

Sécurité des réseaux

La validité des cadenas informat

IDENTIFICATION. La reconnaissance des signatures électroniques passe par une adoption juridique mondiale des certificats d'authentification. La Suisse abandonne la mise. L'avis du Fribourgeois Michel Rueger, spécialiste des réseaux sécurisés.



Michel Rueger «La signature électronique se définit comme un sceau attaché à une donnée numérique.»

Ça gribouille vite dans le domaine des signatures électroniques. Les législations en la matière sont en pleine mutation en Europe et surtout en Suisse, afin d'identifier encore mieux qui est qui au bout de la ligne. Il en va de l'avenir des sites commerçants. Le marché de l'e-business évoluera en offrant de réelles garanties de confidentialité. Ces gages d'authenticité ne sont pas seulement techniques, mais juridiques.

Engagé comme Network Designer dans l'entreprise de feu Mcnet à Fribourg, puis comme Security product manager chez VIA Net.Works (Suisse), Michel Rueger conduit actuellement des projets de connexions internet et de sécurité pour les entreprises. A 27 ans, ce jeune Fribourgeois de Granges-Paccot est à l'aise dans toutes les combinaisons des cadenas informatiques.

Des clefs privées aux clefs publiques, en passant par les certificats, il nous explique les tenants et aboutissants des signatures électroniques.

RK : Une signature manuscrite sur un bout de papier, numérisée ensuite par un scanner, balancée quelque part sur le Web ou attachée à un e-mail, a-t-elle un avenir?

MR : Cette démarche équivaudrait à l'envoi d'un fax. Pour qu'une signature manuscrite ait vraiment de la valeur, elle doit être écrite à la main, sans moyen de reproduction. Ce système n'a aucun avenir sans l'associer à un certificat d'authenticité. Ce serait trop facile de scanner une signature quelconque et de l'appliquer sur un document.

RK : Le terme signature électronique, utilisé dans le sens de «fichier signature», fait référence à une notion de sécurité informatique qui implique un contrôle. Peut-on en dire davantage?

MR : La signature électronique se définit comme un sceau atta-

ché à une donnée numérique. Elle constitue un bloc de données créé à l'aide d'une clef privée; la clef publique correspondante et le certificat permettent de vérifier que la signature provient réellement de la clef privée associée, qu'elle est bien celle de l'expéditeur et que les données n'ont pas été altérées. La clef publique est fournie avec un «certificat de clef». Ce dernier est délivré par un prestataire de service de certification ou par l'autorité de contrôle.

RK : Quel rôle joue véritablement ce certificat?

MR : Il permet, entre autres, d'authentifier un serveur web (serveur HTTP ou HTTPS) et d'identifier un utilisateur accédant à ce serveur web. Ces deux dernières possibilités sont définies par le standard SSL (*Secure Socket Layer*). Le certificat sert également à signer et crypter le courrier électronique (standard S/MIME), ainsi qu'à signer des applets Java ou autres.

RK : Quel est le niveau de fiabilité de la sécurité des signatures sur le Web, actuellement?

MR : Les systèmes de chiffreages traditionnels, comme les DES (*Data Encryption Standard*) par exemple, ne sont pas du tout adaptés à la situation d'Internet. Ils nécessitent en effet l'échange préalable d'une clef qui doit rester secrète entre deux interlocuteurs désirent dialoguer confidentiellement (par une connexion cryptée) : il serait

iques

impossible de préserver le secret de cette clef si elle transitait sur ce réseau, de par sa nature même (gestion décentralisée, contrôle d'accès faible ou absent, etc.). C'est pourquoi les systèmes asymétriques comme RSA offrent une meilleure sécurité, et sont donc déjà largement privilégiés dans les applications de e-commerce.

RK : Quel type de procédure est utilisé dans le système des certificats ?

MR : Pour les signatures digitales, il arrive souvent dans les systèmes à clefs publiques (c'est en particulier le cas de RSA) que la relation entre les deux clefs, privée et publique, soit parfaitement symétrique. Il est possible de crypter un message avec une clef privée et tout le monde pourra le décrypter avec une clef publique. Il n'en résulte ainsi aucune confidentialité, mais par contre une authentification. On pourrait dire ainsi « puisque je suis le seul à posséder cette clef privée, tout le monde peut être sûr que je suis l'auteur du dit message : c'est comme si je l'avais signé. » C'est ce type de procédure qui est utilisé dans le système des certificats.

RK : Ce système de clef publique a-t-il une faiblesse ?

MR : Oui. Ce système est malheureusement sensible aux attaques par intermédiaire (*man-in-the-middle attack*) : un malfrat contrôlant le canal entre deux correspondants peut, lorsqu'ils s'échangent leurs clefs publiques, les mettre de côté et les remplacer par des clefs contrefaites de son choix (en particulier, il dispose des clefs privées qui leur sont liées). Cela lui permettra par la suite de décrypter les messages transmis et les correspondants ne s'apercevront de rien s'il s'assure de les crypter à nouveau avec les clefs contrefaites et de les envoyer au destinataire.

RK : Alors que faire, pour savoir qui est vraiment qui au bout de la ligne ?

MR : La solution est de faire authentifier sa clef publique par une Autorité de Certification. Celle-ci va signer (digitale-ment, comme décrit plus haut) un document électronique liant (après vérification) l'identité d'une personne et sa clef publique. C'est ce document signé qu'on appelle le certificat de cette personne. Chacun vérifie à l'aide de la clef publique de l'Autorité de Certification la signature figurant sur le certificat du destinataire avant d'utiliser la clef publique correspondante pour chiffrer un message qu'il veut lui envoyer. Certes,



Stop! Swisskey l'annonce sur son site. Les certifications sont arrêtées au 1^{er} janvier 2002.

l'identité de la personne sera peut-être reconnue, mais cette personne peut bien se faire passer pour une autre. Comment le savoir ?

Les entreprises de certification demandent des extraits du Registre du commerce ou des numéros personnels, pas facilement transmissibles. La forme authentique est parfois exigée.

RK : Comment s'y prendre pour se faire authentifier ?

MR : Pour enregistrer une signature, il faut s'adresser à une entreprise de certification. Par exemple, chez www.globalsign.com, www.entrust.com, www.verisign.com, www.thawte.com.

RK : A quels développements peut-on s'attendre dans le marché et les technologies ?

MR : Le développement du commerce électronique est directement dépendant des signatures qu'il doit émettre. Autant pour l'échange de dossiers confidentiels que pour les

paiements en ligne. Le problème majeur n'est pas d'ordre technologique, mais réside plus dans l'adoption d'un registre de certificats d'authenticité de valeur mondiale.

En Suisse, Swisskey a stoppé l'émission de certificats numériques à la fin de cette année. Pour différentes raisons et parce que la demande n'a pas atteint le niveau attendu, selon l'entre-

RK : Comment faire au 1^{er} janvier 2002 pour obtenir un certificat suisse, en Suisse ? Et que vont advenir les anciens certificats suisses ?

MR : Les entreprises ou les particuliers suisses peuvent utiliser les services d'autorité de certification étrangère (voir ci-dessus). Les certificats délivrés par Swisskey perdront leur validité le 31 décembre 2001. Ils peuvent continuer à être utilisés pour certaines applications, sans garantie.

Roland Keller