La certification : une opportunité pour les banques

Les technologies PKI, en apportant une solution homogène et globale à la sécurité des échanges, lèveront un des principaux obstacles au développement du commerce électronique. Tiers de confiance, les banques ont un rôle à jouer en se positionnant en autorité de certification.

LAURENT BELLEFIN
Directeur de l'activité sécurité
SoluCom

Une infrastructure PKI (Public Key Infrastructure = infrastructure à clés publiques) est un ensemble de composants, de fonctions et de procédures qui vont permettre de gérer la création, la distribution et le cycle de vie de jeux de clés numériques et de certificats numériques. Grâce à son jeu de clés et de certificats, l'utilisateur peut réaliser la signature électronique des messages et des transactions qu'il émet, et peut chiffrer ses échanges.

Par exemple, pour sécuriser un échange entre un utilisateur et un serveur informatique, il est nécessaire que l'utilisateur, mais aussi le serveur informatique, soient en possession de leurs jeux de clés et de certificats respectifs. Les clés permettent d'assurer le chiffrement et la signature électronique des échanges. Les certificats permettent de garantir l'identité du porteur des clés, avec une fiabilité plus élevée que la saisie d'un nom d'utilisateur et d'un mot de passe.

Pour créer un certificat, il est au préalable nécessaire de procéder à l'enregistrement de l'utilisateur, c'est-à-dire à la saisie et au contrôle des informations d'identité qui seront contenues dans le certificat. Après cet enregistrement, les clés de l'utilisateur sont générées et l'autorité de certification procède à la création et à la distribution du ou des certificats. Les opérations d'enregistrement et de création des certificats sont réalisées par un organisme en qui l'utilisateur doit avoir toute confiance. C'est sur la crédibilité de cet organisme, l'autorité de certification, que repose la sécurité de l'infrastructure.

Chaque autorité de certification distribue des certificats à une population donnée d'utilisateurs et de serveurs informatiques, et crée ainsi un domaine de sécurité pour ces entités. Pour traiter le cas d'échanges entre utilisateurs qui ne font pas partie du même domaine de sécurité, il est possible de mettre en œuvre des mécanismes de certification croisée ou de certification hiérarchique. Ces mécanismes permettent d'envisager la mise en œuvre de très grands domaines de sécurité sur internet (*figure 1*).

A l'intérieur de ces domaines de sécurité, la non-répudiation des transactions peut être assurée, du fait de la reconnaissance légale de la signature numérique : le cadre juridique permettant cette reconnaissance se met en place, grâce à la directive européenne sur la signature numérique, déjà transposée dans le droit français. La technologie des PKI est donc une innovation capitale pour gérer la sécurité dans les grands réseaux intranet et surtout pour permettre le développement des e-Echanges sur internet.

La place des banques et leur positionnement comme autorité de certification

Plusieurs raisons font des institutions financières des tiers de confiance privilégiés pour le commerce électronique, et favorisent leur positionnement comme autorité de certification :

- l'existence d'un réseau d'agences qui permet

de réaliser l'enregistrement des demandes, avec la capacité de gérer les risques clients ;
• une position «naturelle» d'intermédiaire de confiance dans les échanges financiers en général ;

Les PKI : sécurité des intranet et des échanges sur internet

➤ La technologie des PKI permet à un utilisateur, grâce à son architecture originale, de réaliser des échanges sécurisés avec un grand nombre de serveurs sans que ceux-ci aient besoin de connaître l'utilisateur au préalable. Seule l'autorité d'enregistrement a vérifié une fois pour toutes l'identité de l'utilisateur pour le compte de toute la communauté.
Elle offre, sous la forme d'une solution de sécurité unique, une panoplie de fonctions répondant à tous les besoins de sécurité des échanges électroniques (authentification, confidentialité, intégrité, non-répudiation). Grâce à l'utilisation de standards et aux mécanismes de certification croisée ou hiérarchique, il sera possible de créer des domaines de sécurité de très grande taille sur internet, domaines de sécurité ingérables en pratique avec des solutions traditionnelles.

• une expérience du déploiement et de la gestion de solutions de sécurité.

L'Administration des finances ne s'y est pas trompée. Elle a incité les banques à proposer une offre de certification dans le cadre des «Téléprocédures», c'est-à-dire la dématérialisation progressive des échanges avec l'Administration, et sa première application : TéléTVA. Les Banques populaires, BNP Paribas, le Crédit agricole, le CCF, le Crédit lyonnais, La Poste (via sa filiale Certinomis) et la Société générale se sont déjà positionnés.

Se pose maintenant pour les banques la question d'étendre l'usage de cette technologie à d'autres besoins. Les domaines d'applications possibles sont multiples. Les premières demandes proviennent des applications bancaires destinées aux entreprises (*cash management*, gestion de comptes titres, virements de gros montants…), ou bien pour des applications internes à chaque banque. Pour ce type d'applications, les banques peuvent construire une architecture de certification qui leur est propre, et distribuer des certificats à leurs clients et à leurs employés.

Mais au-delà, cette technologie doit permettre les échanges entre des clients de banques différentes. Il est alors nécessaire d'assurer l'interopérabilité des infrastructures PKI, par exemple dans un modèle de certification hiérarchique, ce qui pose la question du choix d'une autorité de certification «racine» qui va garantir la sécurité de l'ensemble de l'édifice et l'interopérabilité des PKI des banques.

C'est dans ce but que de nombreuses banques américaines, européennes et asiatiques (presque une cinquantaine à ce jour) se sont regroupées autour de l'initiative Identrus. Quelques PKI de ce type sont déjà opérationnelles aux Etats-Unis et en Allemagne. En France, les banques adhérentes sont BNP Paribas, le Crédit agricole, le Crédit lyonnais, la Société générale et le CCF, via sa maison mère HSBC.

Identrus est une autorité «racine» de certification, mais aussi une société américaine qui a édité un ensemble de spécifications techniques, procédurales et juri-

1. Modèle de certification hiérarchique avec plusieurs Autorités de certification

diques que doivent respecter les PKI des banques qui souhaitent bénéficier du label Identrus. Pour que ce label soit validé, Identrus fait procéder, pendant la mise en place de l'infrastructure, à des audits de conformité. Orienté uniquement vers le *B-to-B*, Identrus a pour but de sécuriser les échanges entre clients de banques différentes, dans un modèle dit «à 4 coins». L'usage de certificats dans ce modèle donne lieu à une rémunération de la société Identrus.

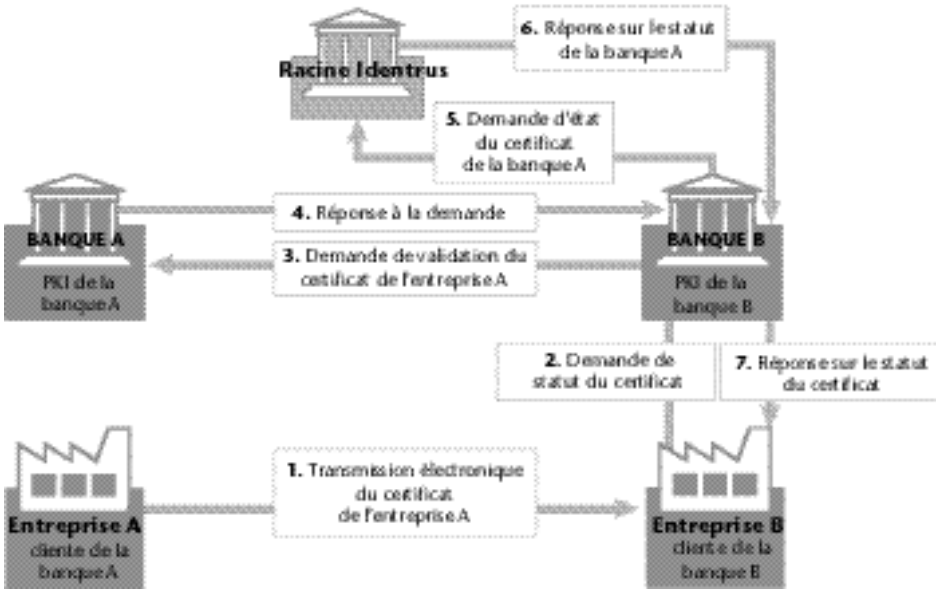
Au niveau européen, une autre initiative rassemble un grand nombre de banques : il s'agit de GTA (*Global Trust Authority*). GTA a un objectif plus large en termes de types d'usages (notamment *B-to-C*), et devrait être ouvert à des organismes non bancaires. Les contraintes techniques imposées sont moins fortes que pour Identrus. En revanche, il n'y a pas de systèmes opérationnels aujourd'hui et le modèle économique d'utilisation de GTA n'est pas défini.

Mais les initiatives comme Identrus ou GTA resteront inutiles si elles ne sont pas complétées par des applications de base nécessaires au commerce électronique (comme la gestion du paiement) qui sauront s'appuyer sur elles. Identrus l'a bien compris et a poussé les banques à lancer la réalisation d'Eleanor, future application de gestion et de suivi d'ordres de paiement. Swift va de son côté lancer prochainement une offre dans ce domaine.

Monter une offre de certification

Un faisceau d'éléments convergents (loi et décrets sur la signature électronique, initiatives de l'Administration, d'Identrus et de GTA, besoins des applications d'e-banking…) pousse donc les institutions financières à se positionner comme autorités de certification. Pourtant, les banques françaises n'ont pas encore d'offre Identrus ou GTA disponible. Certes, elles ont déjà acquis pour certaines d'entre elles une première expérience grâce à TéléTVA. Mais elles sont aussi conscientes des incertitudes qui pèsent encore sur le développement du marché de la certification.

2. Schéma simplifié des échanges pour la validation d'un certificat Identrus



Les risques techniques et financiers sont biens là. Le ticket d'entrée est élevé, du fait du coût de la technologie, et des impacts importants de sa mise en place. En effet, un projet PKI fait intervenir de multiples volets : volet technique et sécuritaire, mais aussi travail d'intégration des applications, mise en place d'un back-office complet (traitement et suivi des demandes, hot-line, support, facturation…), marketing de l'offre, communication interne et client, validation juridique… Les risques techniques sont importants du fait du peu de maturité de la technologie et de l'instabilité des standards.

Mais les concurrents sont déjà en marche. Certaines banques étrangères sont plus avancées, et d'autres acteurs comme les chambres de commerce, les acteurs du domaine santé/social (GIP CPS, GIP/ MDS) ou encore les assureurs se positionnent ! Il sera probablement nécessaire pour les banques françaises de prendre des risques dans les mois à venir pour ne pas perdre l'initiative sur ce domaine clé pour la maîtrise des flux liés aux échanges électroniques sur internet.

Les questions à traiter sont multiples : choisir le bon moment pour démarrer, définir un périmètre prioritaire selon les marchés visés (applications *B-to-B* haut de gamme, e-banking, vente de certificats aux entreprises pour des applications non bancaires…), décider de construire l'infrastructure en interne ou de l'externaliser… Dans ce contexte, le choix de la bonne stratégie sera déterminant. ●