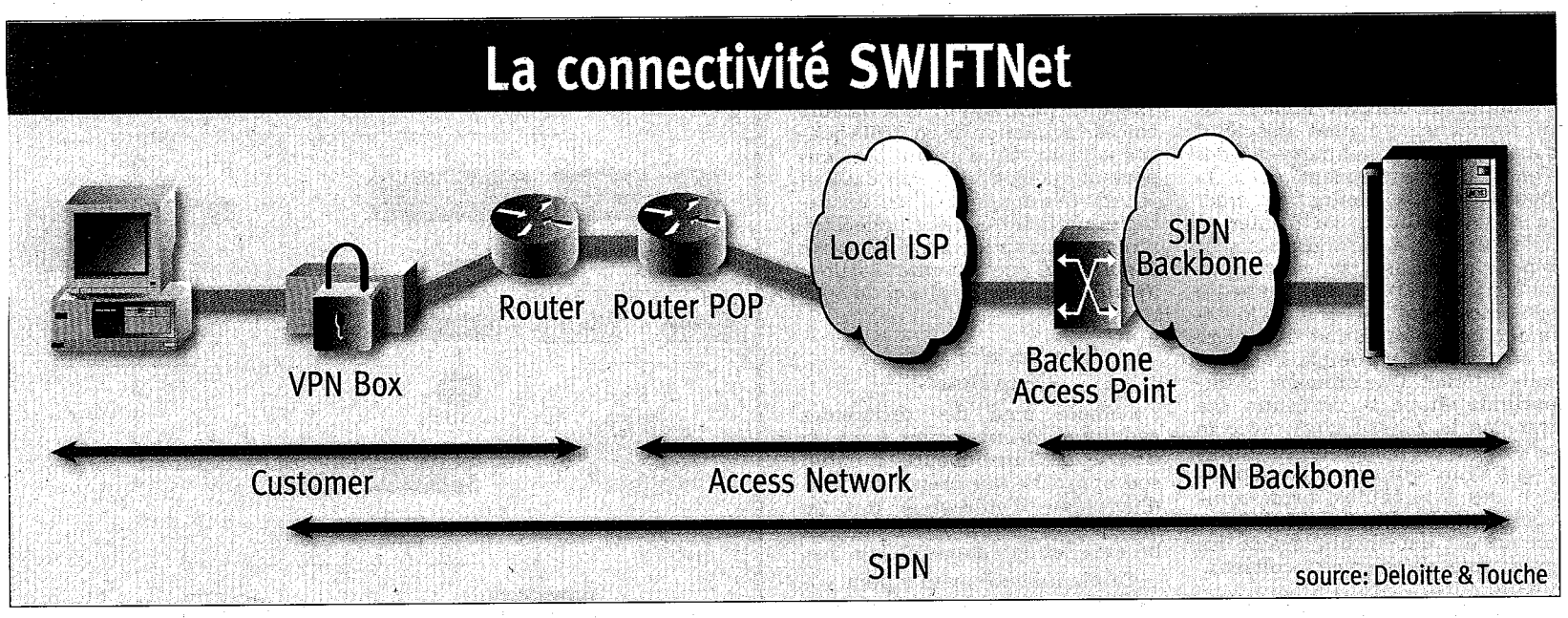
SWIFTNet

La sécurisation du réseau IP SWIFT

Entre juillet et septembre 2003, l'ensemble des utilisateurs grand-ducaux devra migrer sur le nouveau réseau SWIFTNet

par Charles Delbrassine *



SWIFT, l'un des acteurs incontournables de la messagerie financière, procède actuellement à la mise en production de son «Secure IP Network» (SIPN) servant au transport des applications SWIFTNet.

Cette migration obligatoire va toucher plus de 7.000 utilisateurs dans le monde et plus de 99 % des organismes financiers de la place de Luxembourg. Initialement prévue entre mai et juin 2003, SWIFT vient d'annoncer que la migration des utilisateurs grand-ducaux sur SWIFTNet ne se fera finalement qu'à partir du mois de juillet et qu'elle devrait être achevée en septembre 2003.

Pourquoi cette migration?

La connectivité X25 est obsolète et les coûts opérationnels y relatifs sont nettement plus élevés que ceux d'un réseau TCP/IP, tel qu'utilisé par SWIFTNet. De plus, le protocole TCP/IP est déjà largement implémenté et généralement bien maîtrisé par la plupart des organismes financiers.

SWIFTNet permettra aussi l'utilisation de toute une nouvelle gamme de services en temps réel, chose qui n'était que difficilement possible avec la technologie X25.

Quels nouveaux services?

Outre le transport des messages financiers (FIN) actuellement supporté par la plate-forme X25, SWIFTNet permet la mise en place de transfert en temps réel de données sous formats bruts ou prédéfinis, le transport d'autres standards de messagerie financière, ainsi que l'utilisation d'applications de consultation en ligne.

Ces nouveaux services permettront la mise en place d'applications telles que: le reporting, les paiements par lots, les «securities pre-trade», l'initialisation de paiements en ligne, ... répondant aux besoins d'automatisation et de rationalisation des transactions financières.

La connectivité SWIFTNet

Dans chaque pays, SWIFT a choisi plusieurs fournisseurs de services TCP/IP de manière à permettre la mise en place de solutions redondantes. Ces points de connexions sont routés par les ISP locaux sur leur propre réseau jusqu'au point d'accès de la dorsale SIPN, réseau privé propriété de SWIFT. La confidentialité de cette partie de la communication est assurée par un «VPN» basé sur un équipement spécifique procédant au cryptage du trafic entre le site «client» et le point d'accès à la dorsale «SIPN» .

D'autres mécanismes de sécurisation, tels que le filtrage des paquets IP, les «Access-Lists», le «Network Adress Translation» (NAT), l'analyse du trafic (shaping/policing) et des tests réguliers sont les garants d'un haut niveau de sécurité.

Le Module SWIFTNet Link (SNL)

Le «SNL» assure la sécurité entre l'interface utilisateur et le point central de traitement des données SWIFT (end-to-SWIFT) permettant le filtrage des messages ainsi que la vérification des identités. Il fournit également les éléments nécessaires au support de la sécurité «end-to-end» via SWIFTNet PKI.

Cette sécurité est négociée par session sur base de clefs symétriques partagées entre le module SNL et le Switch central.

Quel est le principe d'une solution de PKI?

La PKI est un mécanisme basé sur des clefs asymétriques dans lequel une clef permet de décrypter ce qui a été crypté à l'aide de la première. Il est donc basé sur des clefs produites par paires, constituées d'une clef publique, utilisée par les correspondants et d'une clef privée, uniquement connue par son propriétaire. Deux paires de clefs distinctes sont utilisées pour la signature et le cryptage. Pour signer un message, je vais avoir recours à ma propre clef privée, laquelle sera validée par le(s) récepteur(s) au moyen de ma clef publique de signature. Pour crypter un message, je vais utiliser la clef publique de cryptage du destinataire m'assurant ainsi qu'il sera le seul à pouvoir décrypter le message sur base de sa clef privée de cryptage.

Les clefs publiques sont certifiées par une autorité supérieure appelée «Certification Authority» (CA) et publiées dans un répertoire des certificats ou distribuées directement par le propriétaire. Ce certificat n'est rien d'autre qu'un fichier électronique signé par la «CA» qui contient la clef publique d'un utilisateur et de ce fait l'identifie de manière irrévocable.

Par ce mécanisme, les solutions de PKI offrent donc des services d'authentification, de non-répudiation, d'intégrité et de confidentialité.

SWIFTNet PKI

Dans SWIFTNet, la sécurité «end-to-end» est assurée par la mise en place d'une solution de PKI.

Les éléments constitutifs de cette PKI sont distribués comme suit :

– «Local Registration Application LRA». Située au niveau de l'application SWIFT, elle permet à l'officier de sécurité mandaté de procéder à l'enregistrement d'employés ou de départements et de gérer les clefs et certificats (recouvrement, révocation, ...).

– «Registration Authority – RA». Opérée par SWIFT, elle a pour rôle d'inscrire les institutions financières au service SWIFTNet PKI et de procéder à l'enregistrement des utilisateurs.

– «Certification Authority – CA». Opérée par SWIFT, elle agit sur base des demandes en provenance des «LRA». Son rôle est de produire ou de révoquer des certificats et d'assurer la mise à jour de la base des certificats.

– «Certificate Directory». Cette base hiérarchique de type X500 contient tous les utilisateurs autorisés, leurs certificats ainsi qu'une liste des révocations. Elle est accédée par les «LRA» en mode lecture-seule.

Les clefs utilisées par SWIFTNet sont de type RSA 1024 bits. La paire de clefs servant à la signature est produite par le module SNL et ne quitte pas le logiciel tandis que les clefs de cryptage sont générées par le «CA» et délivrées de manière sécurisée. Les clefs privées sont cryptées puis stockées sur des «smart cards».

Les certificats publiés dans la «Certificate Directory» sont accessibles par les modules «SNL» permettant de cette manière la vérification de la signature d'un message reçu ou le cryptage d'un message à émettre.

Le but est donc à terme de remplacer les mécanismes de «Bilateral Key Exchange» et «SLS» actuellement utilisés par une solution de type PKI complètement intégrée. L'utilisation unique de PKI est planifiée pour l'année 2004. Avant cette date, les messages FIN seront gérés sur base d'une solution mixte «BKE-PKI» transparente pour les utilisateurs.

Impacts à court terme sur les organismes financiers

Au niveau organisationnel, les institutions financières devront nommer un «Security Officer» formé par SWIFT et en charge de la fonction de «Local Registration».

D'un point de vue informatique, la migration de la plate-forme de messagerie actuelle vers la nouvelle version de SWIFT Alliance ou l'intégration du module «SNL» dans des applications «home made» est nécessaire au support de SWIFTNet.

La mise en place de SWIFTNet est à considérer comme un point d'entrée «TCP/IP» supplémentaire et devrait entraîner l'intégration de cette plate-forme dans la gestion globale de la sécurité (protocole, anti-virus,...). Il y a lieu de considérer le module «SNL» comme étant le dernier élément externe de cette nouvelle architecture. Ce module étant intégré au serveur SWIFT Alliance Access ou Entry, lequel est sans conteste un serveur critique, il est préférable d'opter pour la création d'une «DMZ» abritant un ou plusieurs SWIFT Alliance Gateway (SAG) plutôt que de connecter directement le serveur applicatif SWIFT.

L'intégration des nouveaux éléments dans un programme de veille technologique devrait assurer l'évolution du niveau de sécurité face aux nouvelles vulnérabilités et leurs exploitations.

Les messages financiers faisant partie intégrante de la chaîne de production critique des organismes financiers il y a également lieu d'adapter au plus vite les procédures, plans de désastre ou continuité de manière à intégrer les nouveaux éléments tels que: la fonction de «Security Officer» ou la connectivité IP par exemple ...

* *Charles Delbrassine est directeur chez Deloitte & Touche*