termes de charge de travail.

Un autre gain est lié à l'amélioration du processus de travail des agents qui traitent les dossiers. Au lieu de parcourir des formulaires souvent complexes, dont le remplissage de certaines parties est conditionné aux choix effectués dans d'autres (« si vous avez coché la case A2, veuillez remplir le cadre G5 en page 4 »…), les agents se voient présenter à l'écran uniquement les données pertinentes pour leur travail d'analyse, de manière guidée et fluidifiée, ce qui entraîne une accélération du traitement de chaque dossier.

Enfin, la refonte globale des processus métier permet en général de supprimer ou de regrouper des étapes de validation. Cette rationalisation des ressources est sans doute la plus génératrice d'économies de fonctionnement.

S'il est parfois difficile d'afficher les apports du projet de dématérialisation sous la forme de suppressions de postes, en particulier dans le secteur public, négliger cette dimension vouera en général à l'échec la recherche du retour sur investissement du projet.

Copyright © 2012 Eyrolles.

Enfin, les bénéfices non financiers de la dématérialisation, s'ils sont plus difficiles à chiffrer, doivent aussi être pris en considération. Ces aspects sont liés à la qualité de service (enrichissement du service rendu, augmentation de la proximité avec les clients ou les usagers, gain de transparence, meilleur suivi des dossiers, réduction des délais de traitement), mais aussi à l'image de marque (image de modernité, de dynamisme, communication « développement durable »…).

En synthèse : le dossier d'opportunité

Une étude menée en parallèle selon les cinq axes que nous venons de détailler permet de disposer d'un dossier d'opportunité complet, qui présente deux avantages importants :

- d'une part, il permettra aux instances décisionnaires de disposer de tous les éléments objectifs à l'appui du lancement du projet ;
- d'autre part, il constitue une excellente base à la rédaction des spécifications fonctionnelles et techniques du service dématérialisé, ou du cahier des charges en vue d'une mise en concurrence de prestataires de réalisation.

Voyons, au travers du témoignage de la profession des experts-comptables, comment l'ensemble de ces points ont été pris en compte dans la décision d'une implication pionnière et durable dans le domaine de la dématérialisation.

Parole d'expert

Jean Saphores, président de la Commission informatique du conseil supérieur de l'ordre des experts-comptables, président d'EDIFICAS

Quelle relation entretient la profession des experts-comptables avec la dématérialisation ?

Un programme global de dématérialisation a été initié par la profession dès 1998, l'expert-comptable se positionnant au centre des procédures dématérialisées pour en faciliter l'accès aux TPE et PME.

Notre portail « jedeclare.com » permet, grâce à une normalisation des flux conçue avec nos partenaires (DGFIP, centres de gestion agréés, banques commerciales, Banque de France, commissaires aux comptes…), de réaliser des échanges au travers de nombreuses téléprocédures, tant pour l'acquisition que pour la restitution de données. Ainsi, en 2011, le portail regroupait 1,7 millions d'entreprises, pour un total de 30 millions d'échanges. Tous les flux transitant par la plate-forme sont bien entendu scellés et horodatés.

De plus, les textes nous confèrent deux qualités qui sont fondamentales pour la dématérialisation : le statut de tiers de confiance et le mandat implicite.

Au titre de notre rôle de tiers de confiance, nous avons la possibilité de conserver les pièces faisant foi, comme les ordres de paiement, les autorisations de télérèglement,

Copyright © 2012 Eyrolles.

les justificatifs de crédit d'impôt... Ces pièces étant bien souvent de nature électronique.

Au titre du mandat implicite, l'expert-comptable qui a reçu un mandat d'un client peut agir pour le compte de son client sans avoir à prouver ce mandat : le fait de prouver sa qualité d'expert-comptable inscrit à l'ordre suffit à lui donner légitimité.

Tout ceci militait bien entendu pour le déploiement à la profession d'un outil d'authentification forte et de signature électronique : c'est chose faite avec Signexpert.

Vous avez piloté le projet de conception et de déploiement de la signature électronique des experts-comptables, Signexpert. Quels sont les premiers usages que vous envisagez pour cet outil ?

Le projet Signexpert permet de remettre à chaque expert-comptable plusieurs certificats, qui ont des rôles différents.

Tout d'abord, un certificat de signature électronique de niveau RGS (***) est utilisé pour réaliser des signatures emportant présomption de fiabilité au sens de l'article 1316-4 du Code civil et du décret du 30 mars 2001. L'expert-comptable signe, par exemple, à l'aide de ce certificat, les comptes annuels et tous les documents sur lesquels sa signature formelle est requise. Chaque acte de signature nécessite la saisie du code PIN, l'engagement est très solennel.

Ensuite, un certificat de niveau RGS (**) permet l'authentification forte vis-à-vis des serveurs, et le scellement des documents dans le but de produire des originaux électroniques conformes à l'article 1316-1 du Code civil, mais aussi les e-mails sortant du cabinet ou l'ensemble des documents produits couramment. Par exemple, du point de vue fiscal, l'original de la comptabilité d'une entreprise est constitué non pas par les éléments imprimés, mais par les fichiers informatiques originaux : la procédure de clôture destinée à rendre ces fichiers non modifiables inclut naturellement un scellement et un archivage électronique.

Enfin, pour les actes devant être scellés par le cabinet en tant que personne morale, par exemple des factures ou des bulletins de paie dématérialisés, l'expert-comptable a la possibilité d'acquérir un cachet électronique. Le cachet du cabinet et la signature de l'expert-comptable sont parfois apposés conjointement sur les comptes annuels, dans le respect des habitudes papier.

Quels ont été les éléments clés de prise de décision pour le lancement du projet ?

La dématérialisation est indissociable de notre cœur de métier : c'est pour nous non seulement une obligation, mais un véritable besoin. Les aspects fonctionnels offerts par la signature électronique nous sont indispensables, du fait de la très grande quantité d'originaux électroniques que nous gérons au quotidien.

L'évolution des textes législatifs et réglementaires au fil du temps nous a aidés à mettre en œuvre progressivement nos outils : échanges EDI, portail web sécurisé, et aujourd'hui la signature électronique de l'expert-comptable.

Il est fondamental de bien comprendre qu'il ne s'agit pas d'une signature électronique personnelle banale, mais bien de la signature d'un professionnel dans le cadre de l'exercice de sa profession réglementée. Signexpert identifie le signataire non seulement en tant que personne physique, mais en tant qu'expert-comptable inscrit à l'ordre, ce qui a une force juridique extrêmement importante.

Copyright © 2012 Eyrolles.

Cette force juridique est en outre indissociable des aspects organisationnels de l'ordre : nous avons calqué la structure de notre PKI sur celle des Conseils Régionaux de l'Ordre, chacun des 23 CROEC étant autorité de certification et délivrant des certificats à ses membres.

Enfin, du point de vue technique, nous avons adopté des niveaux de sécurité à la hauteur des enjeux, et conçu un outil de signature électronique ergonomique et adapté aux besoins de notre profession.

Nous allons maintenant parcourir les différentes phases de la mise en œuvre effective d'un projet de dématérialisation, en faisant ressortir les éléments particuliers liés aux aspects de sécurité et de confiance.

Le déroulement d'un projet

L'objet de ce chapitre n'est pas de détailler une méthodologie de conduite de projet : de nombreux ouvrages proposent des méthodes formalisées auxquelles le lecteur intéressé pourra se référer. Toutefois, il nous semble important de faire ressortir, au sein des étapes classiques d'un projet informatique, les points d'attention incontournables liés à la mise en œuvre des mécanismes de sécurité et de confiance.

L'expression de besoin et l'identification des contraintes

L'expression de besoin, aussi appelée « spécification fonctionnelle générale », est réalisée en grande partie lors de l'étude d'opportunité. L'élément essentiel est qu'elle consiste en une description fonctionnelle de haut niveau du service, suffisante pour envisager de manière globale les apports et les coûts liés.

Il y a un risque important à faire une expression de besoin trop technique ou trop détaillée lors de la phase amont du projet. Illustrons ce fait par deux fonctionnalités de sécurité : la signature électronique et la confidentialité.

Considérons la différence entre les expressions suivantes : « une signature électronique doit être apposée sur les documents » et « le service doit garantir l'intégrité et la provenance des documents ». Dans le cas de la première formulation, le mécanisme technique est déterminé, on pourra encore envisager l'emploi d'une signature de personne ou d'un cachet, mais les grandes lignes sont tracées. La seconde phrase, quant à elle, laisse le champ ouvert à des solutions alternatives que nous avons vues dans les chapitres précédents : mécanisme de hash, traçabilité, dépôt dans un coffre-fort électronique, tout en laissant bien entendu la possibilité de la signature électronique, du cachet ou de l'horodatage certifié.

Copyright © 2012 Eyrolles.

Cette expression de besoin fonctionnelle ne sera donc précisée qu'une fois l'étude juridique, organisationnelle, technique et financière réalisée.

Il en va de même pour ces deux expressions : « les données du service sont chiffrées » et « la confidentialité des données du service est assurée vis-à-vis de… ». La confidentialité peut être garantie sous plusieurs modes, le chiffrement étant l'un d'entre eux, le plus sûr s'il est mis en application dans de bonnes conditions, mais aussi le plus risqué en termes de disponibilité des données, et le plus coûteux en termes de procédures à mettre en œuvre et de temps de traitement lors des accès aux données.

L'expression de besoin regroupera bien évidemment les contraintes identifiées lors de l'étude d'opportunité, qu'elles soient fonctionnelles (en incluant les aspects d'ergonomie, d'accessibilité, de multilinguisme), juridiques, organisationnelles, techniques, financières ou liées au calendrier et aux délais.

L'analyse des risques et l'étude de sécurité

L'analyse des risques et l'étude de sécurité sont une phase essentielle du projet de dématérialisation, car leur aspect transversal permet de prendre en compte les cinq axes déterminés précédemment pour en déduire les mécanismes de sécurité à mettre en œuvre concrètement au sein du service.

L'Agence nationale de la sécurité des systèmes d'information (ANSSI) a formalisé et rendu publique une méthode de gestion des risques appelée « EBIOS » (Expression des besoins et identification des objectifs de sécurité).

Cette méthode peut être appliquée aussi bien de façon globale à un service dans son ensemble que, de manière plus détaillée, à un sous-ensemble de ce service nécessitant une attention particulière. Elle comporte cinq modules complémentaires :

- **l'établissement du contexte,** qui donne une vision globale du service rendu et de son environnement organisationnel, juridique et technique ;
- **l'étude des événements redoutés,** qui consiste à identifier tout ce qui peut arriver de fâcheux dans le cadre du service, sans limitation sur la cause possible du sinistre : perte de confidentialité sur des données sensibles, indisponibilité du service, remise en cause de la valeur juridique de documents… ;
- **l'étude des scénarios de menaces,** qui se focalise sur les causes possibles de ces événements : bogue informatique, panne matérielle, erreur humaine, attaque délibérée, évolution du contexte… ;
- **l'étude des risques,** qui permet de procéder à leur quantification en termes de conséquences et de probabilité d'occurrence ;

Copyright © 2012 Eyrolles.

- **l'étude des mesures de sécurité,** qui détermine ce qu'il faut mettre en œuvre pour répondre aux menaces en prenant en compte leur quantification.

Ces mesures de sécurité peuvent être de toutes natures : fonctionnelles (par exemple, ajouter de la traçabilité sur certaines actions, améliorer la documentation…), organisationnelles (par exemple, modifier le processus d'exploitation, communiquer vis-à-vis des partenaires…), techniques (par exemple, modifier la constitution des URL pour éviter qu'un numéro de dossier y soit lisible, configurer un pare-feu pour rejeter certains flux…), juridiques (par exemple, rédiger une convention de preuve pour s'assurer de la validité en preuve des documents produits par le service), financières (par exemple, souscrire une assurance pour couvrir un risque).

L'étude de sécurité est donc bien loin de se cantonner au domaine technique, et ne cherche pas nécessairement à établir une sécurité absolue. En effet, un risque peut être :

- évité par les mesures techniques ou organisationnelles adéquates ;
- reporté sur une autre personne, par exemple *via* une assurance ou l'appel à un tiers de confiance ;
- atténué de manière à devenir acceptable ;
- ou simplement pris, en toute conscience, s'il est jugé acceptable.

Les risques résiduels doivent être pris en compte, ainsi que les risques induits par les mesures de sécurité adoptées, en procédant à une nouvelle boucle de la méthode. Ainsi, pour parer un risque sur la recevabilité de documents, on pourra mettre en œuvre une traçabilité fondée sur l'horodatage certifié. Le risque lié à l'indisponibilité du service d'horodatage devra être pris en compte, par exemple en sous-traitant l'horodatage à un prestataire de services d'horodatage électronique, la mesure de sécurité étant alors de nature contractuelle, soit en mettant en œuvre un service d'horodatage interne redondé, soit en prévoyant un fonctionnement du service en mode dégradé dans ce cas…

En matière de sécurisation, les solutions « toutes faites » n'existent pas, et une bonne analyse de risque complétée par une étude de sécurité menée avec rigueur sont indispensables pour la conception pertinente de l'architecture globale de sécurité, qui s'appuiera sur l'ensemble des mécanismes que nous avons détaillés dans le présent ouvrage.

La spécification fonctionnelle

L'objectif de la phase de spécification est d'atteindre un niveau satisfaisant de conception, permettant la réalisation sans risquer de contentieux sur le contenu, mais sans tomber dans les pièges de la « sur-spécification ».

Copyright © 2012 Eyrolles.

Les étapes de la spécification fonctionnelle détaillée sont les suivantes :

- l'identification des acteurs, des principaux processus et des données macroscopiques manipulées ;
- sur cette base, il est souhaitable de réaliser à cette étape l'analyse de risque, dont les résultats servent de base à la rédaction de la spécification ;
- pour chacun des acteurs, description des cas d'usage, par exemple sous la forme :
  - de maquettes d'écrans ;
  - de description des enchaînements qui résultent de l'usage des boutons ;
  - de description textuelle des traitements qui doivent être effectués sur les données ;
  - de schémas de modélisation graphique, par exemple selon le langage UML.
- la validation du document résultant par les services métier, juridique et technique.

Les fonctionnalités de sécurité applicative sont traitées dans les spécifications fonctionnelles de la même manière que les fonctionnalités métier : il y a donc peu de spécificités à faire ressortir à ce sujet.

Il faut toutefois rester conscient que la conception et la description juste d'une fonctionnalité de sécurité requiert un bon niveau de maîtrise de ce domaine riche et subtil. Le présent ouvrage a été conçu pour donner les clés essentielles à cette activité de spécification !

La spécification fonctionnelle servira de base à la conception du cahier de recette, comme nous le verrons plus loin.

La spécification technique

La spécification technique permet de décrire les mesures techniques mises en œuvre à l'appui de l'implémentation de la spécification fonctionnelle.

Elle inclura :

- la définition du framework technique de développement ;
- la définition de l'environnement d'exploitation, en prenant en compte l'existant technique, y compris la configuration des équipements de sécurité, et les mesures de cloisonnement logique et physique ;
- les principales configurations techniques possibles et/ou nécessaires ;
- le schéma de base de données ;
- la sécurisation des accès des utilisateurs ;
- en cas d'appel à des services tiers, les protocoles d'interconnexion ;

Copyright © 2012 Eyrolles.

- les capacités et performances attendues ;
- les mesures prises pour garantir les conformités techniques : accessibilité, multilinguisme… Pour les collectivités publiques, on inclura le respect du Référentiel général d'interopérabilité (RGI) et du Référentiel général d'accessibilité pour les administrations (RGAA) ;
- la charte graphique ;
- les processus de déploiement et d'exploitation courante.

Du point de vue de la sécurité applicative, la spécification technique détaillera :

- les formats de données, en particulier pour les signatures électroniques (XAdES, PAdES, CAdES), le profil des certificats, la structure des preuves cryptographiques ;
- les algorithmes employés (SHA256, AES, RSA…) et les options appliquées à chacun d'entre eux ;
- les tailles de clés ;
- les logiciels de sécurité inclus dans la solution ;
- les matériels de sécurité impliqués (HSM, cartes à puce…) ;
- les services de tiers de confiance auxquels il sera fait appel…

La spécification technique servira de base à la conception du cahier de recette technique, comme nous le verrons par la suite.

Le développement et l'intégration

Le développement et l'intégration de services de dématérialisation incluant des fonctions de sécurité ne comportent pas de différence majeure par rapport aux projets informatiques généralistes.

Un point intéressant à souligner, pour le développement des processus métier, est l'existence de frameworks de conception qui permettent, *via* des interfaces graphiques, de simplifier l'étape de réalisation des logiciels. Voyons, au travers du témoignage de l'éditeur d'un tel moteur d'applications, ce que l'usage de ce type de technologie peut apporter.

Parole d'expert

Didier Plas, PDG du groupe Genitech, éditeur du moteur d'applications web e-Citiz

Qu'apporte selon vous l'utilisation d'un moteur de Business Process Management pour le développement d'applications dématérialisées ?

Les difficultés de la dématérialisation sont à la fois d'ordre psychologique et technique. La dématérialisation remet en cause les usages dans les organisations et si ce point n'est pas correctement pris en compte, le succès est rarement au rendez-vous.

Copyright © 2012 Eyrolles.

Les premiers apports sont donc à envisager du point de vue de la conduite du changement et du management du projet. Par rapport à un développement *ex nihilo*, le fait de s'appuyer sur un studio interactif de spécification et de conception tel que celui d'e-Citiz permet de concrétiser chaque atelier de spécification par la production d'un prototype mis en ligne très rapidement. Cela permet au métier de s'approprier son e-service et de diviser par 3 les temps de réalisation. Ce type d'outil offre de fait une très grande souplesse, ce qui garantit *in fine* l'obtention d'un e-service adapté au besoin. La dématérialisation des démarches ou processus nécessite, outre la dématérialisation proprement dite, une refonte importante du processus de traitement global. Le fait de travailler par étapes successives matérialisées par des versions successives du portail final est particulièrement adapté aux projets de dématérialisation, dont le contour reste souvent flou jusqu'à ce que les utilisateurs aient sous les yeux les premiers écrans concrets.

Le studio de conception e-Citiz est à la portée des experts métiers formés à la dématérialisation. Il ne demande pas de compétence particulière en informatique : ainsi, des agents fonctionnels qui ont suivi une formation adéquate peuvent être autonomes pour développer ou faire évoluer les procédures dématérialisées.

Du point de vue technique, maintenant, un outil de BPM garantit la robustesse de l'application, l'homogénéité des interfaces graphiques, le multilinguisme, l'accessibilité... Le support des standards garantit l'exécution sur tous les navigateurs ou autres smartphones. L'effort de R&D permanent que nous faisons porter sur le moteur e-Citiz pour prendre en compte les nouvelles directives et les nouvelles technologies réduit d'autant les coûts et les risques des projets pour nos clients.

Le moteur e-Citiz n'inclut pas de fonctionnalités de sécurité applicative telles que la signature électronique ou l'horodatage. Pourquoi ?

Les procédures que nous développons viennent en général s'insérer dans un environnement technique préexistant : GED, annuaire, parapheur électronique sont souvent déjà déployés.

Par ailleurs, il existe de nombreux éditeurs de logiciels spécialisés dans les fonctions de pure sécurité applicative.

Il nous est donc apparu plus pertinent de rester concentrés sur notre cœur de métier, la conception des workflows métier, et d'offrir dans notre outil toutes les interfaces permettant d'interagir avec ces logiciels, ou avec les services de tiers de confiance.

La recette

Organiser la recette

La recette, aussi appelée VABF (Vérification d'aptitude au bon fonctionnement) est la phase de tests qui précédera la mise en production de l'application.

Il faut insister sur l'importance de cette phase, à laquelle une attention particulière et un temps important doivent être consacrés. Une balance

Copyright © 2012 Eyrolles.

réaliste dans les délais de réalisation du projet est constituée d'un tiers de développement pour deux tiers de recette.

La recette se déroule selon deux axes : la recette fonctionnelle, sur la base de la spécification fonctionnelle, et la recette technique, sur la base de la spécification technique. En effet, la recette consiste à vérifier la conformité du logiciel à sa spécification. Une bonne pratique consiste à rédiger un cahier de recette en parallèle avec chacune de ces spécifications.

La recette est bien souvent l'occasion d'identifier des améliorations possibles dans le processus qui a été spécifié, et il est tentant de vouloir inclure ces évolutions immédiatement dans le produit en cours de développement. Si elle n'est pas rigoureusement impossible, cette pratique comporte un double risque :

- un risque sur le calendrier du projet, d'abord, car les adaptations nécessitent spécification, développement et recette ;
- un risque contractuel ensuite, car les améliorations envisagées ne sont pas des anomalies imputables au prestataire de développement.

Afin de maîtriser ces risques, il est recommandé de bien dissocier anomalies et améliorations, et de recenser les évolutions souhaitées, pour les inclure dans une version ultérieure du logiciel, sous un mode maîtrisé.

Du point de vue pratique, la réalisation de la recette nécessite de :

- disposer d'un environnement technique « de recette » dédié, distinct de l'environnement de développement, où travaille l'équipe de réalisation, mais aussi de l'environnement de préproduction, qui sert à valider en vraie grandeur les procédures de montée de version avant le passage en production ;
- mobiliser une équipe constituée d'une part de techniciens informatiques, et d'autre part d'agents « métier » ;
- former cette équipe ;
- lui fournir un outil de remontée et de suivi des anomalies ;
- lui fournir un environnement de tests en-dehors des bureaux habituels (par exemple, une salle dédiée aux tests, avec des machines disposant des différents environnements) ;
- et surtout, lui attribuer du temps, libre de toute autre tâche, avec une continuité suffisante (au moins une demi-journée d'affilée).

Les aspects de ressources sont les plus problématiques pour la réalisation des recettes. Leur résolution nécessite un engagement fort et une réelle volonté de la part de la hiérarchie. Une recette sans ressources suffisantes sera mal réalisée ! Une application mal recettée ne donnera pas satisfaction en production !

Copyright © 2012 Eyrolles.

La recette fonctionnelle

La recette fonctionnelle comporte trois familles de tests :

- **le test du cas nominal**, c'est-à-dire la vérification que, dans le mode d'utilisation normal, l'application a le comportement attendu. Cette famille inclut les tests de non-régression, dont le but est de vérifier que la version N+1 n'a pas remis en cause les fonctionnalités de la version N ;
- **le test des cas d'erreur** les plus prévisibles : il s'agit de vérifier le comportement de l'application dans le cas où, par exemple, les formulaires sont mal remplis, il manque un champ en base de données, les volumes de documents sont dépassés, l'utilisateur double-clique sur les boutons, emploie le bouton Précédent du navigateur, etc. ;
- **la recette par échantillonnage**, qui consiste à naviguer au hasard dans l'application et à tester les réactions face à un comportement ressemblant à celui d'un utilisateur réel, non averti.

Seuls les deux premiers types de tests donnent lieu à l'établissement d'un cahier de recette.

La recette technique

La recette technique comporte plusieurs familles de tests :

- les tests de charge ;
- les tests de performances ;
- la vérification des formats de données, en particulier pour les fonctions cryptographiques ;
- si l'application fait appel à des tiers de confiance, la vérification des interfaces avec ces tiers et, éventuellement, de la conformité de leurs pratiques avec leurs engagements ;
- les tests d'intrusion ;
- les tests d'installation et de configuration ;
- les tests de migration ;
- les tests de conformité aux normes applicables, aux diverses versions de navigateurs et d'OS…

La documentation

Menée en parallèle avec le développement, la documentation de l'application est un point fondamental pour garantir la sécurité et la confiance.

Du point de vue fonctionnel, il s'agit des manuels utilisateurs et/ou de l'aide en ligne qui leur sera fournie : ces documents doivent être très explicites sur les fonctions de sécurité mises en œuvre de manière à simplifier l'accès au service et à rassurer les utilisateurs. Il s'agit donc d'un élément clé de la confiance.

Copyright © 2012 Eyrolles.

Du point de vue juridique, il s'agit des conditions générales d'utilisation et de la convention de preuve : ici, la documentation couvre à la fois le domaine de la confiance et celui de la sécurité.

Enfin, du point de vue technique, il s'agit de l'ensemble des procédures de configuration, d'exploitation, de renouvellement des clés et des certificats, de surveillance du bon fonctionnement, etc. On est là purement dans le domaine de la sécurité.

La conduite du changement

La conduite du changement est une activité majeure des projets de dématérialisation, qui est trop souvent négligée, ou restreinte à la formation des utilisateurs.

Le changement doit être anticipé dès l'amont du projet, et pour l'ensemble des populations concernées : utilisateurs externes et internes, décideurs, exploitants et partenaires.

Parmi les bonnes pratiques, citons quelques points incontournables.

Impliquer les utilisateurs dans la conception des services qui les concernent : un projet de dématérialisation qui amènera les personnels de l'entreprise à remplacer le traitement de dossiers papier par un traitement informatisé fait courir un risque d'immobilisation de l'activité si ces agents ne s'approprient pas l'outil. En les associant en amont au choix, à la conception, à la recette du service, voire à la formation de leurs homologues, on peut s'appuyer sur l'enthousiasme de quelques éléments clés de l'organisation pour « faire passer » en douceur l'évolution des modes de travail.

Prendre en compte le temps d'acculturation. Il existe deux modes de déploiement : le « big bang », qui consiste à migrer d'un seul coup de l'ancien mode de fonctionnement au nouveau, et la migration « en biseau », qui fait cohabiter pendant un temps les deux modes de traitement de l'information.

Chacun de ces modes présente des avantages et des inconvénients, et le choix doit être fait en fonction de l'analyse du contexte.

Pour des utilisateurs externes, il est rassurant de conserver la possibilité de traiter les dossiers papier, et mettre en œuvre une politique concertée d'incitation au passage à la dématérialisation, de manière à amener progressivement les usagers aux modes innovants de communication.

Pour une application interne, le fait de ne pas laisser le choix permet d'optimiser les coûts de traitement en ne conservant qu'un seul circuit de traitement. En revanche, en cas de dysfonctionnement de la nouvelle application, le rejet risque d'être sévère.

Copyright © 2012 Eyrolles.

Prendre en compte les aspects techniques : la dématérialisation va induire des évolutions organisationnelles importantes et des processus nouveaux (traçabilité des accès aux serveurs et des actions réalisées, changement des modes d'authentification…). Les exploitants techniques sont aux premières loges du changement ! De plus, de par leur statut d'utilisateurs à forts privilèges, une grande part de la sécurité repose sur leur compréhension et leur acceptation des règles : les solutions de contournement sont toujours rapides à trouver pour un exploitant qui s'inscrit en opposition à une contrainte, il convient donc d'accompagner avec pédagogie les nouvelles contraintes et les nouveaux modes de travail. Après une première phase de réticence, les équipes techniques se réjouissent en général de la sérénité que leur offre un cadre organisationnel bien défini, car l'abandon du « bricolage » pour l'application de règles claires réduit considérablement les risques d'erreurs et les soirées passées à réparer leurs conséquences.

Ne pas négliger les réticences : on ne peut pas se contenter de dire « puisque c'est obligatoire, il faudra bien qu'ils y passent » ! En effet, faute d'un accompagnement suffisant et d'outils ou procédures suffisamment bien conçus, les risques de rejet existent, tant au niveau des utilisateurs des services qu'au niveau des décideurs.

Il faut à ce sujet souligner que, selon les populations visées par le service dématérialisé, l'ampleur et les conséquences des réticences ne seront pas identiques.

Ainsi, le management intermédiaire et les agents administratifs seront souvent prêts à faire l'effort nécessaire à la prise en main d'un nouvel outil, parce que le travail sur ordinateur est leur quotidien. Toutefois, l'augmentation du travail sur écran provoque une fatigue oculaire bien réelle, qui sera en général mise en avant à l'occasion du changement de pratiques. La nier serait interprété par les agents comme un signe de mépris : il est donc fondamental de leur faire savoir que le sujet a été pris en compte, par exemple en les équipant de meilleurs écrans, ou en organisant des pauses régulières, le tout avec le concours du CHSCT.

Des précautions particulières doivent être prévues si l'on déploie des outils de dématérialisation auprès d'opérateurs techniques, plus habitués à travailler sur le terrain, dans le « monde réel » : une moins grande maîtrise de l'outil informatique et une culture plus axée sur le concret ne favoriseront pas leur adhésion.

Enfin, il sera également nécessaire d'être extrêmement prudent dans la façon d'introduire de nouveaux outils auprès de décideurs, pour qui la fluidité et le gain de temps seront des éléments positifs, mais la complexité, la lenteur ou une ergonomie défaillante provoqueront un rejet sans appel.

Copyright © 2012 Eyrolles.

Par exemple, un parapheur électronique mal conçu et complexe à utiliser pourrait entraîner le refus du PDG de s'en servir – et il faudrait alors rematérialiser les documents pour les soumettre à sa signature dans un parapheur papier traditionnel, rompant ainsi la chaîne de la dématérialisation.

Soigner la communication : faire connaître les nouvelles règles, l'existence des nouveaux services, etc., est fondamental, tant en interne que vers les usagers externes et les partenaires. La communication ne commence pas à la mise en production du nouveau processus ou du nouveau service, mais dès sa conception. La phase de démarrage, elle, s'accompagne d'une série de formations qui viennent conclure le plan de communication mis en œuvre depuis longtemps.

Adapter l'organisation et les méthodes de travail : c'est grâce à ce point essentiel de la conduite du changement que la dématérialisation portera ses fruits, en termes de retour sur investissement. Il est possible de compter sur les utilisateurs et sur la souplesse de l'organisation pour qu'elle se réorganise d'elle-même une fois le nouvel outil déployé ; mais il est bien plus efficace de concevoir les nouvelles structures de travail en même temps que l'outil qui les sous-tend.

Ce besoin porte non seulement sur la structure des équipes, pour prendre en compte les gains de temps de traitement générés par la dématérialisation, ou la modification des circuits de l'information, mais aussi sur les pratiques quotidiennes des employés.

Prenons l'exemple de la dématérialisation du processus achat : si l'acheteur, à l'occasion du passage à la dématérialisation, cesse de demander aux fournisseurs un mémoire technique à l'appui de leurs propositions, et remplace cette demande par un cadre de réponse technique et financier formalisé selon ses propres critères, l'outil informatique lui permettra de comparer bien plus efficacement les offres en mettant en parallèle des éléments objectivement comparables. Il bénéficiera ainsi à plein des apports de la dématérialisation, qui ne constituera pas juste un changement de support de l'écrit, mais bien une refonte des processus de travail.

Anticiper les besoins périphériques : les utilisateurs qui sont mis face au nouveau processus dématérialisé ont bien évidemment besoin d'un support, téléphonique ou par e-mail, pour les accompagner dans leur montée en compétence sur l'outil. Pour un service métier dématérialisé au sein d'un service, cette cellule support peut être prévue en interne, par exemple sous la forme d'un expert référent intégré dans l'équipe. Elle peut également être centralisée pour l'ensemble de l'entreprise, ou externalisée auprès d'un prestataire de services.

Un point d'attention est la disponibilité des matériels dont les utilisateurs peuvent avoir besoin : scanners, s'il faut inclure des copies de documents

Copyright © 2012 Eyrolles.

papier reçus, ou imprimantes, pour améliorer le confort de lecture de documents volumineux transmis par voie dématérialisée. Mais il faut être prudent à ne pas perdre le bénéfice de la dématérialisation si les agents en charge des traitements impriment systématiquement toutes les données qu'ils doivent analyser. Plusieurs parades à ce risque peuvent être mises en œuvre : la communication interne, tout d'abord, mais aussi l'éloignement de l'imprimante, de manière à dissuader les agents d'y faire appel systématiquement.

Illustrons maintenant l'importance de la conduite du changement par un retour d'expérience concret.

Parole d'expert

Gilles Pourcher, DGA du pôle Ressources, Région Limousin

Vous pilotez depuis 2009 le projet de portail global de dématérialisation des procédures de la Région Limousin, Planet Limousin. Comment avez-vous appréhendé la conduite du changement ?

La Région a abordé la conduite du changement dès l'amont du projet, car la dématérialisation de nos processus métier constitue un projet stratégique à tous points de vue.

En interne, tout d'abord, la dématérialisation concerne toutes nos équipes, depuis les agents qui traitent les dossiers jusqu'au président de Région qui les signe maintenant électroniquement, en passant par les services supports et le service informatique. En associant très tôt les équipes métier à la conception et à la recette de l'outil, nous avons créé une véritable dynamique autour du projet.

Le projet intègre l'ensemble de nos partenaires (entreprises, organismes de formation, services de l'État...) : la modification de nos échanges avec tous les acteurs de la chaîne a nécessité une longue préparation et beaucoup de diplomatie, ainsi qu'une bonne prise en compte des contraintes de chacun dans la conception des interfaces qui leur étaient destinées.

Enfin, vis-à-vis des usagers des services de la Région, la révolution des usages n'aurait pas été possible sans une communication progressive, des sessions de formation aux nouveaux outils et un accompagnement très fort.

À quels défis principaux avez-vous dû faire face en termes de conduite du changement ?

Le premier défi est de convaincre, en interne, de la pertinence du projet, de ses apports pour la Région et ses usagers, de sa faisabilité. Aujourd'hui, le succès des deux premières procédures dématérialisées (la gestion de la formation professionnelle et la gestion des demandes d'aides) donne aux autres services des perspectives passionnantes, puisque le socle technique mis en place sera mutualisé pour toutes les procédures à venir. Mais au début, il fallait y croire, et sans une motivation sans faille de l'équipe projet, cela n'aurait pas été possible.

Le deuxième défi est l'adéquation des outils aux besoins des utilisateurs. Nous avons fait le choix d'une dématérialisation totale des procédures, ce qui impliquait

Copyright © 2012 Eyrolles.

de gérer l'exhaustivité des cas d'exception ou des situations rares. Il est fondamental de ne pas mettre un agent ou un usager face à un état bloquant qui ne serait pas géré par le système ! Par ailleurs, l'ergonomie des écrans est un facteur de succès indispensable pour l'appropriation du changement par les utilisateurs : si le parapheur électronique est aujourd'hui employé quotidiennement par le président de Région, cela a nécessité une prise en compte minutieuse de ses habitudes de travail.

Enfin, notre troisième défi est devant nous : la conception d'un outil dématérialisé pour gérer les flux métier devient structurante dès que l'outil est déployé. S'il est aisé de faire évoluer une procédure qui passe par des échanges papier, cela devient beaucoup plus lourd lorsque cela nécessite l'évolution de l'outil informatique. La prise en compte des changements futurs va sans doute nous amener, pour les prochaines procédures dématérialisées, à changer de granularité lors de la conception fonctionnelle.

Quels sont pour vous les facteurs clés de succès d'un projet d'une telle envergure ?

Le premier facteur de succès est la motivation, qui passe par la reconnaissance de l'équipe projet. Sur un projet de plusieurs années comme Planet Limousin, conserver intacts l'énergie et l'élan des agents nécessite un soutien sans faille de la hiérarchie.

L'organisation, les ressources mises en œuvre sont également fondamentales : un suivi régulier du projet, avec une implication du plus haut niveau de décision, permettra de débloquer des ressources aussi simples que du temps, pour les agents des services métiers dont le projet de dématérialisation n'est pas la tâche principale, ou des salles et des machines, par exemple pour réaliser la recette de l'application, etc.

Mais le plus important est peut-être le pragmatisme : lorsque chacun fait de son mieux, avec du bon sens, sans idéologie, mais avec la volonté de servir le projet commun, lorsque les décisions sont collégiales et réalistes, le succès se rapproche !

La formation

La formation peut être considérée comme une partie de la conduite du changement, mais il est important de l'en dissocier pour éviter qu'elle en devienne l'élément principal.

La formation portera sur l'ensemble des utilisateurs concernés par le service déployé, internes ou externes, clients ou partenaires, fonctionnels ou techniques.

La formation doit être menée au plus près du déploiement, de manière à ce que les explications fournies soient encore fraîches lors de la mise en œuvre effective du logiciel.

La période de formation à l'outil dématérialisé et aux nouvelles procédures de travail est également un moment privilégié pour procéder à une sensibilisation à la sécurité informatique dans son ensemble, et en particulier aux règles de bonne gestion du poste de travail.

Copyright © 2012 Eyrolles.

Le déploiement

La phase de mise en production se fait en deux étapes :

- l'installation sur une plate-forme de préproduction de l'application, en suivant la procédure préétablie ;
- les tests de bon fonctionnement en préproduction : ces tests ne constituent pas une recette destinée à chercher des anomalies, mais une vérification de bon fonctionnement dans l'environnement de préproduction, supposé identique techniquement à celui de production ;
- l'installation en production, en suivant la procédure préétablie ;
- les tests de bon fonctionnement en production.

Il n'y a pas de spécificité propre aux projets incluant des fonctions de sécurité.

Le maintien en conditions opérationnelles

Le maintien en conditions opérationnelles est ensuite la phase d'exploitation courante du service, dans laquelle s'appliquent les procédures d'exploitation définies en amont :

- authentification et traçabilité des accès des administrateurs ;
- sauvegardes ;
- archivage électronique ;
- redémarrages périodiques ;
- synchronisation des serveurs ;
- veille sur la validité des certificats ;
- purge des données obsolètes ;
- anonymisation des données personnelles ;
- veille sur la configuration des équipements de sécurité (pare-feu, antivirus, sonde de détection d'intrusion, HSM)…

Il convient, au cours de l'ensemble de la vie du projet, de mettre en œuvre une surveillance permanente sur les dates de validité des certificats de la plate-forme et des utilisateurs, de manière à anticiper leur renouvellement.

La phase de production est également le temps de la vérification de service régulier (VSR) : un suivi de l'équipe projet est donc nécessaire jusqu'à la fin de cette période.

Copyright © 2012 Eyrolles.

Chapitre 15

Organiser la dématérialisation

La dématérialisation : un projet d'entreprise transverse

Nous avons vu dans le chapitre précédent que la conception d'un service dématérialisé nécessitait un ensemble de compétences complémentaires qui couvrent quasi tout le spectre des activités de l'entreprise.

Une équipe projet sera ainsi composée de membres des diverses directions de l'entreprise capables de répondre à chacun des enjeux soulevés par la dématérialisation.

De même, un service Recherche et développement appelé à concevoir et développer des logiciels liés à la dématérialisation devra inclure ou pouvoir faire appel à l'ensemble de ces compétences.

Plus largement, dans un projet d'entreprise axé sur la dématérialisation, chacune des entités a son rôle à jouer. Détaillons ici leurs responsabilités respectives.

La direction générale joue un rôle moteur dans le projet. Sans volonté au plus haut niveau, un projet aussi ambitieux que la refonte de processus métier en vue de leur dématérialisation a peu de chance d'aboutir concrètement. L'engagement de la direction générale passe par l'allocation de ressources humaines et financières au projet, mais aussi par la communication interne, puisqu'il s'agit d'une orientation stratégique qui concerne l'ensemble de l'entreprise.

Les directions métier seront bien entendu impliquées au premier chef, pour la définition des processus à dématérialiser et la conception des nouveaux modes de travail. Elles sont détentrices de la connaissance de l'existant et garantes de l'adéquation de la solution mise en œuvre avec

Copyright © 2012 Eyrolles.

les besoins de l'entreprise. Ce n'est que grâce à elles que le déploiement du nouvel outil peut être un succès.

La direction informatique, ou la DSI, porteuse des compétences techniques, joue un rôle essentiel tant pour le choix des solutions techniques et la définition du contexte d'exploitation du service que pour les méthodologies de conduite de projet informatique.

Le RSSI (Responsable de la sécurité du système d'information) occupe une place particulière, puisqu'il garantira le respect des contraintes de sécurité et des procédures qui y sont liées.

La direction juridique sera fortement sollicitée, comme nous l'avons vu tout au long de cet ouvrage, pour l'analyse du contexte, les choix des mécanismes de sécurité à mettre en œuvre pour respecter les obligations, la rédaction de la convention de preuve. Attention toutefois, le droit de la preuve et le droit des nouvelles technologies ne sont souvent pas au cœur des activités de la direction juridique d'une entreprise ou d'une collectivité publique. Il pourra donc être nécessaire de prévoir une mise à jour des compétences disponibles, sous la forme d'une formation, d'un recrutement ou de l'appel à un cabinet spécialisé.

La direction des ressources humaines, enfin, sera fortement mise à contribution pour tous les aspects liés à la gestion d'identités : constitution de l'annuaire, déploiement de certificats, etc.

Devant la multiplicité des compétences nécessaires aux projets de dématérialisation, certains grands groupes ont mis en œuvre une direction de la dématérialisation, aux fonctions transverses.

Vers une direction de la dématérialisation ?

La dématérialisation consiste principalement en une évolution du support de l'information, du papier vers l'électronique. Cette activité a une dimension technique, du fait de son substrat informatique, mais également une dimension organisationnelle importante puisqu'il s'agit de gérer le cycle de vie de l'information qui circule au sein de l'entreprise et dans son environnement, depuis sa création jusqu'à sa conservation à long terme, en passant par son utilisation à des fins métier ou juridiques.

À la lumière de cette définition, là où une direction informatique avait autrefois pour mission principale de gérer des machines et de garantir leur bon fonctionnement, le terme plus répandu aujourd'hui de direction du système d'information prend toute son ampleur. Le système d'information global inclut en effet non seulement les ordinateurs qui servent de support à cette information, mais également les applications au sein desquelles ces informations sont générées, collectées, utilisées, conservées – et, plus

Copyright © 2012 Eyrolles.

largement, les interactions de ces logiciels avec les humains qui sont et doivent demeurer le cœur de l'entreprise.

Il est universellement reconnu que la maîtrise de l'information est aujourd'hui un enjeu majeur pour les entreprises, source de productivité, mais également de souveraineté et de capacité de décision.

La valeur financière et juridique de l'information justifie ainsi d'ajouter un cercle supplémentaire au périmètre de la DSI, en lui insufflant la dimension stratégique. Il ne s'agit plus de gérer le système d'information mais de le concevoir et de le déployer dans une vision globale, incluant au plus haut niveau les aspects décisionnels permis par la traçabilité, et au plus près de chaque utilisateur connecté au réseau, la dimension de sécurité qui ne repose pas seulement sur les dispositifs techniques mais aussi sur les aspects comportementaux.

Les notions de sécurité et de confiance, que nous avions précédemment abordées principalement du point de vue des utilisateurs des services dématérialisés prennent ici une dimension supérieure, parfaitement illustrée par l'affaire Kerviel : les fonctions essentielles de l'entreprise peuvent être remises en cause par un système d'information insuffisamment sécurisé ou des procédures non fiables ou non appliquées.

La capacité de management d'un dirigeant d'entreprise est aujourd'hui entièrement liée à la confiance qu'il peut avoir dans son système d'information. Si le secteur bancaire a parfaitement pris conscience de ces enjeux et a mis en place un arsenal de normes sectorielles adapté aux besoins, il devrait en être de même dans l'ensemble des secteurs de l'industrie ou des services.

L'émergence, dans certains grands groupes, d'une direction de la dématérialisation, qui regroupe des compétences techniques, juridiques et organisationnelles, appuyées par des capacités financières et décisionnelles, marque une nouvelle étape dans la prise de conscience du caractère réellement révolutionnaire, structurant et inéluctable de la dématérialisation.

Copyright © 2012 Eyrolles.

Copyright © 2012 Eyrolles.

Index

Cas pratiques

accès au compte bancaire 56
Achatpublic.com 43, 117, 125, 149, 201
Adobe Reader 200
affaire Kerviel 299
anonymisation de données médicales 26
Applatoo 47, 154
archivage
  des e-mails 241
  des versions de travail des documents 241
  du code source 242
attaque
  man in the middle 104
    contre Facebook 141
authentification forte 195
badge multi-usage 275
Banque Casino 203
Carte nationale d'identité électronique 129
Certigreffe 109
changement de certificat 68
CNIE (Carte nationale d'identité électronique) 129
confidentialité des e-mails 146
conservation des contrats conclus avec des particuliers 248
construction d'un bâtiment 235
dématérialisation
  des achats 293
  des factures 9
  des marchés publics 149, 153, 166, 184, 216, 233
  fiscale des factures 192, 271
dépôt de marque à l'INPI 57
DICT.fr 44, 205
Diginotar 133, 139
documents RH 241, 246
données médicales 157
e-attestations 44, 205
e-bourgogne 280
e-commerce 217
e-stonia 129
ETSCAF 145
horodatage de signature électronique 223
huissiers de justice 244
Idénum 131
jedeclare.com 281
jeux d'argent et de hasard en ligne 215, 233
justificatif de domicile 8
lettre recommandée électronique 217
magasin de certificats de Windows 97
Microsoft Office 199
notaires 244
parapheur électronique 293

Copyright © 2012 Eyrolles.

Planet Limousin 70, 120, 202, 204, 213, 280
réponse aux marchés publics 57
reseaux-et-canalisations.gouv.fr 70
réseaux sociaux 57
scellement
d'un certificat 194
d'une LCR 194
d'une réponse OCSP 194
d'un horodatage 194
de code exécutable 193
des traces applicatives 194
services publics dématérialisés 218
signature électronique
d'e-mails 180
d'un fichier ZIP 179
et engagement 273
par tablette graphique 189
Signexpert 199, 282
souscription de contrat dématérialisé en agence 205
télédéclaration IR 38
Télé IR 202
téléservice Réseaux et canalisations 117, 126, 192, 202, 206, 217
traçabilité
bancaire 215, 220
des FAI et fournisseurs d'hébergement de contenu 216
et données à caractère personnel 272
validation des CGU 206
vérifier une signature manuscrite 87
vote par Internet 150, 153, 155, 231

Définitions

AC (Autorité de certification) 92, 107
accusé de réception 227
AdES-A (Archiving) 177
AdES (Advanced Electronic Signature) 177
AdES-BES (Basic Electronic Signature) 177
AdES-C (Complete) 177
AdES-L (Long-term) 177
AdES-T (Timestamp) 177
AdES-X (Extended) 177
AE (Autorité d'enregistrement) 107
annuaire 78
anonymisation 157
ANSSI (Agence nationale de la sécurité des systèmes d'information) 30
applet Java 200
AR (Autorité de révocation) 108
archivage
électronique 235, 262
plan d' 245
archives
courantes 242
définitives 243
intermédiaires 243
recherche d' 249
restauration d' 249
Arjel (Autorité de régulation des jeux en ligne) 215
attaque
écoute et rejeu 77
force brute 33, 74
man in the middle 133
par dictionnaire 75
authentification 28, 58
d'un serveur 64
faible 69
forte 69
jeton d' 80

Copyright © 2012 Eyrolles.

autorité
d'enregistrement 107
d'horodatage 222
de certification 92, 107
de révocation 108
de validation 108
AV (Autorité de validation) 108
bac à sable 193
badge multi-usage 275
bi-clé 28
BPM 10
cachet 191
politique de 260
serveur 191
CAdES (CMS Advanced Electronic Signature) 177, 197
captcha 76
Card Management System 275
carte à puce 100
cercle de confiance 83
certificat 32, 85
AKI 91
autosigné 110, 118
Basic constraints 92
classe 120
CN (Common Name) 90
CRLDP 91
dates de validité 91
délivrance 109
demande 109
DN (Distinguished Name) 89
enveloppe autonome 97
Extended key usage 91
famille de 92, 107
interopérabilité 122
Key usage 91
magasin de 95
numéro de série 91
porteur de 107
profil de 89
qualifié 121, 168
renouvellement 117
révocation 113
scellement 93
SKI 91
stratégie de 92
support 94
support dynamique externalisé 98
support matériel 99
suspension 115
utilisateur de 107
validation 115
Certificate Revocation List 114
Certificate Signing Request 110
certification
chaîne de la 118
croisée 119
de sécurité de premier niveau 48
opérateur de 108
politique de 259
chaînage cryptographique des traces 225
chaîne
de la certification 118
de la confiance 51
chiffrement 29, 146
classe
1 121
2 121
3 121
3+ 121
de certificat 120
clé
cryptographique USB 100
privée 27
publique 27
secrète 32
symétrique 32
taille de la 30
CMS (Card Management System) 275
coffre-fort électronique 237
Cofrac (Comité français d'accréditation) 49
condensation 24
confiance 35

Copyright © 2012 Eyrolles.

confidentialité 143
  politique de 263
contremarque de temps 222
convention de preuve 254
CRL (Certificate Revocation List) 114
cross-certification 119
cryptage 146
cryptographie
  à clé publique 27
  à clé secrète 32
  asymétrique 27
  symétrique 32
CSPN (Certification de sécurité de premier niveau) 48
CSR (Certificate Signing Request) 110
déclaration de pratiques 257
défi/réponse 64
délivrance de certificat 109
Delta LCR 115
demande de certificat 109
dématérialisation 7
dictionnaire (attaque par) 75
donnée à caractère personnel 144
données métier 212
Dublin Core 246
écoute et rejeu (attaque par) 77
empreinte 24
enregistrement 107
enrôlement 107
entiercement 242
enveloppe autonome 97
étoiles du RGS 123
famille de certificats 92, 107
fédération d'identités 83
FNTC (Fédération nationale des tiers de confiance) 41
fournisseur d'identités 83
GED 10
génération de clés embarquée 101
gestion
  des habilitations 145
  des identités et des accès 10
  des processus métier 10
  électronique de documents 10
Hardware Security Module (HSM) 102
hash 24
horodatage 221
  autorité d' 222
  certifié 222
  jeton d' 222
  politique d' 258
  simple 221
HSM (Hardware Security Module) 102
IAM 10
ICP (Infrastructure à clé publique) 108
identifiant 60
  constitution 72
identification 58
identité 55
  numérique 56
IGC (Infrastructure de gestion de clés) 108
index 238
infrastructure
  à clé publique 108
  de gestion de clés 108
inscription en ligne 82
intégrité 193
interopérabilité des certificats 122
ISO 15836 246
jeton d'horodatage 222
key logger 76
LCR (Liste de certificats révoqués) 114
logs techniques 224
magasin de certificats 95
  de confiance 124
man in the middle 133

Copyright © 2012 Eyrolles.

matériel cryptographique 102
méta-annuaire 79
métadonnées 238, 246
mot de passe 60
  à usage unique 61
  constitution 74
  dynamique 61
  fort 74
obfuscation 157
OC (Opérateur de certification) 108
OCSP (Online Certificate Status Protocol) 116
OTP (One-Time Password) 61
PAdES (PDF Advanced Electronic Signature) 177, 197
PC (Politique de certification) 107
PDF/A 243
PGP 137
phishing 77
PIN (Personal Identification Number) 101
PKI (Public Key Infrastructure) 108
plan
  d'archivage 245
  de classement 245
politique
  d'archivage électronique 240, 262
  de cachet 260
  de certification 92, 107, 259
  de confidentialité 263
  de gestion des identités et d'authentification 263
  de signature électronique 260
  de traçabilité et de gestion de preuves 231, 261
  d'horodatage 258
PoP (Proof of Possession) 109
porteur de certificat 107
prestataire
  de validation de certificats électroniques 43
prestataire de services
  d'archivage électronique 43
  d'horodatage électronique 43, 222
  de certification électronique (PSCE) 43, 92, 107
  de confiance 42
    qualification 42
  de gestion de preuves 43
  de signature électronique 43
  de validation de certificats électroniques 43
preuve
  cryptographique 225
  de possession 109
  renversement de la charge de la 170
principe des quatre yeux 151
profil d'acheteur 216
Proof of Possession 109
protocole de consentement 203
provenance 193
PSAE (Prestataire de services d'archivage électronique) 43
PSCE (Prestataire de services de certification électronique) 43, 92, 107
PSCO (Prestataire de services de confiance) 42
  qualification 42, 49
PSGP (Prestataire de services de gestion de preuves) 43
PSHE (Prestataire de services d'horodatage électronique) 43, 222
PSSE (Prestataire de services de signature électronique) 43
Public Key Infrastructure 108
PUK (PIN Unlocking Key) 101
PVCE (Prestataire de validation de certificats électroniques) 43

Copyright © 2012 Eyrolles.

qualification des produits de sécurité 47
question secrète 68
recherche d'archives 249
rejeu 69
rejouable 69
renouvellement de certificat 117
renversement de la charge de la preuve 170
restauration d'archives 249
réversibilité 240
révocation 113
RGS (Référentiel général de sécurité) 23
  étoiles 123
sauvegarde 236
sécurité 35
  applicative 11, 18
  chaîne de la 21
  comportementale 19
  technique 16
session 60
signataire 168, 171
signature
  d'approbation 179
  de certification 179
  définition
    juridique 165
    pratique 161
  électronique 29
    à la volée 203
    avancée 171
    définition 162, 166, 171, 175
    dispositif sécurisé de création 101
    politique de 260
    présumée fiable 166, 170
    sécurisée 169
    simple 168
    vérification 180, 181, 184
Single Sign-On 80
source de temps 221
SSL (Secure Socket Layer) 63
SSO (Single Sign-On) 80
stockage 236
strate 221
stratégie de certificat 92
support
  de certificat 94
  dynamique externalisé 98
  logiciel 95
  matériel 99
système de gestion des cartes 275
TBS Certificate 110
test de Turing 76
tiers
  archiveur 240
  de confiance 40
TLS (Transport Layer Security) 63
traçabilité 211
traces applicatives 224
Turing (test de) 76
URL 63
utilisateur de certificat 107
VABF (Vérification d'aptitude au bon fonctionnement) 288
validation de certificat 115
Vérification d'aptitude au bon fonctionnement (VABF) 288
vérification de signature électronique 180
XAdES (XML Advanced Electronic Signature) 177, 197

Normes

2TUP 267
AES 32, 147, 149, 154, 287
AES CBC 32
AES ECB 32

Copyright © 2012 Eyrolles.

CAdES (CMS Advanced Electronic Signature) 22, 177, 178, 179, 197, 202, 222, 261, 287
CAPI 104
CMS 148, 177
Convergence 140
CSP (Cryptographic Service Providers) 104, 193
CSPN (Certificat de sécurité de premier niveau) 233
EBIOS (Expression des besoins et identification des objectifs de sécurité) 124, 284
ElGamal 151
ETSI 101456 50, 127
extreme programming 267
GS1, recommandations pour l'échange de factures dématérialisées fiscalement 192
ISO 14641 237
ISO 14641-1 22
ISO 14721 237
ISO 15408 48
ISO 15489 237
ISO 27000 22
ITIL 267
label FNTC
  coffre-fort électronique 237
  tiers archiveur 237
LDAP 79
Merise 267
MoReq2010 237
NF Z42-013 22, 237
NF Z42-025 23
NTP (Network Time Protocol) 221
OAIS (Open Archival Information System) 237
PAdES (PDF Advanced Electronic Signature) 22, 177, 178, 179, 197, 202, 261, 287
PC/SC (Personal Computer/ Smart Card) 104
PGP 137
PKCS 22
PKCS#7 148, 177
PKCS#11 104, 193
PKCS#12 98, 156
PKCS#15 105
RACHE (Rapid Application Conception and Heuristic Extreme-programming) 267
Référentiel général d'accessibilité pour les administrations (RGAA) 287
Référentiel général d'interopérabilité (RGI) 287
RFC 2527 22
RFC 2560 22, 116
RFC 2630 22, 148
RFC 3039 92
RFC 3161 22, 222
  annexe A 223
RFC 3647 259
RFC 4055 22
RFC 4330 221
RFC 5280 22, 89, 115
RGAA (Référentiel général d'accessibilité pour les administrations) 287
RGI (Référentiel général d'interopérabilité) 287
RGS (Référentiel général de sécurité) 23, 167, 172, 191, 258, 259, 274, 282
  étoiles 23
RSA 27, 147, 149, 154, 164, 175, 287
SHA256 24, 175, 287
S/MIME 148
Sovereign Keys 140
SSL (Secure Socket Layer) 63, 151
standard d'échange de données pour l'archivage DAF 237
Time Stamp Protocol (TSP) 222

Copyright © 2012 Eyrolles.

TLS (Transport Layer Security) 63
TSP (Time Stamp Protocol) 222
UML 286
X.500 79
X.509 89, 90
XAdES (XML Advanced Electronic Signature) 22, 177, 178, 179, 197, 261, 287
XMLDSig 178

Paroles d'experts

Borghesi Alain, Cecurity.com 239
Caprioli Éric, avocat, cabinet Caprioli et associés 252
Colin Pascal, Keynectis 50
Denuzière Jean, Ilex 81
Du Boullay Charles, CDC Fast et CDC Arkhinéo 218
Kaeb Thomas, Wacom 188
Maraval Philippe, Pôle Emploi 185
Maréchaux Bertrand, ANTS 130
Mattatia Fabrice, CDC 131
Plas Didier, Genitech 287
Poidevin Emmanuel, e-attestations 45
Pourcher Gilles, Région Limousin 294
Saphores Jean, CSOEC 281
Treins Michel, Ineris 71
Trotin Armelle, LSTI 135
Vantorre Ignace, Sogelink 20
Zimmermann Philip, cryptologue 139

Textes législatifs et réglementaires

arrêté
- du 26 juillet 2004 49
- du 28 août 2006 252
- RGS du 18 mai 2010 24

Code civil
- article 1108-2 270
- article 1156 255
- article 1162 255
- article 1316 12
- article 1316-1 12, 194, 239
- article 1316-2 252, 254
- article 1316-3 12
- article 1316-4 164, 165, 166, 187, 260, 272, 273, 282
- article 1369-8 217

Code de commerce, article L.123-22 248
Code de la consommation
- article L.132-1 253, 255
- article L.134-2 248
- article R132-2 253

Code de la propriété intellectuelle
- article L.331-12 216
- article L.336-3 216

Code des marchés publics 185
- article 56 216, 271
- article 57 270

Code des postes et télécommunications, article L.34-1 216
Code général des impôts
- annexe 3, article 96 F 272
- article 289 V 192, 271

communication de la Commission européenne du 8 octobre 1997 38
décret
- n° 79-1037 du 3 décembre 1979 242
- n° 2001-272 du 30 mars 2001 101, 107, 122, 164, 166, 168, 169, 170, 191, 272, 282

Copyright © 2012 Eyrolles.

n° 2002-535 du 18 avril 2002 47, 49
n° 2011-144 du 2 février 2011 217
RGS 2010-112 du 2 février 2010 48
délibération CNIL n° 2010-371 du 21 octobre 2010 150, 232
directive
1999/93/CE du 13 décembre 1999 38, 39, 121, 164, 171, 172, 173, 191, 192, 251
Commerce électronique 2000/31/CE du 8 juin 2000 39
loi
Informatique et libertés n° 78-17 du 6 janvier 1978 7, 11, 144, 220, 230, 272
n° 2000-230 du 13 mars 2000 11, 164, 166, 251, 252
n° 2004-575 pour la confiance dans l'économie numérique (LCEN) du 21 juin 2004 39, 122, 215
n° 2004-801 du 6 août 2004 144
n° 2009-526 du 12 mai 2009 270
n° 2010-476 du 12 mai 2010 215
ordonnance n° 2005-1516 du 8 décembre 2005 23, 42, 218, 227, 256
règlement n° 97-02 de la Banque de France 51
RGS (Référentiel général de sécurité) 23, 39, 42, 123

Copyright © 2012 Eyrolles.