Square des Utilisateurs

Signature cryptographique : du numérique à l'électronique

Après l'article paru dans La Lettre d'ADELI n°42 de janvier 2001, présentant les généralités concernant la sécurité (au sens « security »), la sûreté (au sens « safety ») et la sûreté de fonctionnement (au sens « dependability ») des systèmes d'information, puis l'article paru dans La Lettre d'ADELI n°44 de juillet 2001 évoquant les problématiques de sécurité, sûreté et sûreté de fonctionnement relatives à l'intimité (au sens « privacy ») des données à caractère personnel, ce troisième article se focalise sur un premier niveau de généralités autour des concepts et propriétés de la signature électronique.

- *Qu'entend-on par signature… cryptographique : signature numérique ? signature électronique ?*
- *Que peut-on faire à l'aide de signature : s'authentifier ? authentifier ? certifier ? accréditer ?*
- *Quelles responsabilités peuvent être supportées : techniques ? organisationnelles ? juridiques ?*

Cet article présente les quelques fondements historiques et technologiques de la signature avec une vision sur ses retombées envisageables à moyen et long termes. Le lien est fait avec la propriété d'auditabilité, évoquée dans les précédents articles de la commission « Sécurité(s) & Sûreté(s) », comme étant un des piliers de la sécurité des systèmes d'information et donc de la confiance en ceux-ci et de leur maîtrise.

L'article qui suit est constitué d'extraits d'un ouvrage à paraître en janvier 2002 aux éditions Eyrolles qui s'intitule « Sécuriser ses échanges avec une PKI : Solutions techniques et aspects juridiques ». Les auteurs sont Thierry Autret d'Ernst & Young, Laurent Bellefin de Solucom et Marie-Laure Oble-Laffaire du cabinet d'avocats HSD Ernst & Young.

Nous ne traiterons pas dans cet article des aspects propres à la cryptographie et nous n'introduirons que les bases élémentaires pour comprendre le développement de l'article.

Préambule

Un premier article, paru dans la lettre n°42, décrivait comment « Sécurité(s) et Sûreté(s) » participent à la qualité des données, des programmes et des systèmes tout au long du cycle de vie du logiciel.

Après un rappel des concepts et de la terminologie en sûreté de fonctionnement dont la sécurité informatique et la sûreté-innocuité font partie, cet article ouvrait une première réflexion adélienne en la matière. C'était une mise en appétit, riche de termes consacrés et de sigles afin de lancer des appels aux adhérents pour les inviter à : rédiger des articles, proposer des thèmes de réflexions, etc.

Un deuxième article, paru dans la lettre n°44, abordait très précisément la problématique « Sécurité(s) et Intimité… des données à caractère personnel ».

Il replaçait ce sujet dans le cadre générique de la sûreté de fonctionnement, puis dans le contexte général de la sécurité informatique (disponibilité, intégrité, confidentialité et auditabilité) et y ajoutait une réflexion spécifique relative au respect de la vie privée et à la garantie d'intimité électronique, si tant est que cela puisse se résumer ainsi.

Ce nouvel article propose une déclinaison de la propriété d'auditabilité des systèmes d'information par le biais des technologies de signature électronique (originellement appelée signature numérique) à laquelle est désormais attribuée la valeur juridique de force probante depuis l'adaptation, puis son adoption en loi française, de la directive européenne sur la signature électronique.

Une tendance actuelle de la sécurité des systèmes d'information et de communication, notamment dans des domaines d'une sensibilité toute particulière comme ceux de la santé, du social, du bancaire et de la communication électronique en général, consiste à prendre en compte au plus tôt du cycle de

vie du système un autre axe de besoins et d'exigence, pour construire la confiance dans le système.

Cet axe de besoins ou d'exigence correspond à ce que l'on appelait non-répudiation (des échanges), ou encore « contrôle et preuve » : il s'agit de *l'auditabilité* du système. L'auditabilité du système d'information, tant lors de son élaboration, sa construction, sa validation ou son utilisation, consiste à faire en sorte que les décisions prises et les actions entreprises, pour élaborer, construire, valider ou utiliser, soient de confiance au sens de prouvables, tant techniquement que juridiquement.

Lorsqu'il n'y avait que le niveau technique de la preuve (numérique), l'auditabilité était restreinte à de la *traçabilité* (capacité à garder la trace des décisions prises et des actions entreprise), voire à de l'*imputabilité* (capacité à attribuer à un auteur une décision ou à un exécutant une action). En aucun cas il n'y avait certitude sur l'engagement de responsabilité concernant ces décisions et actions, ni donc sur la possible reconnaissance juridique de cette responsabilité.

Depuis que l'on dispose également d'un niveau juridique de la preuve (électronique), l'auditabilité peut être vue comme une propriété englobant l'*opposabilité* (possibilité de présenter une décision ou une action comme étant opposable à son auteur ou son exécutant devant un juge), et aussi l'*irréfutabilité* (possibilité de devenir irréfutable après la prise d'une décision de justice) : au terme *« irréfutable »*, un juriste préfèrerait très certainement le terme *« irréfragable »*.

Cet article présente un tout premier niveau de détail de ce qu'est une signature cryptographique en liaison avec cette progression que nous venons de décrire concernant la propriété d'auditabilité : progression depuis sa restriction (technique) à de la traçabilité et de l'imputabilité, jusqu'à son évolution (juridique) vers de l'opposabilité et de l'irréfutabilité ; d'où notre titre : *« Signature cryptographique : du numérique à l'électronique »*.

Introduction

La signature électronique est une application très concrète de la cryptographie asymétrique qui fut inventée dans le milieu des années 70. Elle va permettre à tout un chacun de signer un acte électronique avec une valeur juridique identique à celle que l'on accorde actuellement à la version papier de cet acte. Alors que beaucoup d'autres technologies cryptographiques sont utilisées à l'insu même de l'utilisateur, et pour sa plus grande satisfaction, comme le chiffrement pour la confidentialité ou le scellement pour garantir l'intégrité, la signature électronique doit garder une marque de la volonté de s'engager sur ce que l'on signe. A ce titre cet outil va prendre une place importante dans la vie quotidienne des responsables d'entreprises et à terme des citoyens.

« *La signature nécessaire à la perfection d'un acte juridique identifie celui qui l'appose.* » dit le législateur français dans 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. Pour le spécialiste de la sécurité ceci permet d'assurer la traçabilité des actes effectués et l'auditabilité des actions. Pour le spécialiste des questions relatives à la vie privée ceci peut également devenir une menace si la signature électronique est utilisée comme un moyen de surveillance des individus par pistage de leurs actions.

Mais ne mélangeons pas tout. La signature électronique n'a pas d'autre finalité que celle de la traditionnelle signature manuscrite, à savoir identifier le signataire d'un acte et manifester son consentement aux obligations qui découlent de cet acte. Le reste est l'application des techniques cryptographiques à d'autres besoins de sécurité.

Après un bref rappel de la cryptographie asymétrique nous citerons les différents mécanismes de sécurité auxquels elle peut s'appliquer. Ensuite nous expliquerons la différence qui existe entre la signature numérique et la signature électronique, puis nous introduirons le certificat de clé publique et décrirons brièvement les infrastructures qui permettent d'assurer la gestion des clés cryptographiques qui y sont liées.

De la cryptographie à la sécurité

La cryptographie, du grec *kruptos* (*κρυπτοσ*), caché, et *graphein* (*γραφειν*), écrire, est la science des

écritures secrètes. Les cryptographes, qui sont aujourd'hui des mathématiciens, étudient l'ensemble des techniques qui permettent de concevoir des systèmes cryptographiques, en même temps que les moyens de les casser dans le but d'en tester la résistance. La cryptographie est donc indissociable de la cryptanalyse. Les utilisateurs autorisés, c'est-à-dire ceux qui possèdent les secrets, font du chiffrement ou du déchiffrement, alors que les cryptanalystes, ou agresseurs (car ils ne possèdent pas les secrets ni les autorisations pour les détenir), font du décryptage afin de retrouver l'information en clair sans se servir des clés cryptographiques. La logique étymologique voudrait donc que l'on n'emploie jamais le terme de *« cryptage »*[1] et encore moins le néologisme angliciste de *« encryptage »* (mauvaise traduction du terme anglais *« encryption »*), ni même *« enchiffrer »* (très mauvaise traduction de *« to encipher »*).

Symétrique et asymétrique

La cryptographie utilise des données spécifiques qui sont appelées des clés et qui ne sont ni plus ni moins que des suites de caractères traités au niveau le plus élémentaire à savoir le bit. Ces clés sont utilisées dans des algorithmes qui sont des suites organisées d'opérations mathématiques, précisément définies, portant sur des données externes, comme le texte d'un message électronique.

Les systèmes cryptographiques symétriques sont sans doute les plus connus car ils ont été utilisés depuis la nuit des temps pour assurer la confidentialité des messages. La caractéristique principale d'un système symétrique est que l'émetteur et le récepteur utilisent la même valeur de clé. Cette classe d'algorithmes est également appelée « *systèmes à clé secrète partagée* ». Les systèmes bancaires utilisent largement ces techniques aujourd'hui.

Les systèmes asymétriques sont également appelés systèmes à clé publique parce qu'ils sont fondés sur l'existence de deux ensembles de valeurs distinctes : les valeurs qui sont conservées privées par leur propriétaire et celles qui sont rendues publiques. Pour ne pas créer de confusion avec les systèmes symétriques décrits ci-dessus où l'on parle de clé secrète, ici les valeurs qui ne doivent pas être divulguées sont appelées les clés privées.

Application à la sécurité

Les techniques cryptographiques symétriques s'appliquent aux différents besoins de sécurité pour les échanges de données informatisées :

- L'authentification : par challenge cryptographique (défi-réponse), c'est à dire transformation, avec l'aide d'une valeur secrète, d'une valeur (le défi) pour donner une valeur attendue par le vérificateur (la réponse).
- L'intégrité : par calcul d'une empreinte numérique du texte à protéger avec un algorithme résistant aux collisions (risque que deux textes différents donnent la même empreinte).
- La confidentialité : par transformation cryptographique, avec l'aide d'une clé secrète, du texte à protéger.
- La non-répudiation : par calcul d'une valeur propre à l'acteur qui a fait telle ou telle action.

Signature et non-répudiation

Les trois premiers services de sécurité énoncés ci-dessus peuvent être réalisés à l'aide de mécanismes cryptographiques symétriques ou asymétriques. Nous n'entrerons pas dans les détails qui font que tel ou tel algorithme est plus approprié qu'un autre pour chacun des services, mais nous dirons que les techniques asymétriques trouvent une pleine application de leurs propriétés intrinsèques pour garantir la non répudiation.

Le service de non-répudiation est complexe à présenter. En une approche volontairement simple mais peu rigoriste, nous dirons qu'il s'agit d'apporter à l'un des participants d'un échange des protections dans le cas où l'autre participant viendrait à soulever un litige quant à l'aboutissement de la transaction. Par exemple, un client nie avoir commandé des marchandises car il a changé d'avis, ou un

---

[1] *« cryptage »* est un terme en lui seul contradictoire puisqu'il signifierait : *"protéger cryptographiquement (i.e. donc avec l'aide d'une clé cryptographique) sans l'aide d'une quelconque clé cryptographique"*, par analogie avec *« décryptage »* dont le sens est bien *: "déprotéger cryptographiquement par des techniques d'attaques en cryptanalyse, c'est-à-dire sans l'aide d'une quelconque clé cryptographique"*.

commerçant nie avoir reçu un paiement pour tenter de se faire payer deux fois. Notons au demeurant que la non-répudiation n'est pas un service juridique car tout acte est *"contestable"* devant une cour de justice, au sens où il n'est pas juridiquement recevable, ni donc opposable à son auteur, bien que techniquement fidèle à la réalité et techniquement authentique (i.e., non-répudiable).

En signant numériquement un message avec sa clé privée, le signataire prouve qu'il a participé à ce message et ne peut pas le nier *a posteriori*.

De la signature numérique à la signature électronique

Signature numérique

Le principe des systèmes asymétriques est fondé sur la complexité de résolution de certains problèmes mathématiques. Les problèmes complexes auxquels nous faisons référence sont la factorisation d'un nombre entier formé de grands facteurs premiers (RSA, RW), la résolution d'un logarithme discret sur un corps fini (DH, El Gamal, DSA), ou encore la résolution d'un logarithme discret sur une courbe elliptique (ECDSA). Le principe général de tous ces systèmes est que chaque partenaire souhaitant communiquer dispose d'un couple de clés complémentaires, nommées respectivement la clé publique et la clé privée. Les deux éléments du couple sont liés par des caractéristiques mathématiques très précises qui rendent les deux clés complémentaires, et l'ensemble unique pour un partenaire donné.

La particularité principale des systèmes asymétriques est leur capacité à réaliser le mécanisme de signature numérique. La signature est réalisée en utilisant la clé privée du signataire, tous ses partenaires pouvant alors vérifier sa signature en utilisant sa clé publique. Dans tous les protocoles opérationnels, c'est en fait une empreinte numérique, et non pas l'ensemble du document, qui est signée, ce pour des raisons de performance, les algorithmes asymétriques étant très consommateurs de ressources.

Jusqu'ici, nous n'avons évoqué que la signature numérique, mais les débats autour d'Internet et du commerce électronique évoquent plutôt la notion de signature électronique. Est-ce la même chose ?

Pour bien comprendre la nuance entre les deux notions, il convient de rappeler quelques définitions. Voici, selon la norme ISO 7498-2 relative à l'architecture de sécurité pour les systèmes ouverts, la définition de la signature numérique : « *Données ajoutées à une unité de données, ou transformation cryptographique d'une unité de données, permettant à un destinataire de prouver la source et l'intégrité de l'unité de données et protégeant contre la contrefaçon par le destinataire par exemple »*

Signature électronique

Le 16 avril 1997, la Commission européenne a présenté au Parlement européen, au Conseil, au Comité économique et social et au Comité des Régions une communication sur une initiative européenne dans le domaine du commerce électronique. Dans ce texte, tout en mentionnant très clairement le mécanisme de signature numérique qui s'appuie sur la cryptographie asymétrique, le rédacteur fait référence en une seule occasion à la signature électronique en relevant : « *Propre à chaque expéditeur et à chaque message envoyé, la signature électronique est vérifiable et doit être honorée ».* C'est en fait cette appellation qui sera reprise, le 13 décembre 1999, par le Parlement européen et le Conseil de l'union européenne qui fait paraître la directive 1999/93/CE sur un cadre communautaire pour les signatures électroniques.

Cette directive ne mentionne plus que la notion de signature électronique qui est définie comme : « *Une donnée sous forme électronique qui est jointe ou liée logiquement à d'autres données électroniques et qui sert de méthode d'authentification.* »

Cette définition ne vise qu'à remplir les besoins de l'authentification et, à ce titre, plusieurs technologies pourraient la satisfaire. Il s'agit de l'authentification reposant sur le principe du partage de secret, du calcul d'une donnée biométrique ou encore de la signature numérique. Le texte de cette directive européenne, qui se devait d'être neutre d'un point de vue technologique, ne parle donc pas directement de signature numérique ni même de cryptographie asymétrique, mais il mentionne néanmoins les notions de certificat et de données qu'un tel certificat doit contenir : on parle alors de certificat de clé publique.

Mais le texte introduit en outre la notion de signature électronique « *avancée* » (ou signature électronique *« sécurisée »*, dans la transposition française), qui doit satisfaire 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 et

d) être liée aux données auxquelles elle se rapporte de telle sorte que toute modification ultérieure des données soit détectable.

Pour répondre à ces besoins, qui sont ceux de la non-répudiation, les seules techniques qui puissent être aujourd'hui mises en œuvre sont celles de la signature numérique utilisant la cryptographie asymétrique et les certificats de clé publique.

En résumé, nous pouvons conclure en disant que la signature numérique est une technique informatique alors que la signature électronique est une solution technico-organisationnelle qui répond à un besoin juridique.

Le certificat de clé publique

Pour pouvoir utiliser une clé publique avec sécurité, il faut donc que le récepteur puisse répondre au moins aux deux questions suivantes : « *à qui appartient cette clé publique ?* » et « *à quoi sert cette clé publique ?* ».

Pour cela, il faut que la clé publique soit accompagnée d'informations descriptives de son propriétaire et de son usage. Cela pourrait alors ressembler à une carte de visite électronique du propriétaire de la clé, sur laquelle le récepteur trouverait le nom, la valeur de la clé publique et son usage.

Mais, de plus, il faut que cette carte de visite soit rendue infalsifiable, sinon une personne malveillante pourrait constituer une fausse carte de visite électronique. En fait, un certificat ressemble en bien des points à une pièce d'identité, carte d'identité ou passeport, dont il constitue une sorte d'équivalent électronique. Dans le monde électronique cette pièce d'identité électronique s'appelle un « certificat de clé publique », plus simplement appelé « certificat ». Un certificat est délivrée par une Autorité de Certification (AC).

Le format de certificats aujourd'hui le plus utilisé est le format normalisé par le standard X.509 dans sa version 3. Ce dernier permet l'utilisation des protocoles normalisés ou des applications telles que SSL, IPSec, S/MIME ou SET.

Un certificat X.509 v3 contient les données suivantes :

Version du certificat (*certificate format version*)
Numéro de série du certificat (*certificate serial number*)
Description de l'algorithme de signature de l'AC (*signature algorithm identifier for CA*)
Nom de l'AC qui a généré le certificat (*issuer X.500 name*)
Période de validité (*validity period*)
Nom de l'utilisateur auquel appartient le certificat (*subject X.500 name*)
Clé publique (*subject public key*)
Description de l'algorithme à utiliser avec la clé publique (*subject public key information*)
Identification possible de l'AC (optionnel) (*issuer unique identifier*)
Identification possible de l'utilisateur (optionnel) (*subject unique identifier*)
Extensions (optionnel)
Signature de l'AC (*CA signature*)

Infrastructure à clé publique

Comme son nom l'indique, une infrastructure à clé publique (ICP) , ou *"Public Key Infrastructure"*

(PKI) en anglais, est un ensemble de moyens matériels, de logiciels, de composants cryptographiques, mis en œuvre par des personnes, combinés par des politiques, des pratiques et des procédures requises, qui permettent de créer, gérer, conserver, distribuer et révoquer des certificats basés sur la cryptographie asymétrique.

Cette définition empruntée à l'IETF (normalisation de l'Internet) montre qu'une ICP est bien plus qu'un système technique. Les politiques, pratiques et procédures décrivent le cadre de mise en œuvre des moyens dédiés à l'ICP de façon sûre, et qui correspondent à l'attente, en termes de confiance, de ses utilisateurs.

Le guide de l'IETF, *PKI Roadmap*, et certains documents du NIST américain, présentent une ICP comme un ensemble constitué des cinq types de composants suivants :

- Les autorités de certification (AC) qui émettent et révoquent les certificats.
- Les autorités d'enregistrement (AE) organisationnelles qui se portent garantes du lien entre une clé publique, l'identité du porteur du certificat et d'autres attributs.
- Les porteurs de certificats auxquels sont attribués des certificats et qui peuvent signer et/ou déchiffrer des documents.
- Les utilisateurs qui vérifient les signatures numériques ou chiffrent des données, et valident les chemins de certification des certificats à partir d'une AC digne de confiance.
- Le service de publication, qui comprend les répertoires qui contiennent et rendent disponibles les certificats de clés publiques et les listes de certificats révoqués.

Conclusions

Après les deux articles publiés dans les Lettres d'ADELI n°42 et n°44, cet article est le troisième maillon proposé dans le cadre de notre réflexion adélienne sur la sécurité des systèmes d'information et de communication.

Ce n'est qu'un premier pas vers une meilleure compréhension de l'actualité florissante autour des concepts d'IGC (PKI) et autres notions liées à la signature numérique, désormais devenue signature électronique. Il contribue à la réflexion adélienne dans son ensemble.

D'autres pas de compréhension et de réflexion autour de la signature électronique seront proposés à l'avenir ; ils feront partie de la vie de la commission « Sécurité(s) et Sûreté(s) » pour laquelle les contributions, avis et retours d'expériences et autres interventions des adhérents de l'ADELI sont comme toujours souhaitables et souhaités.

Avis : par courriel : *thierry_autret@ernst-young.fr* *gilles_trouessin@ernst-young.fr*
par la toile : *www.ey.com* *www.adeli.com*
par téléphone : +33 (0) 1 4693.8266 +33 (0) 6 8255.7406
par télécopie : +33 (0) 1 5847.4318 +33 (0) 1 5847.1033
par courrier : Ernst & Young Audit (France) – Tour Egée – 92037 PARIS La Défense Cedex

Thierry Autret
Directeur au sein de Ernst & Young Audit

Gilles Trouessin
Directeur de Mission au sein de Ernst & Young Audit
Vice-président d'ADELI "en charge de l'innovation"
Responsable de la commission "Sécurité(s) & Sûreté(s)"

Quelques noms d'algorithmes de signature :

RSA (Rivest – Shamir – Adleman) :	algorithme cryptographique asymétrique, du nom de ses auteurs.
RW (Rabin – Williams) :	algorithme cryptographique asymétrique, du nom de ses auteurs.
DH (Diffie – Hellman) :	algorithme à l'origine de la cryptographie asymétrique, du nom de ses auteurs.
El Gamal :	algorithme de signature à base de logarithmes discrets, du nom de son auteur.
DSA (Digital Signature Algorithm) :	nom d'un algorithme mondial standardisé de signature numérique.
ECDSA (Elliptic Curve DSA) :	version du DSA reposant sur les courbes elliptiques.