Utilisations des certificats d'attribut pour accélérer l'usage de la signature électronique

Paul Axayacatl FRAUSTO BERNAL
LGI2P- Site EERIE, Ecole de Mines d'Alès
Parc Scientifique Georges BESSE, 30035 Nîmes, France.
Paul.Frausto@ema.fr

Christian ANTOINE
URC EMA-CEA, Site EERIE,
Parc Scientifique Georges BESSE, 30035 Nîmes, France.
Christian.Antoine@ema.fr

Ahmed SERHROUCHNI
Télécom Paris (école nationale supérieure des télécommunications)
46, rue Barrault - 75634 Paris Cedex 13
Amhed.Serhrouchni@enst.fr

Résumé

Actuellement, de plus en plus d'ordinateurs sont interconnectés à l'Internet ou à des réseaux locaux. Il est donc indispensable de partager et de protéger l'information de façon performante. Pour accélérer et favoriser le développement de nouvelles applications et e-services autour des transactions électroniques, la sécurité devient alors une priorité. La PKI est une réponse conçue pour assure la sécurité des transactions électroniques et permet l'échange de renseignements sensibles entre des parties qui n'ont pas établi au préalable de liens commerciaux entre elles. La signature électronique est un service de base de la PKI qui permet l'authentification, la confidentialité, l'intégrité et la non-répudiation de la transaction électronique. Elle devient une composante fondamentale des transactions sécurisées. Elle pourra bientôt se substituer légalement à la signature écrite. Dans ce contexte, notre objectif est de contribuer au développement et à la création de nouveaux e-services nécessaires à la croissance des transactions électroniques: le rôle associé à la signature (pour connaître les privilèges du signataire aux moyens de la définition d'un rôle), l'habilitation et délégation de signature (pour donner l'autorisation à quelqu'un d'exercer un pouvoir à sa place et pour donner l'autorisation de transférer ce pouvoir à un tiers) et le contrôle de la signature/multisignature électronique d'un document (pour indiquer qui peut signer un document, et/ou contrôler la séquence et les priorités des signatures). Nous proposons donc d'utiliser le certificat d'attribut ,qui nous semble un instrument particulièrement avantageux pour générer ces nouveaux e-services. Son utilisation rend possible la délégation des droits, la signature avec un rôle plutôt qu'avec un identifiant et le contrôle de la signature électronique. Nous présentons aussi une infrastructure de confiance pour manipuler ces certificats et gérer ces nouveaux e-services.

Mots clefs

Infrastructure de confiance; E-services; Transactions électroniques; Signature électronique.

1 Introduction

Les réseaux informatiques ouverts tels que l'Internet ont été techniquement optimisés pour assurer le transport de données. Dans cette optique les aspects liés à la sécurité n'étaient pas une priorité essentielle. Or, Internet ayant vocation a devenir la plate-forme universelle d'échange de produits et de services, la sécurité devient primordiale.

Dans cette perspective, il est indispensable d'organiser les échanges électroniques par la mise en place de garanties spécifiques à la fois sur le plan technique et sur le plan juridique. Ces deux aspects sont indissociables.

Le chiffrement, et en particulier le chiffrement asymétrique (clé publique/clé privée) représente l'une des pistes les plus sérieuses pour avancer dans la sécurisation et l'authentification des échanges. L'infrastructure à Clé publique est mieux connue sous le nom de Public Key Infrastructure (PKI). C'est une réponse conçue pour assurer la sécurité des transactions électroniques et permettre l'échange de renseignements sensibles entre des parties qui n'ont pas établi au préalable de liens commerciaux entre elles.

Les certificats électroniques sont l'un des principaux composants des PKI actuelles. Les certificats d'identité lient une clé à une identité pour authentifier le possesseur du certificat, ils posent néanmoins certains problèmes, parmi lesquels on peut citer : leur rôle, leur durée de vie, leur association avec les listes de révocation de certificats et la gestion des modifications. Les certificats d'attribut ne contenant pas d'information explicite sur l'identité de la personne, ils ne peuvent pas être utilisés pour authentifier le possesseur du certificat. Ils permettent plutôt d'attribuer des permissions à une entité. Ces deux types de certificats (identité et attribut) sont complémentaires et leur association permet de développer de nouveaux services liés à la signature électronique en donnant une valeur juridique aux transactions.

La signature électronique est un service de base de la PKI, elle pourra bientôt se substituer légalement à la signature écrite. Pour cela, une infrastructure de confiance doit fournir aux différents acteurs (clients, fournisseurs, administrations, tiers de confiance) les éléments nécessaires pour utiliser de nouveaux e-services : les rôles associés à la signature, l'habilitation et délégation de signature et le contrôle de la signature/multisignature électronique d'un document. Notre objectif est d'utiliser les certificats d'identité et d'attribut pour créer des e-services comme :

- Certification de rôles : qui permet à une identité de signer comme représentant d'une fonction.
- La habilitation/délégation de la signature : qui permet au titulaire d'un pouvoir d'autoriser légalement un tiers à exercer ce pouvoir à sa place.
- La signature électronique contrôlée d'un document: qui indique qui peut signer un document, et contrôler la séquence et les priorités des signataires.

Les PKIs existantes PKIX [1], SPKI [2], SDSI [3], Keynote [4] et PGP [5] ne répondent pas encore à ce type de besoin, une infrastructure spécifique pour les certificats d'attribut est donc nécessaire pour prendre en compte ces nouveaux e-services. Nous proposons alors une architecture parallèle à la PKI pour gérer ses e-services et les certificats d'attribut.

Cet article présente dans un premier temps les concepts de base de la PKI, suivi des différentes approches utilisant les certificats d'attribut, dans un deuxième temps les e-services sont présentés avec des exemples représentatifs, nous continuons avec une proposition d'infrastructure parallèle pour la manipulation des certificats d'attribut et la gestion des nouveaux e-services. Ces travaux ont été réalisés au cours du projet RNRT I-CARE [6].

2 Principes de base

La Public Key Infrastructure permet de sécuriser de façon globale l'accès à un réseau, à des informations et données. La PKI est utilisée dans les domaines suivants : Email, e-commerce, réseau privé virtuel, extranets. Elle permet d'assurer de bout en bout la sécurisation des accès et de transferts de données. Plusieurs éléments entrent en jeu dans ce système, notamment les serveurs de certificats [7], les signatures électroniques, le cryptage du trafic et le certificat électronique. Dans ce chapitre nous présentons la définition de PKI et ces principaux composants.

2.1 Le concept PKI

PKI est la terminologie utilisée pour parler d'un système à clé publique qui offre les quatre services de base de la sécurité, essentiels aux échanges des informations :

1. **Confidentialité**.- Assurer le caractère privé de l'information.
2. **Intégrité**.- Attester que l'information n'a pas été manipulée.
3. **Authentification**.- Attester de l'identité d'un individu ou d'une application.
4. **Non-répudiation**.- Assurer que l'information ne pourra être plausiblement désavouée.

"La PKI est l'ensemble des algorithmes, protocoles et services pour gérer et sécuriser les échanges d'information. Elle s'appuie principalement sur la manipulation de certificats électroniques et l'utilisation de la cryptographie" [8].

2.2 La Cryptographie

La cryptographie est une discipline vieille de plusieurs siècles. L'usage de plus en plus répandu de l'ordinateur et l'arrivée des réseaux non protégés comme Internet lui ont donné une nouvelle impulsion surtout avec la cryptographie à clé publique dite aussi asymétrique [9].

La cryptographie classique est également appelée cryptographie symétrique. Elle repose sur l'utilisation d'une "clé" mathématique qui sert au chiffrement et au déchiffrement des données. Ainsi, pour faire parvenir un message de façon sûre, il faut le chiffrer à l'aide d'une clé connue uniquement de l'expéditeur et du destinataire. Le problème se pose pour faire parvenir au destinataire prévu la clé, de façon à ce que seul celui-ci puisse déchiffrer le message et ainsi l'authentifier.

Pour répondre aux problèmes de la cryptographie symétrique et obtenir plus de fonctionnalités la cryptographie à clé publique est apparue. Elle utilise deux clés, la première restée privée, tandis que la seconde est publique. Si l'on utilise la clé publique pour chiffrer un message, la clé privée permet de le déchiffrer. Autrement dit, il suffit de chiffrer un message à expédier à l'aide de la clé publique du destinataire, et ce dernier peut ensuite utiliser la clé privée pour le déchiffrer. Inversement si on utilise la clé privée pour chiffrer un message, la clé publique permet de le déchiffrer.

Avec l'application de la cryptographie à clé publique ou asymétrique nous avons les quatre fonctions principales de sécurité, essentielles aux échanges des informations: si on utilise la clé publique pour chiffrer un message, la clé privée permet de le déchiffrer dans ce cas on a la confidentialité et l'intégrité du message. Si on utilise la clé privée pour chiffrer un message, la clé publique permet de le déchiffrer et on a l'authentification et la non-répudiation car une et une seule personne possède la clé prive.

2.3 La signature électronique

La cryptographie à clé publique rend possible l'utilisation des signatures électroniques. Celles-ci permettent de corroborer l'origine d'un message. Pour signer un message, on utilise une fonction mathématique (fonction de hachage) qui produit un résumé du message. Le résumé obtenu est chiffré à l'aide de la clé privée de l'expéditeur. Le résultat, qui constitue la signature électronique, est annexé au message. Le destinataire du message peut ensuite s'assurer l'origine du message et l'intégrité de l'information.

2.4 Le certificat électronique

Le certificat est le document émis et signé par une entité (organisme digne de confiance ou un utilisateur normal), associant une clé publique à des informations relatives au propriétaire du certificat. Cette définition d'un certificat est la plus générale et est applicable à tous les certificats existants. Dans le chapitre suivant nous parlons de différents types de certificat électroniques.

3 Les certificats d'attributs

Pour pouvoir identifier le possesseur d'une clé publique et sa signature, les certificats d'identité ont été standardisés [10]. Ils lient une clé publique à une identité pour authentifier dans les échanges sécurisés. Une Autorité de Certification (CA) [7]émet les certificats d'identité, cette autorité joue le rôle de tiers de confiance. Le certificat d'identité est la représentation électronique du passeport dans le monde réel. Néanmoins, ils posent certains problèmes, parmi lesquels on peut citer : leur rôle, leur durée de vie, leur association avec les listes de révocation de certificats (CRL) [7] et la gestion des modifications. Ils ne sont pas recommandés pour inclure des attributs (par exemple: des informations portant sur les droits), car la durée de vie des attributs n'est pas forcement la même de celle du certificat d'identification, de plus les attributs peuvent être donnés par une entité différente de l'Autorité de Certification émettrice du certificat d'identité et enfin les attributs ne sont pas nécessairement demandés au même moment que la demande de certificat d'identité.

Les certificats d'attributs ont été créés pour résoudre les problématiques des certificats d'identité. En particulier, avec les certificats d'attributs la notion "de lier une clé à une identité par un certificat" est abandonnée. Le rôle d'un certificat est plus générale grâce à l'attribution de permissions au possesseur d'une clé. Un certificat d'attribut contient donc un ensemble d'attributs qui donnent des informations sur les privilèges du possesseur du certificat. Un certificat d'attribut est la représentation d'un visa dans le monde réel.

Les deux propositions les plus répandues sont le certificat d'attributs X.509 [8] et le certificat d'attributs SPKI [2]. Chacun d'entre elles offre des services ressemblants mais avec des mécanismes et des formats différents.

Le certificat d'attributs X.509 est une solution partielle orientée vers les services d'authentification du possesseur (par exemple : Le contrôle d'accès); L'infrastructure est centralisée et orientée sur l'authentification. Son point faible est la complexité à déployer les certificats d'attribut. Une part de cette complexité est attribuable à l'encodage des certificats X.509 en format ASN.1 et à la difficile intégration de nouveaux attributs.

Une autre solution sont les certificats d'attribut SPKI qui sont encodés en S-expressions et sont orientés vers l'autorisation et l'anonymat du propriétaire. Son infrastructure décentralisée permet de mettre en œuvre de manière rapide une plate-forme de certification. Mais, les contraintes de supports des listes de contrôle d'accès (ACL), des noms SDSI et la non distribution des certificats ont limitées son développement.

Malgré la souplesse ou les avantages de standardisation aucune de ces deux propositions ne répondent à tous nos besoins. Le certificat d'attribut proposé [11] nous semble un instrument particulièrement avantageux pour faire évoluer les

fonctionnalités de la signature électronique classique. L'encodage du certificat en format XML [12] amène une grande souplesse et le développement des usages. Le certificat rend possible la délégation des droits, la signature avec un rôle et le contrôle de la signature électronique.

4 Usages de Certificat d'attribut

"Dans les architectures de l'Internet du futur, producteurs et consommateurs d'information se retrouvent sur le même plan : tout individu peut être producteur/consommateur d'information, et les consommateurs peuvent consulter les informations d'autres producteurs d'information pour enrichir leur propre travail. Producteurs et consommateurs utilisent les moyens les plus appropriés à leur métier, à leur usage pour préparer les informations et les consulter." [6]

Le nombre des utilisateurs travaillant sur Internet a augmenté considérablement dans la dernière décennie, la nécessité de nouveaux outils pour réaliser ou faciliter leurs tâches est donc apparu. Or l'automatisation des procédures de travail devient primordiale pour les utilisateurs/entreprises car l'enjeu économique/fonctionnelle que celle-ci peut apporter est considérable. Par ailleurs, les échanges d'informations entre les différents utilisateurs augmentent exponentiellement, les documents sensibles sont de plus en plus envoyés dans des réseaux non-protéges. Un document sensible devrait indiquer son expéditeur, son destinataire et aussi devait être protéger de modification ou de la lecture d'un tiers non autorisé.

L'alliance de la cryptographie asymétrique avec les certificats d'attribut [11] rend possible le développement des multiples services pour sécuriser les procédures de travail, habiliter/déléguer les droits, utiliser les rôles, sécuriser les documents dans les réseaux non-protéges, ajouter des contraintes à la signature/multisignature électronique, automatiser la vérification de fichiers signés, etc. Dans ce contexte nous utilisons les certificats d'attribut pour générer trois types de e-services liés à la signature de fichiers:

1. La certification de rôles.
2. L'habilitation/délégation de droits.
3. La signature électronique contrôlée.

Ces e-services deviennent nécessaires à la croissance des transactions électroniques sécurisés dans les réseaux car ils sécurisent la transaction en utilisant comme base la signature électronique et en automatisant sa vérification. Le certificat d'attribut permet cette automatisation, ainsi que l'habilitation/délégation de la signature et la signature avec un rôle. Avec ces nouveaux e-services l'usage de la signature électronique devrait se développer en permettant aux utilisateurs de retrouver dans une environnement électronique le contexte et les contraintes quotidiennes des signatures papiers. Dans ce chapitre chacun des e-services est présentes avec un exemple pratique.

4.1 Acteurs dans les e-services

Les différents acteurs qui intéragissent pour mettre en oeuvre une transaction avec les e-services sont:

Générateur
Entité qui détient le pouvoir ou les droits sur certaines ressources,, c'est l'administrateur des certificats d'attribut, il réalise la gestion complète de la génération jusqu'à la répudiation de certificats. Dans cette étude le générateur crée les certificats d'attributs pour le contrôle des fichiers, génère les certificats de rôles et les certificats d'habilitation/délégation. Il faut remarquer que ses fonctionnalités ne s'arrêtent pas là, il peut aussi générer aussi un certificat d'attribut générique pour indiquer des attributs quelconques.

Utilisateur
Usager du système, c'est l'entité qui interagi avec les autres entités, il demande la génération/révocation de certificats d'identité, de certificats d'attribut, de certificats de rôles. Il peut signer/vérifier les documents, habiliter sa signature à une autre entité, et déléguer ses droits ou partie de ses droits (représentés avec rôles).

Vérificateur
Entité qui vérifie/utilise un fichier contrôlé ou un certificat électronique. Son rôle est simplement de regarder/vérifier(intégrité, non répudiation et authentification) les informations.

Tiers de confiance
Tout système qui aide les différents acteurs des e-services à se faire confiance. Des exemples de tiers de confiance : l'autorité de confiance de la PKI, le serveur de TimeStamp, le serveur OSCP ou de CRL, les annuaires, etc. [7].

4.2 La certification de rôles

L'utilisateur du certificat d'attribut est une entité quelconque, son identificateur peut-être notamment un rôle. Le rôle correspond à la représentation des privilèges du signataire dans sa fonction, il donne la possibilité de garder l'anonymat dans certaines transactions et permet d'associer un pouvoir à une personne, et en particulier le droit de signer. La signature électronique apposée sur les messages électroniques est une signature de "personne physique", alors que dans la pratique des affaires, de nombreux professionnels signent *en qualité* (par exemple en qualité de, directeur de laboratoire, directeur commercial, d'avocat, d'expert-comptable pour une téléprocédure, ...). Cette qualité est le rôle que le signataire porte. Dans ce contexte, quatre scénarios sont possibles :
- plusieurs entités sont liées à un rôle (par exemple le rôle "Secrétaire")
- une seule entité est liée à un rôle (par exemple le rôle "Directeur de laboratoire")
- plusieurs rôles sont liés à une entité (par exemple le "Directeur de laboratoire" peut aussi avoir le rôle "chef du projet I-CARE")
- une entité sans rôle.

Prenons pour exemple un scénario dans le laboratoire X. Carl est Directeur de laboratoire, Sylvie est secrétaire et Jean est directeur adjoint. Ils ont les rôles suivants :
- Carl → Directeur de laboratoire.
- Carl → Directeur de laboratoire - signer les congés.
- Carl → Directeur de laboratoire - commander des fournitures
- Carl → Directeur de laboratoire - embaucher du personnel
- Sylvie → Secrétaire
- Jean → Directeur adjoint.

Ces rôles sont en fait un niveau d'indirection entre les identités et leurs prérogatives. Ainsi, chacun peut choisir de déléguer sa signature ou bien seulement une partie du pouvoir associée à cette signature.

Avec les certificats d'attribut, les rôles peuvent être assignés de manière dynamique (sécurité configurable). Par exemple si un employé change de fonction, il faut seulement révoquer l'ancien certificat et générer un certificat d'attribut qui lui assigne sa nouvelle fonction (rôle). Cela permet de garder son certificat d'identité pour la signature de documents. L'utilisation de certificat d'attribut permet ainsi la certification de rôles de chaque individu dans un environnement électronique.

4.3 L'habilitation/ délégation de droit

L'habilitation donne l'autorisation à une identité (généralement l'un de ses subordonnés) d'exercer un pouvoir à sa place, alors que la délégation donne l'autorisation de transférer ce pouvoir à un tiers. Ces deux actions souvent utilisés par la plupart des employés dans leur vie professionnelle peuvent maintenant être réalisées dans un environnement électronique.

Il faut remarquer qu'il est possible d'habiliter tout ou une partie de ce droit avec un attribut particulier. Dans le cas de l'habilitation de signature électronique, le type de document à signer (feuille de congé, réservation de salle, etc.) peut aussi être pris en compte.

Pour obtenir une telle habilitation, le certificat d'attribut est la solutions que nous utilisons. Une entité A fournit un certificat d'attributs à une entité B, pour qu'elle puisse effectuer en son nom des actions pendant une durée déterminée. Par exemple (figure 1)dans le cas d'habilitation, considérons la situation où Carl est absent pendant 2 semaines, et ne peut donc pas signer les demandes de congés. Il va donc habiliter (avec un certificat d'attribut) la signature des demandes de congés ("Directeur de laboratoire - signer les congés") pendant son absence au rôle secrétaire (dans cette cas à Sylvie). En revanche, il ne va habiliter à personne son rôle "Directeur de laboratoire - embaucher du personnel", ainsi il est sûr que personne ne pourra embaucher du personnel pendant son absence. Ce certificat d'habilitation est alors joint à tout demande de congé signé par la secrétaire, il prouvera que la secrétaire a bien le droit de la faire.

Il existe aussi la possibilité de déléguer sa signature de manière totale. C'est à dire transmettre l'ensemble de son pouvoir, pour faire cela se suffit de lui habiliter le rôle "Directeur de laboratoire".

En général, le certificat d'attributs est composé de l'identificateur de l'émetteur, de l'identificateur du propriétaire, des droits à donner (attributs), du temps de validité du certificat et de la capacité de déléguer à un tiers. Dans la figure 1 Carl a habilité à Jean son rôle de directeur et indique qu'il peut déléguer lui aussi ce pouvoir. Jean peut donc dans les mêmes conditions, habiliter à Tom (ou autre) toutes ou une partie des fonctions de directeur (par exemple la signature de rapports techniques), et ainsi de proche en proche. Une chaîne de délégation de signature est créer dans laquelle le niveau de confiance ne se dégrade pas. L'identité des entités est alors garantie (sur demande) par l'émetteur du certificat d'attribut. Il vérifiera le certificat d'identité au moment de faire l'habilitation grâce à l'autorité de confiance.

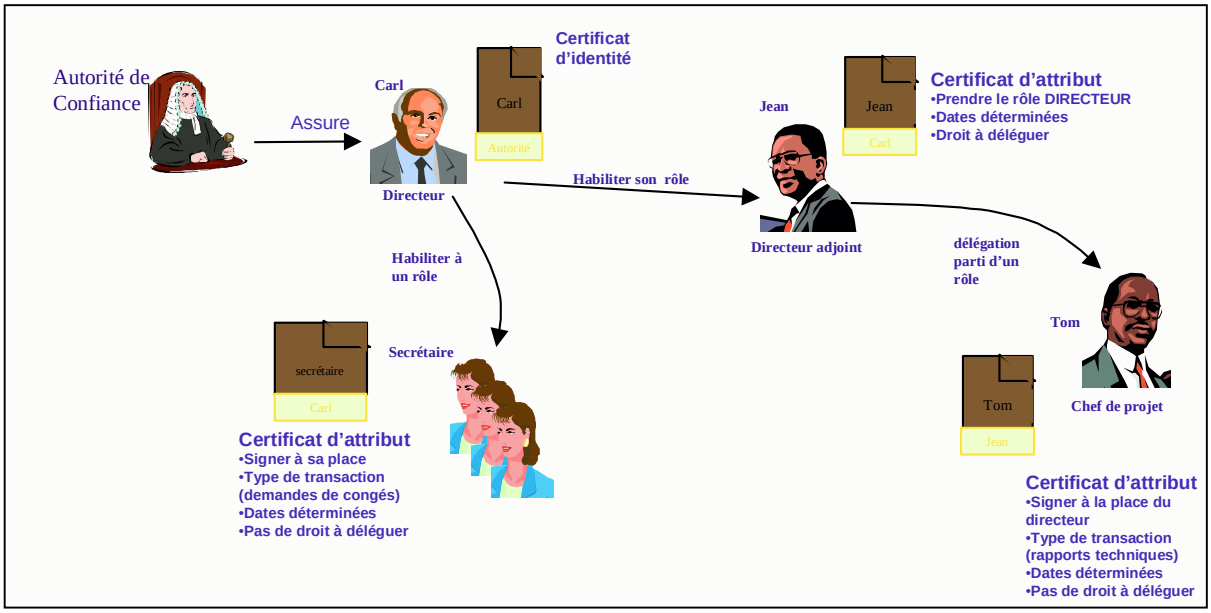

Figure 1- *Exemple habilitation/délégation et rôles*

4.4 Signature électronique contrôlée

La signature contrôlée est un nouveau e-service de signature utilisant le certificat d'attribut. Celle-ci permet d'étendre la signature d'un document en ajoutant des autorisations ou des contraintes particulières. Son objectif est d'indiquer qui doit signer le document et si c'est nécessaire dans quel ordre. Comme dans tout document en papier, le format électronique portera le nom du signataire du document. Cette action permet de vérifier automatiquement la signature, il suffit de vérifier la validité de la signature du fichier et de comparer le signataire avec le signataire demandé dans le certificat d'attribut.

Dans cet e-service, on attache un certificat d'attribut à un document. Le certificat indique l'entité (clés publiques ou identificateur) qui doit signer le document. D'autres informations essentielles comme les politiques de signature et le TimeStamp ne sont pas pour l'instant inclus dans la signature [13]. Ci-dessous une description des principales informations que nous proposons d'inclure dans cette signature :

- Le contenu de la transaction.- Le données signés peuvent être inclues dans la signature ou peuvent être référencées.
- L'heure et la date de la signature(TimeStamp) devront être dans un format standard et faire référence à la signature et non au résumé du document.- chaque signature du TimeStamp est protégée par son demandeur pour connaître sans possibilité de répudiation les dates de la signature. Les politiques de signatures avec toutes les informations relatives à la création de la signature : qui, quand, comment doit être signé le document.
- Les références aux certificats et CRL pour la vérification de la signature.

Des informations additionnelles peuvent être contenues pour faciliter le caractère légal de la signature :
- Les certificats et CRLs (ou les réponses de serveurs en ligne OSCP) qui valident les certificats pour vérifier à tout moment que les certificats étaient valables de la création de la signature.
- TimeStamp2 .- Un cache TimeStamp aurait pu être faire sur l'ensemble contentant les certificats et CRLs afin d'assurer sont contenu.

- Le type de transaction, pour indiquer le type de document, afin d'appliquer les règles valables. Exemple : bon de commande, un devis, un mail professionnel, un conte rendu , etc.
- Le lieu de la signature, afin de savoir quel droit appliquer pour la défense du signataire.

La mise en œuvre de services de signature électronique contrôlée a besoin d'un nouveau format pour encapsuler la signature et le certificat d'attribut. Pour cela, il est indispensable d'étendre la normes XMLDSIG [13]. L'extension de XMLDSIG [14] permet d'ajouter un ou plusieurs certificats d'attribut à la signature XMLDSIG pour indiquer les politiques de signature et les contraintes ou indication du document à signer. En plus avec ce format chaque signature du TimeStamp est protégée par son demandeur pour suivre sans répudiation les dates de la signature et éviter de falsifier ou d'antidater des engagements des autres signataires. Il faut noter que certaines informations sont déjà intégré dans la directive [15] de l'Union Européenne.

Dans la figure 2 nous montrons un schéma de la signature contrôlée d'une feuille de congés. Le certificat d'attribut lié au document indique les entités qui doivent le signer et l'ordre croissant (Vincent, Marc, Carl). D'abord c'est Vincent qui signe, après c'est Marc, ensuite Carl ne peut pas signer car il est absent. Donc en reprenant le cas de la figure 1, où Carl a habilité son rôle "Directeur de laboratoire - signer les congés" au rôle secrétaire. C'est une d'entre elles qui signe à sa place pour obtenir un document multisigné valide électroniquement et aussi juridiquement, si les certificats d'habilitation sont acceptes comme preuves.

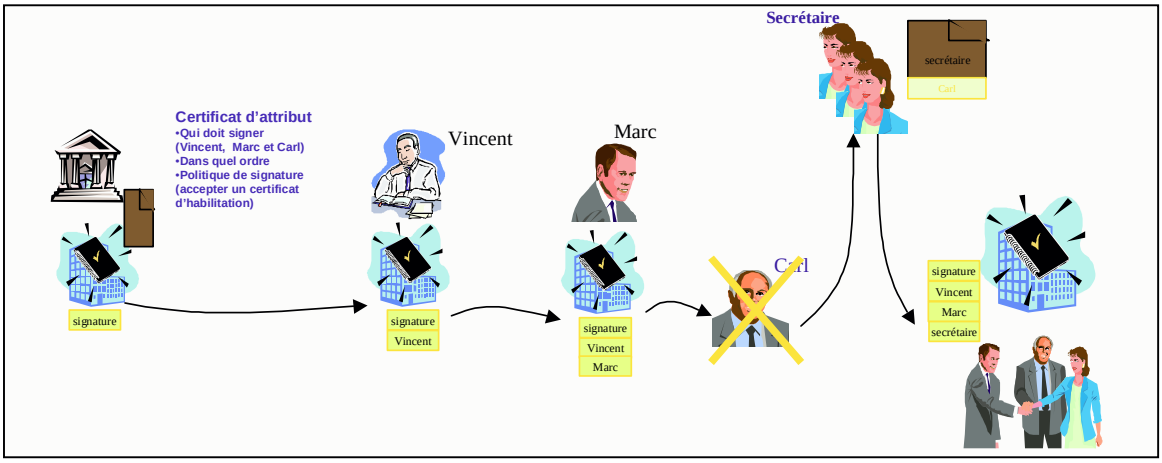

Figure 2- *Exemple de multisignature contrôlée*

Ce service permet de suivre l'état d'un document et de vérifier le respect de l'ordre de signataires. Son utilisation cible principalement les démarches administratives inter-entreprise. Dans le cas de contrat d'achat sur l'Internet où l'ordre des signatures n'a pas de valeur juridique ce service permet alors d'indiquer et de vérifier uniquement l'ensemble des signataires, leurs rôles , et les habilitations associées.

5 Infrastructure de confiance

Une infrastructure spécifique pour les certificats d'attribut est nécessaire pour prendre en compte ces e-services. Les PKI existantes ne répondent pas encore à ce type de besoin [16], il est donc indispensable d'ajouter de nouvelles fonctionnalités.

L'infrastructure doit supporter l'émission décentralisée des certificats d'attributs. Par exemple: un utilisateur quelconque pourra délivrer un document avec certaines contraintes de signature, ou délivrer un certificat d'attribut pour habiliter/déléguer à un tiers ses droits de signature. La décentralisation de la gestion des certificats d'attributs est donc nécessaire, contrairement à la gestion des certificats d'identité qui doivent être délivré par une entité centrale qui joue le rôle d'autorité de confiance. Cette infrastructure doit assurer la compatibilité générale de toutes les technologies utilisées dans les applications commerciales/industrielles.

Si un certificat d'attribut est délivré localement, les attributs n'ont pas besoin d'être définis globalement. La standardisation des attributs pourrait pénaliser leur souplesse d'utilisation.

Pour des certificats d'attribut avec des durées de vie courtes, il n'est pas nécessaire de mettre en place des mécanismes de révocation (il est alors possible en cas de problèmes d'attendre leur expiration et de ne pas les renouveler). Sinon il existe

des systèmes alternatifs de vérification, par exemple les serveurs de vérification en ligne OCSP qui peuvent attester la validité du certificat.

La réduction de la chaîne de certification [17] est nécessaire, pour faciliter la vérification des services. Par exemple dans la signature contrôlée, il y a une quantité non négligeable de certificats à vérifier, avec la réduction de la chaîne de certificat les temps de vérification diminueront énormément ainsi que la taille du message transmis.

5.1 Infrastructure

Pour répondre aux fonctionnalités précédentes nous proposons [18] de faire converger les différentes infrastructures PKIs. Le résultat est une PKI de base [1] avec une infrastructure parallèle gérant les certificats d'attributs, cette infrastructure s'inspire de la dernière proposition de la PKIX [14] et SPKI [2], avec plusieurs différences :

- L'infrastructure des certificats d'attribut est décentralisée et indépendante de la PKI.
- Le modèle de confiance est adaptable aux besoins et services des utilisateurs, il peut être distribué, centralisé, ou "web of trust", et permet la combinaison de ces différents types de modèles.
- Le modèle de confiance suit le principe de SPKI, mais valide toujours l'identité avec les certificats X.509.
- Le générateur peut être un utilisateur quelconque, celui-ci doit avoir seulement le droit de déléguer un pouvoir.
- La manipulation de rôles: avec un serveur de rôles ou avec des certificats de rôles, selon les besoins des utilisateurs.
- Le certificat d'attribut possède des fonctionnalités provenant des différentes spécifications. Son format ouvert à nouveaux usages est encoder en XML [12].
- Plusieurs identificateurs pour reconnaître le propriétaire et l'émetteur du certificat (noms X.500 [7], noms SDSI [3], clé publique, adresse IP, mail, etc.).
- La réduction de la chaîne de certificat est prévue ainsi que les mécanismes de vérification de certificat en temps réel avec OSCP ou hors ligne avec CRLs.

Le modèle simplifié de cette infrastructure est montre dans la figure 4.

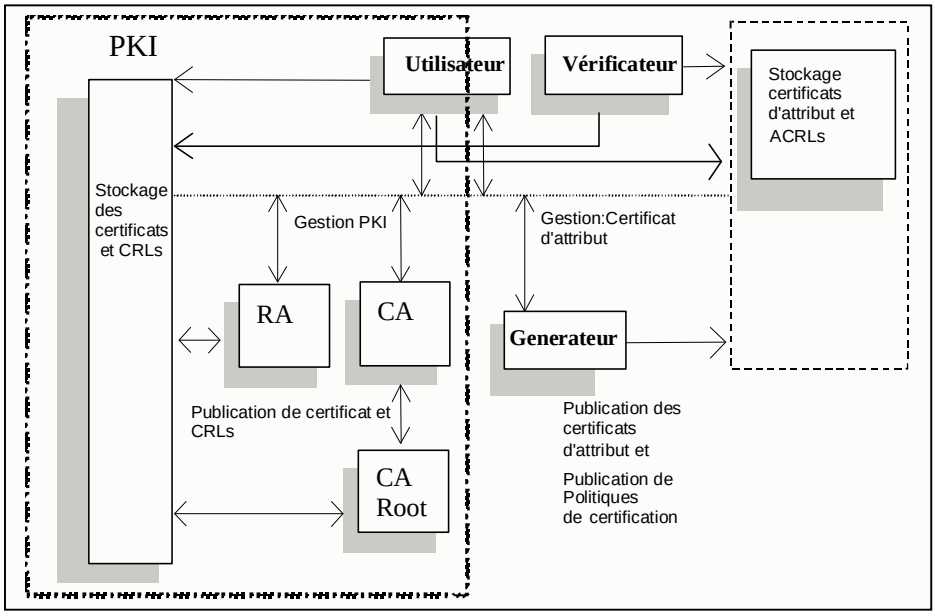

Figure 3- *Modèle simplifie de l'infrastructure.*

Les principaux acteurs de cette infrastructure sont :

PKI : Infrastructure qui supporte la gestion des certificats d'identité. Ses principaux composants sont la CA root classique, la CA, la RA et les serveurs PKI (LDAP, OSCP, TimeStamp, etc.) [7].

Utilisateur: Entité qui a besoin des certificats électroniques (d'identité et d'attribut). Il gère des certificats. Dans le contexte de la signature, l'utilisateur habilite / délègue signatures, signer/vérifier des objets.

Vérificateur: Entité qui interagit entre la PKI et l'infrastructure de certificats d'attribut pour vérifier la validité des certificats et signatures. Les tâches principales de cet acteur sont:

- Vérifier le certificat d'attributs.
- Extraire les attributs (en passant par la relation rôle → privilège si ce nécessaire) et vérifier la cohérence avec les politiques.

- Donner l'état du document (en ce qui concerne les signatures et la validité des certificats associés).
- Communiquer avec la PKI pour vérifier les certificats d'identité et CRLs.

Générateur des Attributs: Celui qui peut générer le certificat d'attribut (peut être un utilisateur quelconque s'il a le droit de délégation). Les tâches principales de cet acteur sont:

- Vérifier les certificats d'identité pour authentifier les demandeurs de privilèges.
- Définir les rôles: le rôle correspond à la représentation des privilèges du signataire. Par exemple le rôle de "chef de projet" donne au propriétaire du certificat d'attributs le pouvoir d'effectuer les opérations concernant un "chef de projet".
- Définir les politiques de signature pour la génération / utilisations de la signature. Par exemple: établir la taille minimum de la clé, la fonction de signature, etc.
- Définir les politiques de certification pour l'ensemble de règles qui surveillent le processus de vie d'un certificat. Par exemple les procédures pour demander le certificat, indiquer si un certificat est applicable à une communauté particulière ou une classe d'application, etc.
- Interagir avec les différents serveurs de la PKI (CA, RA, OSCP, TimeStamp, LDAP, etc.) pour valider les certificats et les signatures.

La PKI gère les certificats d'identité, les services et outils associés : La génération de clés, l'enregistrement des utilisateurs, la certification du lien entre les utilisateurs et ses clés publiques, la révocation de certificats, la certification réciproque, la publication de certificats et de CRL, la compromission des clés, la génération et maintenances de politiques de certification, la mis en ouvre des outils pour gérer tous ces services, etc. Cette infrastructure donne accès aux services de base de sécurité et permet le développement des nouveaux services.

En parallèle, l'infrastructure pour gérer les attributs administre les certificats d'attributs et les e-services associés (délégation, signature avec les certificats d'attribut, etc.). Cette infrastructure est fonctionnellement indépendante pour fournir l'ensemble des services avancés de signature.

La figure 3 schématise l'infrastructure de confiance général. Cette infrastructure permet l'authentification d'un utilisateur via un certificat d'identité X.509; Une fois l'utilisateur authentifié, on peut l'autoriser ou non à effectuer des opérations, sur la base des droits contenus dans le certificat d'attributs.

6 Conclusion

L'utilisation d'une infrastructure de confiance peut contribuer à réduire les coûts globaux d'exploitation et de transaction du commerce électronique, en assurant la protection des renseignements des entreprises et des particuliers, et en assurant également que les transactions électroniques sont valides. La sécurité est une composante fondamentale des applications de commerce électronique, notamment : courrier électronique, transmission de bons d'achat, échange de renseignements sur les cartes de crédit, transmission de contrats, automatisation des procédures de travail au moyen de formulaires nécessitant une ou plusieurs signatures.

L'utilisation de certificats d'attribut permet le développement de nouveaux e-services, indispensables pour accélérer l'usage de la signature électronique. Les e-services permettent de retrouver des actions courantes de la vie professionnelle, dans un environnement électronique sûr et simple. Ces e-services rassurent les utilisateurs où des engagements pourraient être falsifier ou antidater.

Dans la signature contrôlée, le fait que le document soit propriétaire du certificat d'attributs permet de spécifier des contraintes sur la signature et de suivre son état. Toute altération annulera la validité du document.

Le service d'habilitation de droits augmente les possibilités d'utilisation de la signature électronique. La signature peut être habilitée et utilisée dans l'environnement électronique de la même façon qu'avec des documents papier. L'utilisation des certificats d'attribut pour habiliter/déléguer droits permet de créer une chaîne de confiance qui ne se dégrade pas et de vérifier facilement cette délégation. Ces droits peuvent aussi bien être assignés à un rôle qu'à une identité physique.

L'infrastructure de confiance proposée permet dès à présent de tester ces nouveaux e-services. Cette infrastructure est basée d'une part sur PKIX (pour authentifier les entités) et d'autre part sur une infrastructure ouverte et décentralisée (pour la gestion des attributs). Les fonctionnalités de cette infrastructure ne s'arrêtent pas aux e-services présentés, des services comme le contrôle d'accès peuvent aussi être gérer sur ces mêmes bases.

Remerciements

Nous remercions le Réseau National de Recherche en Télécommunication français (RNRT) qui a financée ces travaux à travers du projet I-CARE (Infrastructure de Confiance sur des Architectures de RésEaux Internet & Mobile).

Références

[1] R. Housley, W. Ford, W. Polk, D. Solo, "Internet X.509 Public Key Infrastructure Certificate and CRL Profile" RFC 3280 IETF, avril 2002.
[2] C. Ellison, B. Frantz, B. Lampson, R. Rivest, B. Thomas, T. Ylonen, "SPKI Certificate Theory" RFC 2693 IETF, sep. 1999.
[3] R. Rivest, B. Lampson, "A Simple Distributed Security Infrastructure version 2" MIT, février 1998.
[4] M. Blaze, J. Feigenbaum, J. Ioannidis, A. Keromytis, "The KeyNote Trust-Management System Version 2" RFC 2704 IETF, sep. 1999.
[5] J. Callas, L. Donnerhacke, H. Finney, R. Thayer, "OpenPGP Message Format", Draft IETF, Août 2002.
[6] Projet I-CARE, "I-CARE Infrastructure de Confiance sur des Architectures de Réseaux Internet & Mobiles", RNRT 2000.
[7] Groupe de travail Public-Key Infrastructure (X.509) (PKIX), IETF, http://www.ietf.org/html.charters/pkix-charter.html
[8] ITU-T Recommendation X.509 | ISO/IEC 9594-8: “Information Technology – Open Systems Interconnection – The Directory: Public-Key And Attribute Certificate Frameworks” ITU-T, 03/2000.
[9] W. Diffie and M.E. Hellman, "New Directions in Cryptography", IEEE Trans. on Info. Theory, vol. IT-22, pp. 644-654, Nov. 1976.
[10] Rec. X.509 | ISO/IEC 9594-8: “Technologies de l'information – Interconnexion des systèmes ouverts – l'annuaire: cadre d'authentification” ITU-T, 08/1997.
[11] P. Frausto, C. Antoine, A. Serhrouchni, "Attribute certificates for the growth of e-services", Dans Actes du congrès GRES’03, Fortaleza, Brazil, février 2003.
[12] W3C "The Extensible Mark-up Language (XML) the base specifications XML 1.0", W3C Rec 02/1998.
[13] D. Eastlake, J. Reagle, D. "XML-Signature Syntax and Processing" RFC 3275 IETF, mars 2002.
[14] P. Frausto, C. Antoine, "Controlling digital multi-signature with attribute certificate", 18th Annual Computer Security Applications Conference, Las Vegas, dec. 2002.
[15] ETSI, « XML Advanced Electronic Signatures (XAdES)”, ETSI TS 101 903 v1.1.1 .02/2002.
[16] P. Frausto, C. Antoine, Vincent Derozier, "Etude et analyse des problèmes liés aux certificats X.509 et etude d’autres alternatives", Rapport de Recherche RR02/G3/013, Ecole des Mines d'Alès-LGI2P, juin 2002.
[17] D. Clarke, J. Elien, C. Ellison, M. Fredette, A. Morcos, R. Rivest, "Certidicate Chain Discovery in SPKI/SDSI", Computer Security Journal, v 9, Issue 4, pp. 285 – 322, January 2001.
[18] P. Frausto, C. Antoine, A. Serhrouchni, "Infrastructure de confiance pour integrer de nouveaux e-services utilisant les certificats d'attribut - ", IEEE Canada
[19] S. Farrell, R. Housley, "An Internet Attribute Certificate Profile for Authorization" IETF RFC 3281, April 2002.
[20] C. Ellison and B. Schneier, ``10 Risks of PKI", Computer Security Journal, v 16, n 1, pp. 1-7, 2000.
[21] ABA, "Guidelines to help assess and facilitate interoperable trustworthy Public Key Infrastructures", Draft Information Security Committee, American Bar Association, Juin 2001.
[22] ETSI, "Electronic Signatures Formats", ETSI TS-101-733-v1.2.2, 12/2000.
[23] Michel Riguidel, "La problématique de la sécurité dans l'Internet du futur", Workshop RNRT, Brest 2000.
[24] Michel Riguidel, "Pour l'émergence d'une nouvelle sécurité dans les réseaux de communication et les systèmes d'information futurs", OFTA, Paris 2000.
[25] A. Serhrouchni, M. H. Sherif, "La monnaie électronique et les systèmes de paiements sécurisés" , Editions Eyrolles, 2000.