La sécurité des échanges s'améliore

Les besoins de sécurisation des échanges sur le Net sont multiples : éviter les intrusions indésirables, protéger son système d'information, authentifier les émetteurs… Les solutions techniques disponibles se multiplient.

ERIC GUILLERM
Directeur général
NetSecure Software

Le CCF a mis en place son service de banque à distance accessible via l'Internet depuis fin novembre 1997. Cette offre est venue compléter les accès télématiques disponibles comme le minitel ou le téléphone. La banque se devait d'adopter une solution de sécurité robuste et fiable, afin de protéger son système d'information et d'assurer à ses clients la confidentialité des opérations effectuées. Elle ne pouvait prendre le risque d'échanger avec ses clients en utilisant des clés de chiffrement faibles de 40 bits qui pouvaient être cassées en quelques heures avec des équipements bon marché.

De même le CCF ne souhaitait pas déchiffrer les informations dans une zone librement accessible de l'extérieur, ce que font les serveurs web équipés SSL, afin d'éviter que les informations puissent être récupérées par une intrusion sur le serveur web lui-même (bien que complexe cette opération est souvent possible).

«La demande en matière de sécurité Internet est encore largement centrée sur les firewalls : leur marché devrait croître de 174 % par an jusqu'en l'an 2000.»

Enfin le CCF voulait se protéger de toute intrusion externe en garantissant un cloisonnement complet de son réseau vis-à-vis de l'extérieur.

EVITER LES INTRUSIONS

La banque a donc mis en œuvre un chiffrement fort de 128 bits, autorisé en France et à l'export. La solution sélectionnée permet d'assurer l'intégrité, la confidentialité des échanges sur tout type de poste de travail, sans installation de logiciel sur le poste grâce à la technique d'applet Java. Elle garantit un chiffrement 128 bits quel que soit le pays d'origine de la connexion, où SSL fournira du 40 bits en France, du 100 bits en Espagne et 128 bits aux Etats-Unis.

Evidemment, le service bancaire proposé par le CCF nécessite d'accéder à certaines ressources du système d'information. Afin de garantir la sécurisation d'une interconnexion réseau, le principe le plus communément retenu est de placer un *firewall* en coupure sur le réseau. Ainsi placé, celui-ci peut inspecter toutes les données et appliquer la politique de sécurité définie par la banque. La demande en matière de sécurité Internet est encore largement centrée sur ce type d'outil : encore embryonnaire dans les années 1990, le marché du *firewall* devrait croître, selon les spécialistes, de 174 % par an jusqu'en l'an 2000.

Pour éviter tout risque d'intrusion, le CCF a de plus retenu une solution de sécurisation qui permet d'échanger avec le système d'information en utilisant un mécanisme original de collecte : il autorise le client à récupérer les informations le concernant sans laisser aucune possibilité d'intrusion du fait qu'aucun canal n'est ouvert de l'intérieur vers l'extérieur. Le déchiffrement des informations est réalisé à l'intérieur du réseau de l'entreprise, sans qu'elles aient jamais pu être consultées en

1 Le coût d'une transaction

En dollars

Dans une banque	**1,07**
Par courrier	**0,73**
Par téléphone	**0,54**
Par Internet	**0,01**

Source : American Banking Association.

clair sur l'Internet ou le serveur web, contrairement à ce que permettent les serveurs SSL.

Authentifier l'émetteur

Cependant, les services en ligne bancaires sont de plus en plus nombreux. Ils devraient encore croître comme le confirme la réduction du coût de la transaction liée à l'utilisation d'Internet (*encadré 1*). L'élargissement de cette offre, qui permet maintenant le passage d'ordre en ligne, implique de renforcer les moyens d'authentification et garantir la non-répudiation. Celle-ci permet par des techniques cryptographiques de signature électronique de rendre impossible la contestation d'une transaction par son auteur. Enfin, de plus en plus de banques souhaitent maintenant diffuser des informations, parfois confidentielles, vers leurs clients particuliers ou entreprises (mode *push*).

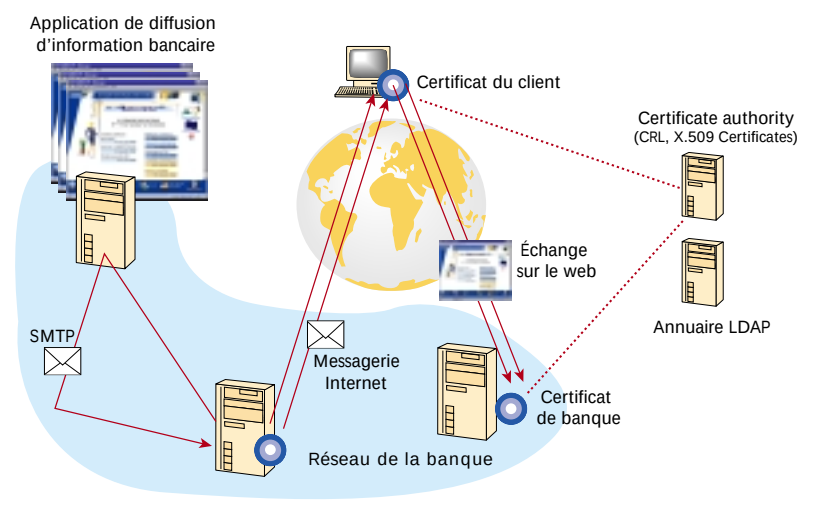
C'est pourquoi les outils de sécurisation des services en ligne bancaires vont devoir évoluer pour intégrer les techniques récentes d'infrastructure de clés publiques (PKI) et de certificats X509. Les infrastructures à clés publiques permettent de générer et d'acquérir le certificat qui va authentifier chacun des clients, de chiffrer tous types de flux TCP-IP (http, ftp, telnet, SQLnet), de les déchiffrer et de chiffrer la messagerie électronique de façon bi-directionnelle. Celle-ci sera sécurisée au niveau de l'intégrité du contenu des messages, mais aussi des signatures de l'émetteur et du récepteur.

La carte à puce, solution d'avenir

La baisse du coûts des lecteurs de carte à puce et leur progressive intégration dans les ordinateurs personnels permettent d'envisager très prochainement l'utilisation de ces carte comme moyen d'authentification pour les transactions en ligne. Les cartes à puce peuvent en effet stocker les certificats renforçant ainsi le niveau de sécurité. Ce pourra être les prochaines cartes bancaires (EMV : EuroCard MasterCard Visa) qui prévoient un champ à cet effet ou des cartes dédiés pour le service en ligne.

Reste à savoir si les utilisateurs devront posséder un certificat par service en ligne, ce qui dépend de la politique de l'entreprise, ou si une normalisation des organismes de certification bancaire permettra d'utiliser le même certificat pour communiquer avec plusieurs banques ?

Intégrer les infrastructures à clés publiques (PKI)



Une infrastructure PKI permet à un client de se connecter à un service en ligne sécurisé et d'assurer de façon transparente l'authentification mutuelle, le chiffrement des échanges et la signature, en utilisant les certificats du client et du serveur en ligne. Elle permet également à un client d'envoyer ou de recevoir des messages chiffrés et signés (non-répudiation) à un service en ligne. Les certificats sont certifiés par l'autorité de certification (Certificate Authority). Ils sont accessibles via un annuaire LDAP.