Certification et archivage légal de dossiers numériques

Maxime Wack, Nathanael Cottin, Bernard Mignot, Abdellah ElMoudni

Laboratoire Systèmes et Transports
Université de Technologie de Belfort-Montbéliard
90010 BELFORT Cedex
{Maxime.Wack, Nathanael.Cottin, Bernard.Mignot, Abdellah.Elmoudni}@utbm.fr

RÉSUMÉ. *La certification et l'archivage légal des données, alliée à la signature électronique des documents, ouvrent de nouvelles perspectives à la sécurisation des documents. Ainsi, ces technologies offrent des capacités : d'identification, d'authentification, de certification qui concourent à la capacité globale d'archivage sécurisé des dossiers numériques.*
Cependant, il apparaît que la certification et la signature électronique ne répondent pas complètement aux besoins des entreprises en ce qui concerne l'authentification et le stockage des données sécurisées. Dans la suite de cet article, nous proposons une solution à ces problèmes.
ABSTRACT. *The certification and legal data storage, bound to data electronic signature open new perspectives to data security. Like this, these technologies offer capabilities such as : identification, authentification, certification, aiming to the global capacity of secured data storage.*
However, it appears that certification and electronic signature does not completely answer to enterprise needs concerning authentification and secured data storage. The purpose of this paper is a solution proposal to these problems.

MOTS-CLÉS : *document, légal, archivage, sécurité, certification, autorités, signature, cryptage, clés.*

KEYWORDS: *document, legal, storage, security, certification, authorities, cryptography, keys.*

Document numérique. Volume 6– n° 1-2/2001, pages 145 à 158

1. Introduction

Depuis la loi n°2000-230 du 13 mars 2000 relative à la signature électronique (JO du 14 mars 2000, p.3968), le support d'archivage de la preuve n'est plus obligatoirement un support papier mais aussi un support électronique. Ce support répond aux caractères de fidélité et de pérennité énoncés par le Code civil ainsi qu'aux exigences futures d'intégrité et d'imputabilité de la preuve. C'est pourquoi, sensibilisés au problème de la conservation des documents et à sa rentabilité économique, les professionnels pourront dorénavant avoir recours à d'autres méthodes telles que l'archivage électronique des documents (AED).

Le remplacement des supports physiques traditionnels ou la prise en compte de documents d'origine électronique dans une solution de Gestion Electronique des Documents (GED) implique, notamment lorsque les projets ont pour vocation un archivage légal, le respect de certaines recommandations telles que celles contenues dans le *guide de l'archivage électronique* et la norme *Afnor NF Z42-013*.

Notre contribution est donc de proposer un environnement informatique réalisant quatre fonctions : une certification de la transaction électronique par l'intermédiaire d'un tiers certificateur, l'archivage sécurisé par l'intermédiaire d'un tiers archiveur, un moyen de recherche d'information et la traçabilité des différentes transactions.

2. Architecture du système d'archivage et de certification

Nous avons étudié une architecture basée sur le principe d'autorités de tiers de confiance (Figure 1) où chaque autorité joue un rôle clé pour authentifier les données et certifier les documents et les entités (individuels, entreprises, serveurs ou programmes). Le point de départ de cette architecture est la CA (Autorité de Certification) qui délivre les certificats électroniques. Il est fondamental que la fourniture des certificats assure que tout certificat est donné à la bonne personne et que l'information incluse est valide et vérifiée.

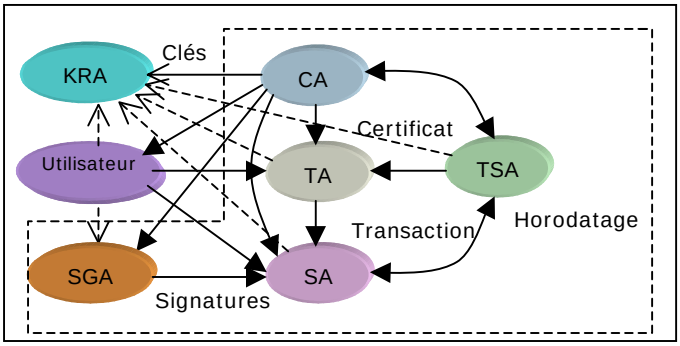

Figure 1. *Schéma général de l'architecture*

Supposant que les certificats sont délivrés sans aucune corruption ou fraude possible, l'architecture est articulée autour de cinq autres autorités toutes tiers de confiance (TTPs) : Autorités d'Horodatage (TSAs), Autorités de Signature (SGAs), Autorité de Recouvrement de clés (KRAs), Autorités de Stockage (SAs), et Autorités de Transactions (TAs).

2.1. *Autorité d'horodatage*

Une autorité d'horodatage (TSA) attribue un valeur de temps légale à un message donné. Ainsi, la signature n'a pas de valeur légale si elle n'est pas horodatée parce qu'il n'y a pas de moyen de contrôler si la signature a été créée pendant que le certificat du signataire était valide (non révoqué ou expiré). Il est également utilisé pour authentifier un document et répudier une copie frauduleuse de celui-ci, dans le cas où le document original a été signé avant la copie.

Nous pouvons donc définir une extension à la structure de la signature numérique présentée par (Housley, 1999) et exprimée avec la notation ASN.1 (Dubuisson, 2000), comme une signature légale incluant une marque de datage basé sur le protocole d'horodatage.

Dans cette structure, la signature est composée de la signature elle-même et du certificat d'identification du signataire (composé du numéro de série du certificat et du nom du fournisseur) (Housley, 1999) (Myers, 2001). Cet identifiant est utilisé pour donner l'information du certificat pour le CA correspondant et être sûr que l'information de la signature corresponde à la donnée signée.

De plus, la signature légale représente une signature générée sur toute donnée (un message) donné par une partie tiers (un SA ou TA par exemple). Cette signature est complétée avec une marque d'horodatage et peut être contresignée par les autorités d'accréditation d'horodatage, ou accréditeurs. Ceci assure que la marque d'horodatage proposée est valide sur tout procédé d'horodatage (ETSI, 2001).

2.2. *Autorité de signature*

L'autorité de signature (SGA) résout le problème de la multi-signature sur un document donné. En effet, les SGAs interviennent comme des notaires électroniques qui supervisent le processus de signature en collectant les différentes signatures. Considérant que tout signataire doit avoir la confiance des autres signataires, le SGA aura la permission de stocker (et coder) le document (ETSI, 2000).

Un document d'entreprise peut être un ensemble et doit être signé par plus d'une personne (contrats, factures par exemple). Comme il peut avoir plusieurs propriétaires, les protocoles de signature du document, consultation et destruction doivent être définis.

Le principal objectif à réaliser est de permettre aux multiples signataires de signer la donnée sur Internet. Nous proposons un protocole pour traiter cet aspect. Ce protocole est basé sur les définitions signed-and-enveloped-data pkcs#7. L'idée de base en est que les autorités de signature supervisent et gèrent les processus de signature multiples (Cottin, 2001).

2.3. *Autorité de recouvrement des clés*

L'autorité de recouvrement des clés (KRA), également connue sous le nom de Key Escrow ou Trust Center, est requise par les institutions gouvernementales de telle sorte qu'elles puissent avoir accès aux données cryptées. Avec la législation de la cryptographie, les clés asymétriques peuvent être de 2048 bits ou plus, et il est ainsi pratiquement impossible de décoder la donnée dans un temps acceptable.

Pour ce faire, les gouvernements souhaitent être capables de décoder toutes les données publiques pour être sûr que des documents secrets ne quittent pas leur territoire, et que des documents non autorisés ne circulent pas à l'intérieur de leur pays.

Les utilisateurs et institutions ont donc à fournir une copie de leurs clé de cryptage/décryptage aux autorités de recouvrement des clés. Celles ci ne peuvent les rendre disponibles que sur la requête des seuls gouvernements.

3. Processus de certification

Le transfert de message en général et à travers Internet en particulier reste non sécurisé. Les communications peuvent être sécurisées par des protocoles de cryptage tels que SSL (Freier, 1996) et PPP (Kaeo, 1999) (ETSI, 2000). Il vaut souvent mieux identifier incontestablement l'émetteur et le récepteur du message, plutôt que d'établir l'authenticité du matériel ou des applications (navigateurs web par exemple). Ainsi, le récepteur d'un message possède la preuve concrète de l'identité de l'émetteur. Cependant, il reste deux risques : d'une part qu'une personne intermédiaire (MITM) se fasse passer pour l'émetteur du message (Kaeo, 1999), ou d'autre part que le récepteur ne puisse plus prouver que le message reçu est le message que l'émetteur a tenté de lui communiquer. L'utilisation de la signature numérique et des certificats électroniques permettent de résoudre ces deux problèmes.

3.1. *Signature numérique et bases de la signature du message*

La signature numérique est le moyen courant d'authentification d'une donnée électronique. C'est le résultat de nombreuses recherches sur la cryptographie des clés asymétriques et le code de hachage.

3.1.1. *Concepts de cryptographie des clés asymétriques*

Quand une entité émettrice (une personne, un serveur ou un programme) doivent envoyer un message sécurisé à une entité réceptrice, elle crypte le message en utilisant la clé publique du récepteur. Cette clé est diffusée de telle sorte que tout émetteur puisse utiliser la clé publique du récepteur pour crypter la donnée. Le message crypté est ainsi illisible et ne peut être décrypté sans la clé privée correspondante. La clé privée doit être conservée de manière sécurisée par le récepteur, qui ne doit pas la publier. Seul le récepteur doit être capable de décrypter le message codé. Le cryptage de la clé asymétrique assure le caractère privé et la confidentialité.

Les algorithmes de clé asymétriques les plus largement utilisés sont RSA (RSA, 1993) et triple-DES (NIST, 1999).

3.1.2. *Le code de hachage*

Le code de hachage (Menezes, 2001) a pour but la création d'un message de longueur fixe pour tout ensemble de données de taille variable. Ce code est indépendant de la taille des données sources. Considérons h(), une fonction de hachage à sens unique utilisée pour calculer un code sur un ensemble de données s. La plus importante propriété de cette fonction est de permettre la reconstruction de l'ensemble de données seulement si le code calculé est connu. Bien que la reconstruction des données d'origine s à partir d'un code donné d soit être théoriquement possible, elle apparaît comme informatiquement infaisable :

$(h(s)=d) \Rightarrow (p(h^{-1}(d) = s) \rightarrow 0)$

De plus, la probabilité p que deux différents ensembles de données s1 et s2 obtiennent le même code avec un algorithme de hachage donné ha tend vers 0. La fonction de hachage est ainsi dite résistante aux collisions :

$(s1 \neq 2) \Rightarrow (p(h(s1,ha) = h(s2,ha)) \rightarrow 0$

De nombreux algorithmes de codage tels que MD2 (Kaliski, 1992), MD4 (Rivest, 1992) et RIPEMD (Dobbertin, 1996) (Preneel, 1997) ont été développés. Les algorithmes très répandus SHA-1 (NIST, 1995) et MD5 (Rivest, 1992) sont spécifiquement conçus pour le calcul des signatures numériques.

3.1.3. *Signature numérique*

Les signatures numériques définies par (NIST, 2000) reproduisent les sceaux de cire utilisés dans l'antiquité pour cacheter les lettres.

Le sceau peut être comparé à une clé de signature secrète qui ne doit être en possession que du signataire, c'est à dire l'entité qui signe le message. Bien que le sceau reste indépendant de l'information de la lettre, la signature numérique est dépendante du message. Cette manière d'appliquer une clé de signature (la clé privée du signataire) à deux différents messages va résulter en deux signatures numériques différentes. Au contraire, le même message va toujours générer la même signature dans le cas où un algorithme de signature donné est utilisé. Cependant, la clé de vérification (la clé publique) unique correspondant au signataire doit être utilisée pour être certain que la signature a été générée en utilisant sa clé de signature.

La génération des signatures numériques est la simple application du cryptage par clé asymétrique sur les données des codes de hachage. Contrairement au cryptage de données, le but de la signature numérique n'est pas de consister en la confidentialité des données, mais plutôt d'assurer (Kaeo, 1999) :

- l'intégrité des données : les signatures numériques permettent de détecter les sources de modification des données, c'est à dire les modifications non autorisées des données

- l'authentification : comme la clé de signature est (théoriquement) détenue seulement par le signataire, il est impossible à toute autre personne de générer la signature de l'émetteur sur un ensemble de données. La donnée est authentifiée en comparant la signature avec la clé de vérification correspondante du signataire.

- la non-répudiation : ce service basé sur l'authentification est une preuve effective de la transaction. L'entité de la signature ne peut nier l'auteur de la signature parce que personne d'autre n'a pu créer une telle signature sur un ensemble de données particulières.

La signature numérique est généralement calculée sur les codes de hachage plutôt que directement sur les données. La principale raison est que la signature numériques est plus consommatrice en temps et processeur que le processus de hachage. Il est ainsi préférable d'appliquer seulement les algorithmes de génération de signature (DSA (NIST, 2000) et ECDSA (ANSI, 1999) par exemple) sur les codes de hachage.

Bien que la signature numérique rende possible d'authentifier la donnée reçue, elle n'identifie pas l'entité qui a signé la donnée (le signataire), du point de vue du récepteur. Ainsi, aucun lien irréfutable n'existe entre le signataire et sa clé de signature. Une telle identification est permise par le certificat électronique.

3.2. *Certificat électronique (qualifié)*

Un certificat électronique qualifié (certificat) est une preuve électronique d'identité (Figure 2). Il est destiné à permettre l'identification de l'émetteur par les récepteurs des message signés. La confiance dans les certificats dépend de la confiance de leurs fournisseurs. Seules les autorités de certification (CAs) sont considérées comme TTPs dans les PKIs qui se basent sur la standard X.509 (Mel, 2001). Les autres entités ne sont pas accréditées par les gouvernements à délivrer les certificats électroniques. Une fois une adéquation entre une entité et une clé de signature démontrée, un certificat qualifié est délivré.

Figure 2. Description d'un certificat

Chaque certificat est identifié par son numéro de série unique donné par l'autorité de certification (CA). En effet, la règle primaire des certificats électronique est d'associer une clé de vérification de signature et un signataire. En fonction des règles sur la clé de signature, ils peuvent être utilisés pour :

- sécuriser les emails : les certificats peuvent être intégrés à l'intérieur de standards d'emails sécurisés tels que PGP (Garfinkel, 1994) (Callas, 1998) (Elkins, 2001), PEM (Balenson, 1993) (Kent, 1993) (Linn, 1993), et S/MIME (Ramsdel, 1999)

- signer du code : les Archives Java (Sun, 2001) (Farley, 1998) et Authenticode Microsoft (Garfinkel, 1997) réalisent la plupart des certifications de code

- identifier les parties : au cours des transactions Internet, les entités terminales doivent être identifiées en décodant leurs signatures numériques avec leur clé de vérification. Cette clé est incluse dans leurs certificats

Les certificats sont valides jusqu'à ce qu'ils soient révoqués ou jusqu'à leur expiration (Figure 3). Dans les deux cas, un nouveau certificat doit être ré-émis par le CA. Une révocation de certificat intervient quand son propriétaire est informé que son certificat est corrompu, ou qu'une entité non autorisée ait pu l'utiliser. Il est aussi possible pour un gouvernement ou le CA de révoquer un certificat dans le cas où son propriétaire en a fait une utilisation frauduleuse.

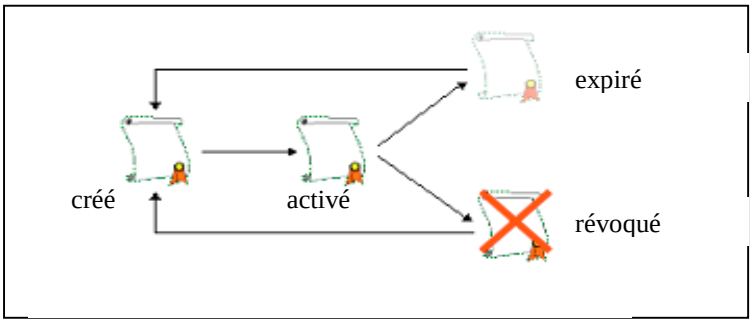

Figure 3. Cycle de vie d'un certificat

Les objectifs principaux des certificats et signatures numériques sont l'authentification des données. Ceci conduit à définir une autorité de confiance responsable du stockage sécurisé des données, considérant qu'une telle TTP doit conserver les données d'entreprises de manière sécurisée et légale.

4. Stockage de données sécurisées et conservation

Selon la loi, les documents électroniques n'ont aucune valeur légale tant qu'ils n'ont pas été signés numériquement (Figure 4), et leurs signataires été identifiés.

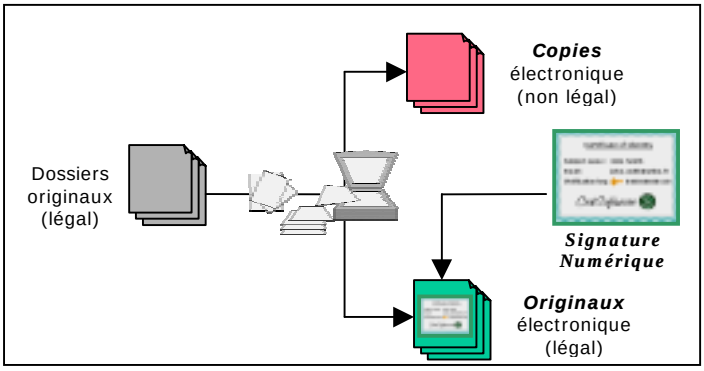

Figure 4. Utilisation de la signature numérique

Les deux caractéristiques techniques en jeu ici sont d'une part de donner aux copies électronique des documents une valeur similaire au document initial, et d'autre part de stocker et conserver de manière sécurisée ces dossiers numériques légaux. La signature numérique et les certificats électroniques combinés ensemble répondent à la première partie en permettant respectivement l'authentification de la donnée et l'identification des signataires. Cependant, le stockage des dossiers signés dans un contexte légal n'a pas encore été considéré.

4.1. *Présentation des autorités de stockage*

Une autorité de stockage (SA) est une TTP qui répond aux besoins de stockage des documents d'entreprise. Ces besoins peuvent être classés comme suit :

- Intégrité des données : ce service est fourni par un stockage sécurisé combiné avec une signature numérique qui indique si un document donné a été modifié ou non. Le document original (celui stocké en premier) doit être conservé par le SA pour être sûr que les institutions gouvernementales autorisées ont accès à la première version de chaque document conservé.

- Confidentialité : le cryptage peut être utilisé par les SAs pour être sûr que la donnée ne soit pas lisible tant qu'elle n'est pas explicitement décryptée. Cette protection logicielle peut être complétée par une protection matérielle telle que les architectures 3-tiers (Brethes, 2000).

- Privilège d'accès : il est réalisé par le contrôle d'accès aux documents conservés. Les entités autorisées sont uniquement les représentants des gouvernements et les signataires.

- Disponibilité des documents : comparé au stockage traditionnel de données, le délai d'accès aux documents est moins important que la disponibilité et l'authentification des documents. C'est le SA qui assure la disponibilité des documents conservés pour les entités autorisées. La tracabilité d'utilisation des documents est également de son ressort.

- Pérennité des documents : les SAs assurent la préservation des documents. Ces documents devant être archivés et lisibles tout au long de leur vie.

- Traçabilité : De manière similaire aux CAs, ces autorités doivent établir des traces de toutes les transactions (incluant le stockage des documents, consultation, destruction, modification). Le tracabilité débouche sur la détection de fraude et le diagnostic.

4.2. *Architecture de l'autorité de stockage*

La SA est fondamentalement composée de une ou plusieurs bases de données sécurisées (Figure 5) utilisées pour conserver les documents signées et d'autres informations relatives qui apportent le caractère légal au stockage.

Nous avons défini une structure générale de donnée pour les documents pour être intégrée dans la classe de base pkcs#7 (« just data », sans codage cryptographique) et conservées par les SAs.

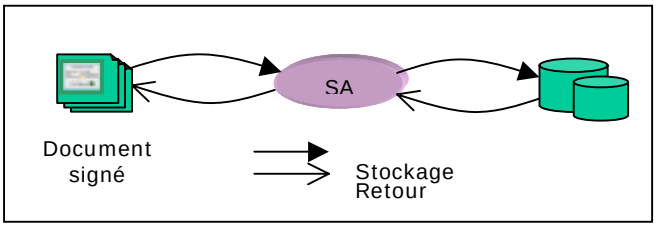

Figure 5. Architecture de l'autorité de stockage

5. Le secret partagé

5.1. *Introduction*

L'évolution de la législation et l'apparition de la notion de tiers archiveur ont fait évoluer la notion de stockage de données, passant d'un simple service assurant la fiabilité des données à un concept plus global, incluant l'assurance de la confidentialité.

Si les mécanismes de réplication des données sécurisant le stockage sont désormais bien connus (RAIDs), leur équivalent distribué en terme de confidentialité reste encore à mettre en œuvre de manière industrielle.

Le concept initial est de découper l'information à stocker en morceaux, et de trouver ensuite un mécanisme qui garantisse l'intégrité et la confidentialité des données.

Après avoir mené recherches et réflexions pour trouver un modèle satisfaisant à ces critères, le mécanisme dit de secret partagé introduit par Adi Shamir en 1979 nous est apparu pouvoir répondre à ces exigences.

5.2. *Objectifs et contraintes*

La performance et la tolérance aux pannes de systèmes de stockage des données peut être améliorée si les emplacements de stockage sont physiquement distribués. C'est le principe des systèmes de réplication de données de type RAID notamment, le RAID 5 en particulier.

Pourtant, la nature même d'un système distribué en rend la sécurisation d'autant plus difficile que le nombre d'emplacements de stockage est grand.

Dans un système centralisé, une approche radicale de la sécurité consisterait à garder les disques de données de longue conservation dans un emplacement

physiquement sûr (coffres, places fortes). Dans un système distribué, il faut s'assurer de l'intégrité de chacune des composantes.

Une difficulté apparaît quant à la garantie de disponibilité de ces systèmes distribués. En effet, plus il y a de composants indépendamment faillibles, moins il y a de chance que l'ensemble du système soit opérationnel à un moment donné. On résout ce problème en rendant ces systèmes tolérants aux pannes, c'est à dire qu'ils sont capables de fonctionner correctement même en présence d'un certain nombre de pannes de leurs sous-composants.

La disponibilité de données de longue conservation peut être ainsi améliorée en stockant ces données de manière redondante. Cette technique est communément appelée réplication.

Des techniques récentes permettent d'adapter ces mécanismes de réplication des données à des besoins de sécurisation.

On peut affiner la notion de sécurité en deux propriétés distinctes :

- La confidentialité : il s'agit de s'assurer que des personnes mal intentionnées ne peuvent pas lire des données secrètes.

- L'intégrité : il s'agit là d'empêcher la modification de ces données.

5.3. *Le principe de secret partagé*

Le principe de secret partagé a été développé en réponse au risque de consultation d'informations par des personnes non autorisées. Ce risque peut être réduit en exigeant la coopération de plusieurs personnes pour accéder aux données. Cela peut être accompli par un algorithme semblable à l'utilisation d'une serrure pour laquelle plusieurs clefs seraient nécessaires. Dans la version algorithmique de cette serrure à plusieurs clefs, il est possible de ne pas permettre l'accès aux données si le nombre de personnes requises n'est pas atteint, mais par contre permettre un accès total dès que ce quorum est obtenu.

Les données peuvent être distribuées sur N serveurs et divisées de telle manière que l'obtention des données nécessite l'accès à M sites (M <= N). Toute l'information devient disponible avec M sites, tandis que l'accès à M-1 sites ne délivre rien. L'obligation d'accès à plusieurs sites de stockage (à opposer avec un serveur central unique) peut permettre d'éviter tout accès abusif d'un individu isolé.

Deux schémas de secret partagé ont été découvert indépendamment par Blakley (Blakley, 1979) et Adi Shamir (Shamir, 1979). Leurs motivations étaient la recherche d'un mécanisme de partage de clefs. Cependant, l'ensemble des implémentations que nous avons trouvées utilisent le modèle de Shamir, et c'est celui que nous préconisons.

6. Conclusion

Dans cet article nous avons présenté une architecture basée sur des autorités que nous avons partiellement implémentée. Cette architecture tend à répondre aux besoins des entreprises et particuliers en termes d'identification de l'émetteur du message et d'authentification de la donnée reçue. Sa modularité réside dans la distinction entre les multiples tiers de confiance définis par les services qu'ils fournissent. Elle est particulièrement conçue pour intégrer facilement de nouveaux protocoles et prévoir l'extensibilité. Nous avons partiellement implémenté un prototype basé sur l'architecture proposée. Ce prototype inclus actuellement une autorité de certification, qui délivre des certificats X.509.v3 (Housley, 1999), une autorité de stockage, une autorité d'horodatage, et une autorité d'accréditation d'horodatage, qui sont tous conformes aux structures de données et protocoles proposés.

Nous travaillons actuellement sur la modélisation et la simulation des protocoles de certifications (SCDPs), les protocoles de multi-signature (MSPs), ainsi qu'à la définition des paramètres de la Qualité de Service (QoS), basée sur nos recherches antérieures (Cottin, 2000). Dans l'état actuel de nos recherches, il apparaît que de nouveaux concepts tels que l'autorisation de délégation de certificats et la protection de données intrinsèque sont nécessaires pour anticiper les futurs besoins des utilisateurs.

7. Bibliographie

ANSI - American National Standards Institute, "Public Key Cryptography for the Financial Services Industry: The Elliptic Curve Digital Signature Algorithm", Janvier 1999

Balenson D., "RFC 1423: Privacy Enhancement for Internet Electronic Mail: Part III: Algorithms, Modes, and Identifiers", TIS, IAB IRTF PSRG, IETF PEM WG, Février 1993

Blakley G.R., "Safeguarding cryptographic keys", AFIPS Conference Proceedings, 48, pp 313-317, 1979

Brethes, T., Hisquin F., Pezziardi P., *"Serveurs d'applications"*, Eyrolles, 2000

Callas J., Donnerhacke L., Finney H., Thayer R., "RFC 2440: OpenPGP Message Format", Network Associates, IN-Root-CA Individual Network e.V., EIS Corporation, Novembre 1998

Cottin N., Baala O., Gaber J., Wack M., "Management and QoS in Distributed Systems", *in Proceedings of the International Conference on Parallel and Distributed Processing Techniques and Applications* (PDPTA'00), Vol. III, Las Vegas, NV, Juin 2000

Cottin N., Mignot B., Wack M., "Authentication and enterprise secured data storage", IEEE international conference ETFA 2001, Sophia-Antipolis, France, 15-17 Octobre, 2001

Dobbertin H., Bosselaers A., Preneel B., “RIPEMD-160, a strengthened version of RIPEMD”, Fast Software Encryption, LNCS vol. 1039, D. Gollmann Ed., pp. 71-82, 1996

Dubuisson O., “ASN.1: Communication between Heterogeneous Systems”, Morgan Kaufmann Publishers, ISBN 0-12-6333361-0, Juin 2000

Elkins M., Del Torto D., Levien R., Roessler T., “Draft: MIME Security with OpenPGP”, Network Presence LLC., CryptoRights Foundation, University of California at Berkeley, Avril 2001

ETSI - European Telecommunications Standards Institute, *ETSI TS 101 733 v1.2.2*, “Electronic Signature Formats”, Décembre 2000

ETSI - European Telecommunications Standards Institute, “Policy requirements for time-stamping authorities”, *Draft ETSI TS XXXX STF 178-T1 draft H*, technical specification, ref. DES/SEC-004007-2, Sophia Antipolis, Juillet 2001

Farley J., *JAVA Distributed Computing*, O'Reilly and Associates, USA, ISBN 1-56592-206-9, Janvier 1998

Freier A. O., Karlton P., Kocher P. C., “Draft: The SSL Protocol Version 3.0”, Netscape Communications, Independant Consultant, Novembre 1996

Garfinkel S., *PGP: Pretty Good Privacy*, First Edition, O'Reilly, ISBN 1-56592-098-8, Décembre 1994

Garfinkel S., Spafford E. H., *Web Security & Commerce*, First Edition, O'Reilly, ISBN 1-56592-269-7, Juillet 1997

Housley R., Ford W., Polk W., Solo D., ‘”RFC 2459: Internet X.509 Public Key Infrastructure, Certificate and CRL Profile”, Spyrus, VeriSign and Citicorp, Janvier 1999

Kaeo M., *Designing Network Security*, Macmillan Technical Publishing, USA, ISBN 1-57870-043-4, 1999

Kaliski Jr B. S., “RFC 1319: The MD2 Message-Digest Algorithm”, RSA Laboratories, Janvier 1992

Kent S., “RFC 1422: Privacy Enhancement for Internet Electronic Mail: Part II: Certificate-Based Key Management”, BBN, IAB IRTF PSRG, IETF PEM WG, Février 1993

Linn J., “RFC 1421: Privacy Enhancement for Internet Electronic Mail: Part I: Message Encryption and Authentication Procedures”, IAB IRTF PSRG, IETF PEM WG, Février 1993

Mel H. X., Baker D., *Cryptography Decrypted*, Pearson Education Corporate, ISBN 0-201-61647-5, 2001

Menezes A. J., Van Oorschot P. C., Vanstone S. A., *Handbook of Applied Cryptography*, CRC Press, USA, ISBN 0-8493-8523-7, Février 2001

Myers M., Adams C., Solo D., Kemp D., “RFC 2511: Internet X.509 Certificate Request Message Format”, VeriSign, Entrust Technologies, Citicorp, DoD, Mars 1999

Myers M., Ankney R., Malpani A., Galperin S., Adams C., “RFC 2560: X.509 Internet Public Key Infrastructure, Online Certificate Status Protocol – OCSP”, VeriSign, CertCo, ValiCert, My CFO, Entrust Technologies, Juin 1999

Myers M., Ankney R., Adams C., Farrell S., Covey C., “Online Certificate Status Protocol, version 2”, *draft-ietf-pkix-ocspv2-02*, Mars 2001

NIST - National Institute of Standards and Technology, “Secure Hash Standard (SHS)”, Federal Information Processing Standards Publication, FIPS PUB 180-1, Avril 1995

NIST - National Institute of Standards and Technology, “Data Encryption Standard (DES)”, Federal Information Processing Standards Publication, FIPS PUB 46-3, Octobre 1999

NIST - National Institute of Standards and Technology, “Digital Signature Standard (DSS)”, Federal Information Processing Standards Publication, FIPS PUB 186-2, Janvier 2000

Preneel B., Bosselaers A., Dobbertin H., “The cryptographic hash function RIPEMD-160”, *CryptoBytes*, vol. 3, No. 2, pp. 9-14, 1997

Ramsdell B., “RFC 2632: S/MIME Version 3 Certificate Handling”, Worldtalk, Juin 1999

Ramsdell B., “RFC 2633: S/MIME Version 3 Message Specification”, Worldtalk, Juin 1999

Rescorla E., “RFC 2631: Diffie-Hellman Key Agreeement Method”, RTFM Inc., Juin 1999

Rivest R. L., “RFC 1320: The MD4 Message-Digest Algorithm”, MIT Laboratory for Computer Science and RSA Data Security, Avril 1992

Rivest R.L., “RFC 1321: The MD5 Message-Digest Algorithm”, MIT Laboratory for Computer Science and RSA Data Security Inc., Avril 1992

RSA Data Security Inc., “Public Key Cryptography Standards, PKCS 1-12”, disponible en ligne à ftp://ftp.rsa.com/pub/pkcs, 1993

Shamir A., “How to share a secret”, Communications of the ACM 22 (11), pp 612-614, Novembre 1979

Sun Microsystems, “’Lesson: Signing and Verifying JAR Files”, available on-line at http://java.sun.com/docs/tutorial/jar/sign/index.html, 2001