ABSTRACT A LA PUBLICATION CNRS

LA SIGNATURE ELECTRONIQUE ET LES PROCESSUS DE CERTIFICATION ET DE SECURITE

CONTEXTE

Les Systèmes d'Information et de Communication (SIC), répondant aux besoins des organisations sont souvent bien protégés des dangers et des menaces externes. Ces organisations doivent, depuis quelques années, relever le défi de l'ouverture au commerce électronique : les échanges inter-entreprises, les échanges entre l'entreprise et le client particulier, les échanges entre l'entreprise et les administrations,…

La sécurité de ces échanges empruntant les réseaux Internet reste une exigence très forte, exprimée par l'ensemble des acteurs et des décideurs au sein des organisations. En particulier, pour certaines transactions critiques, la nécessité d'associer une valeur juridique à la signature électronique des documents échangés est mise en évidence.

Face à cette opportunité, il s'agit de clarifier les caractéristiques essentielles de la signature électronique, les processus de certification de la signature électronique par un tiers de confiance, ainsi que les processus de sécurité associés aux SIC.

ORIGINE ET EVOLUTIONS D'INTERNET

En 1969, l'organisation américaine Defense Advanced Research Projects Agency (DARPA) initialisa un programme de recherche et de développement pour la création d'un réseau à commutation par packets, appelé ARPANET. L'expérience d'ARPANET eut un tel succès que de nombreuses organisations adoptèrent ce réseau pour la télécommunication de leurs données.

En 1975, ARPANET devint un réseau opérationnel sous la responsabilité de Defense Communication Agency (DCA). Le protocole de communication TCP/IP fut développé à partir de cette expérience et adopté en tant qu'un standard militaire pour donner naissance au réseau MILNET. Le terme Internet désigna alors les deux réseaux ARPANET et MILNET.

L'Internet est ainsi devenu le réseau mondial le plus ouvert capable d'interconnecter plusieurs milliers de réseaux d'entreprises, d'universités, d'organisations gouvernementales, quels que soient les équipements, les systèmes d'exploitation et les réseaux, grâce à un processus d'adressage universel des réseaux ainsi reliés entre eux.

La mondialisation du commerce et la montée des échanges internationaux ont mis en évidence l'intérêt de ce réseau facilitant les échanges électroniques : commande, achat, facturation, paiement, opérations bancaires et boursières, échanges avec les administrations, les hôpitaux, les universités,...

RISQUES ENCOURUS PAR L'UTILISATION D'INTERNET

Les risques encourus proviennent essentiellement des défauts ou des manques de sécurité dans les échanges d'informations sous les protocoles Internet :

- Non garantie de l'adresse et de l'identité de l'expéditeur de l'information.
- Non garantie de l'acheminement de l'information transmise par l'expéditeur.
- Non garantie du délai d'acheminement de l'information transmise.
- Non garantie de l'intégrité de l'information reçue.

- Non garantie de la confidentialité de l'information reçue.

En général, les risques liés aux échanges sur Internet sont bien analysés par les Risk Managers au sein des organisations et ceci depuis la fin des années 1990. Des premières parades techniques ont été mises en œuvre pour protéger les Systèmes d'Information et de Communication des premiers dangers de l'Internet.

Des dispositifs de sécurité tels que le pare-feu (fire-wall), sécurisant l'accès aux systèmes d'informations critiques, aux serveurs Web et aux équipements de télécommunication ont été installés. De même, des procédures d'authentification des utilisateurs ont été généralement mises en oeuvre. Ces mesures sécuritaires n'ont pas pour autant dissuadé les pirates spécialistes, qui ont su organiser depuis plusieurs pays des attaques (passives ou actives) contre les sites les plus exposés.

Les opportunités d'Internet et du commerce électronique ont été telles que les organisations ont eu tendance à ouvrir davantage leurs Systèmes d'Information et de Communication aux clients, aux partenaires et aux administrations, sans avoir érigé des barrières protectrices suffisamment efficaces pour dissuader l'intrus.

Il s'ensuit une progression de la cybercriminalité, accrue par l'insuffisance, voire l'absence de moyens d'authentification de l'internaute et aggravée par un manque de cadre juridique clair, permettant le développement des échanges électroniques en toute confiance.

La directive européenne n° 1999-93 du 13 décembre 1999 sur la signature électronique et la loi française qui la transpose, donnent un cadre juridique général aux besoins de sécurisation des échanges sur l'Internet. La solution technique répondant à ces besoins, est basée sur des Infrastructures de Gestion de Clés (IGC) ou Public Key Infrastructures (PKI en Anglais).

BESOINS ET EXIGENCES LIES A LA SIGNATURE ELECTRONIQUE

Avant la généralisation de l'Internet, les besoins d'échanges sécurisés, par exemple entre les banques ou entre un donneur d'ordres et ses sous-traitants ne concernaient que des communautés fermées, pour lesquelles des solutions satisfaisantes de sécurisation ont été mises en place, reposant généralement sur la cryptographie.

Sécuriser des échanges électroniques pour des populations très nombreuses, souvent fluctuantes et de plus en plus cosmopolites, par exemple, les échanges entre les particuliers et les commerçants, entre les entreprises elles-mêmes, entre les administrations et les administrés, requiert un niveau de sécurité permettant d'éviter des risques inacceptables. Dans ces cas, les besoins de sécurité concernent :

- l'identification de l'expéditeur et du destinataire,
- la garantie que le message est bien remis au destinataire,
- la non répudiation, aussi bien par le destinataire que par l'expéditeur : ils ne doivent pas pouvoir nier, l'un avoir envoyé le message, et l'autre l'avoir reçu,
- l'horodatage du message, équivalent au cachet de la poste faisant foi,
- l'intégrité du message, garantissant que le message reçu est celui envoyé par l'expéditeur,
- la confidentialité du message, garantissant que son contenu ne peut être lu que par les deux correspondants, et que son existence même ne peut être connue que par les deux correspondants.

Les besoins de sécurité à satisfaire dépendent des exigences requises par type d'échanges électroniques. Ces exigences sont généralement de 3 ordres :

- Les exigences juridiques.
- Les exigences techniques.
- Les exigences financières.

Exigences juridiques :

Pour pallier aux insuffisances de sécurité, la réforme législative du 13 mars 2000, alignée sur la directive européenne n° 1999-93 du 13 décembre 1999 relative au cadre communautaire des signatures électroniques, a été effectuée pour permettre « à la France, à ses entreprises et à ses consommateurs, de profiter pleinement de l'essor du commerce électronique ».

Cette loi adapte le droit de la preuve aux technologies de l'information, associe une valeur juridique à la signature électronique et instaure la présomption de fiabilité au bénéfice des procédés de signature qui répondent aux exigences fixées par le Conseil d'Etat.

La France confirme sa position en faveur d'un haut niveau de sécurité dans les échanges électroniques par le décret n° 2001-272 du 30 mars 2001 portant sur :

- les dispositifs sécurisés de création de signature électronique,
- les dispositions permettant de garantir l'exactitude de la signature électronique,
- le cadre réglementaire et le rôle accordé aux prestataires de services de certification électronique.

Il reste cependant à préciser la procédure d'accréditation des organismes qui qualifient les prestataires de services de certification.

Exigences techniques

En principe, la sécurité des échanges électroniques doit répondre aux 4 besoins de sécurité, donnant l'assurance de la preuve :

- identification et authentification des deux parties de la transaction,
- confidentialité des informations échangées,
- intégrité des informations échangées,
- non répudiation de la transaction par l'expéditeur, ainsi que par le destinataire (en raison de l'absence de garantie d'acheminement de message par Internet).

Pour assurer la confidentialité des informations, la cryptographie, soumise à une réglementation, est utilisée. En France, cet usage était jusqu'à ces dernières années soumis à l'autorisation préalable des services spécialisés du Premier Ministre.

Jusqu'à la fin des années 70, les correspondants échangeant un courrier chiffré n'utilisaient que des systèmes dits à clés symétriques : les deux correspondants détiennent la même clé, qui permet à la fois de chiffrer et de déchiffrer le message.

La cryptographie à clés asymétriques, ou à clés publiques, est apparue à la fin des années 70. A chaque correspondant sont remises deux clés complémentaires : l'une, publique, servant à son correspondant pour chiffrer les messages qu'il lui adresse, l'autre, privée ou secrète, qu'il conserve pour déchiffrer ces messages. Les clés publiques sont accessibles dans un annuaire sécurisé, où chacun trouve la clé publique de son correspondant pour chiffrer le message qu'il lui destine. Il est difficile de calculer la clé privée de son correspondant par la connaissance de sa clé publique.

La cryptographie à clés publiques permet également de signer les messages et d'en garantir l'intégrité. Les Infrastructures de Gestion de Clés (IGC) utilisent la cryptographie à clés publiques et signent, avec leur propre clé privée, le certificat (carte d'identité électronique) remis à leurs clients. L'organisme qui met en œuvre une IGC, remplit ainsi le rôle du tiers de confiance et les certificats délivrés par celui-ci sont utilisés par les correspondants lors des échanges électroniques de documents.

La signature électronique repose sur la cryptographie à clé publique et permet d'assurer l'identification et l'authentification de l'émetteur, l'intégrité et la non répudiation du message

envoyé par l'expéditeur. La confidentialité du message est assurée par la fonction de chiffrement ou de cryptage.

La signature électronique d'un document (message, formulaire, transaction,…) est ainsi caractérisée par 3 fonctions :

- La fonction de hachage permettant d'obtenir l'empreinte (le condensé ou condensat) du document à envoyer.
- La fonction de chiffrement de l'empreinte du document (le document est ainsi signé par l'expéditeur).
- La fonction de gestion de la clé : chaque partie détient une paire de clés publique et privée ; l'expéditeur signe le document à envoyer avec sa clé privée et envoie sa clé publique au destinataire pour qu'il puisse vérifier la signature du document.

Les étapes de signature électronique d'un document sont représentées par le schéma suivant (l'étape 3 : l'accusé de réception étant facultatif) :

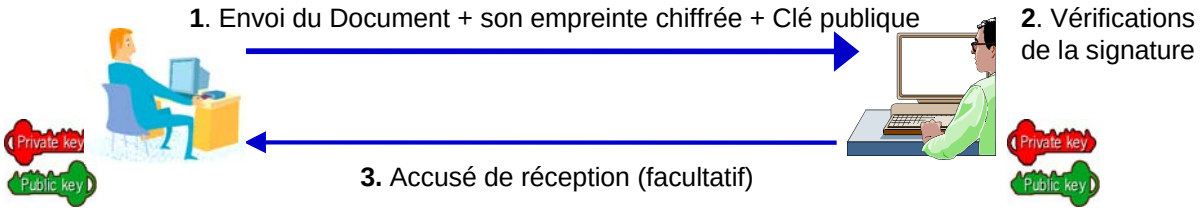

Schéma 1 : Signature électronique du document

Lorsqu'un document est signé électroniquement, l'organisme tiers de confiance appelé dans le décret du 30 mars 2001 « le prestataire du service de certification », est responsable de la certification de cette signature.

Le tiers de confiance peut être un prestataire de service. En France, la Poste, France Télécom et Thomson, parmi d'autres, proposent ce service. Lorsque les deux correspondants appartiennent à un même organisme ou à une même communauté, le tiers de confiance peut être une entité de cet organisme ou de cette communauté. On peu citer deux exemples : le service de tiers de confiance assuré par une entité au Ministère de l'Economie et des Finances, pour les besoins internes du Ministère, et le service de tiers de confiance destiné aux professionnels de santé.

Exigences financières

Il s'agit, d'une part, d'analyser les risques (impacts et probabilités) et de calculer l'investissement nécessaire basé sur les exigences de sécurité permettant de réduire ces risques.
Il y a lieu, d'autre part, de bien s'assurer de la pérennité de la solution retenue.

SOLUTION BASEE SUR UNE INFRASTRUCTURE DE GESTION DE CLES (IGC)

Une Infrastructure de Gestion de Clés comprend un ensemble de dispositifs en matériels et en logiciels, ainsi que des moyens organisationnels, qui sont mis en œuvre par un tiers, à qui les deux correspondants font confiance.

Généralement, le tiers de confiance est responsable des opérations suivantes :

- enregistrer les demandes de certificat émises par les utilisateurs qui doivent justifier leur identité. Ces opérations sont déléguées à l'autorité chargée de ces enregistrements,

- remettre à l'utilisateur un certificat qui sera joint à tous les courriers qu'il enverra, permettant à ses correspondants de s'assurer de l'origine de ces courriers. L'utilisateur reçoit également les éléments secrets nécessaires pour signer les courriers, suivant des règles précisées par les pratiques de certification : les éléments peuvent être envoyés par un échange électronique en ligne ou bien stockés dans une carte à microprocesseur remise de façon sécurisée.
  Ces opérations sont déléguées à l'autorité chargée de la délivrance des certificats,
- entretenir la liste des certificats révoqués et la date de leur révocation.

La politique de certification précise les règles et les pratiques de certification. Le coût de mise en œuvre de ces règles et de ces pratiques est d'autant plus élevé que les garanties de sécurité associées sont importantes. Il est donc nécessaire d'apprécier le niveau de sécurité assuré par le tiers de confiance, en rapport avec le prix du certificat proposé.
Dans cette perspective, la directive européenne prévoit une signature avancée, qui satisfait aux exigences suivantes :

- elle est liée uniquement au signataire,
- elle permet d'identifier le signataire,
- elle est créée par des moyens que le signataire peut garder sous son contrôle exclusif.

Chaque pays définit les conditions dans lesquelles les exigences de sécurité sont remplies. En France, le projet de décret sur la signature électronique prévoit que les services spécialisés auprès du Premier Ministre garantissent la satisfaction de ces exigences, au terme d'une évaluation.

DEMARCHE PROPOSEE

Sécuriser les échanges électroniques doit se faire suivant une démarche adaptée aux besoins réels de l'organisation. Les échanges électroniques, empruntant un Intranet (pour les échanges internes) ou un Extranet (pour les échanges avec les partenaires, clients ou fournisseurs répertoriés), ne nécessitent pas une certification telle que proposée par une IGC.

Notamment, la mise en œuvre d'un service de certification reste complexe et peut engendrer certaines lourdeurs administratives, des changements importants dans l'organisation de la sécurité et des investissements techniques importants.

La démarche proposée est présentée par le schéma suivant :

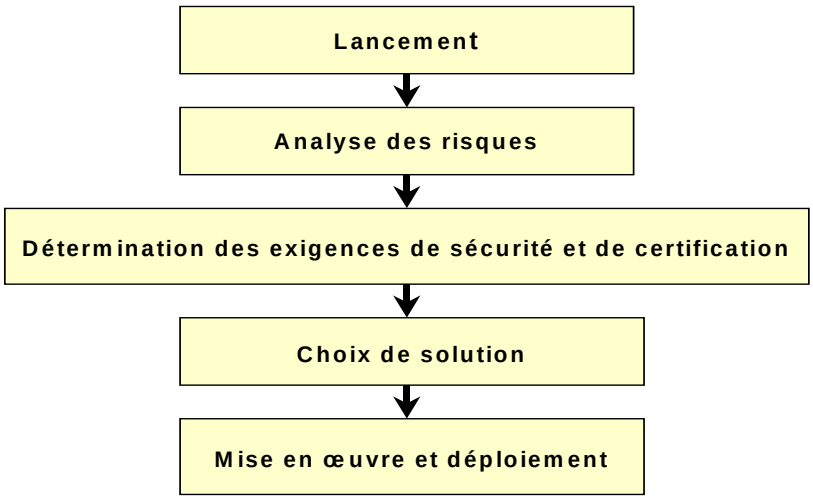

Schéma 2 : démarche de conduite de projet des processus de sécurité et de certification

Cette démarche comprend les étapes suivantes :

1. Identifier et analyser les risques liés aux échanges électroniques de documents sensibles relevant des Systèmes d'Information et de Communication,
2. Déterminer les exigences de sécurité et de certification des documents échangés électroniquement,
3. Choisir une solution adaptée à l'organisation et répondant aux besoins et aux exigences du métier, tout en recherchant :

- la rentabilité des investissements nécessaires à la réduction des risques.
- la détermination d'une charte de sécurité et la définition des règles et des pratiques de certification pour les échanges électroniques,
- l'adaptation de l'organisation de la sécurité à ces nouvelles exigences,
- la sensibilisation aux processus de sécurité et de certification de tous les utilisateurs de la signature électronique,

4. Mettre en œuvre la solution et réaliser son déploiement.

PERSPECTIVES DE DEVELOPPEMENT DE LA SIGNATURE ELECTRONIQUE ET DES PROCESSUS DE CERTIFICATION

Actuellement la signature électronique est surtout utilisée par les applications E-Administration telles que la télé-déclaration des revenus, la télé-TVA, le vote électronique ou les applications liées au domaine de la santé.

Dès 2006, les techniques de signature électronique seront généralisées aux cartes d'identité électroniques.

Le développement de la signature électronique et des processus de certification dans les entreprises est à étudier secteur par secteur et en fonction des risques majeurs liées aux systèmes d'information et de communication.

Michel PRIE et Ladan PEGAH

Césys