1 L'Authentification de A à Z

1.1 Introduction

L'**Authentification** est la vérification d'informations relatives à une personne ou à un processus informatique. L'authentification complète le processus d'identification dans le sens où l'authentification permet de prouver une identité déclarée. Dans un serveur, un processus de contrôle valide l'identité et après authentification, donne l'accès aux données, applications, bases de données, fichiers ou sites Internet. Dans le cas contraire, l'accès est refusé.

L'authentification peut se faire de multiples manières, et notamment par la vérification de :

- « Ce que je sais », un mot de passe par exemple,
- « Ce que je sais faire », une signature manuscrite sur écran tactile/digital (de type PDA),
- « Ce que je suis », une caractéristique physique comme une empreinte digitale,
- « Ce que je possède », une carte à puce par exemple.

Le choix de telle ou telle technique dépend en grande partie de l'usage que l'on souhaite en faire : authentification de l'expéditeur d'un email, authentification d'un utilisateur qui se connecte à distance, authentification d'un administrateur au système, authentification des parties lors d'une transaction de **B2B** (Business to Business), etc.

La combinaison de plusieurs de ces méthodes (aussi appelées facteurs d'authentification) permet de renforcer le processus d'authentification, on parle alors d'authentification forte.

Les techniques d'authentification les plus usitées sont, de loin, les mots de passe mais aussi, de plus en plus, les **Certificats de clés publiques.**

1.2 Méthodes courantes d'authentification

1.2.1 Mots de passe

Les mots de passe pris dans leur ensemble sont le moyen d'authentification le plus répandu à ce jour. On distingue deux catégories : les mots de passe statiques et les mots de passe **Dynamiques**.

Les mots de passe statiques sont des mots de passe qui restent identiques pour plusieurs connexions sur un même compte. Ce type de mot de passe est couramment rencontré sous Windows NT ou Unix. Cette technique d'authentification est la plus utilisée dans les entreprises mais aussi la moins robuste. En fait, les **Entreprises** devraient restreindre l'usage des mots de passe statiques à une authentification locale d'un utilisateur car les attaques qui permettent de capturer un mot de passe qui circule sur un réseau sont nombreuses et faciles à mettre en pratique.

Pour palier les faiblesses de l'usage des mots de passe statiques, sont apparues des solutions d'authentification combinant deux facteurs (« ce que je possède » et « ce que je sais ») afin d'obtenir une authentification **Forte.** Les mots de passe sont obtenus par des **Générateurs** de mots de passe activés à l'aide d'un code d'identification personnel ou PIN (*Personal Identification Number*). La mise en place d'un tel mécanisme d'authentification forte rend la capture du mot de passe en cours d'aucune utilité puisque, dès que le mot de passe dynamique a été utilisé, celui-ci devient caduc. Parmi ces mots de passe à usage unique – One Time Password (OTP) en Anglais – on trouve notamment le programme SKEY dont la sécurité repose sur une fonction à sens unique et qui permet de générer un mot de passe différent pour chaque nouvelle connexion. En version logicielle, ces générateurs de mots de passe dynamiques utilisent certains composants du PC, comme le microprocesseur, le CPU ou l'**Horloge** interne (on parle alors de méthode d'authentification en mode synchrone dépendant du temps). Que le mot de passe à usage unique soit obtenu à partir d'un générateur matériel ou logiciel, l'utilisateur est authentifié de manière forte grâce à la vérification du mot de passe dynamique par un serveur appelé serveur d'authentification.

Afin d'éviter aux utilisateurs de retenir de nombreux mots de passe, il est possible de mettre en place un outil qui rende l'authentification de l'utilisateur unique pour chaque session : le Single Sign On (SSO).

Notons toutefois que la mise en place d'un SSO ne renforce en aucun cas la robustesse du processus de contrôle d'accès au SI, il sert juste de point d'entrée unique au SI : c'est une mesure pratique pour les

utilisateurs. Par conséquent, si ce point d'entrée venait à céder à la suite d'une malveillance, d'un disfonctionnement ou d'une attaque venant d'**Internet**, cela pourrait avoir des conséquences désastreuses pour la sécurité du SI de l'entreprise. Il est donc souhaitable de coupler le contrôle d'accès des utilisateurs au système d'information via un serveur SSO à une méthode d'authentification forte comme un mot de passe **Jetable** (i.e. mot de passe à usage unique), des certificats X.509 ou des systèmes biométriques, suivant le niveau de risque des informations auxquelles l'utilisateur nécessite un accès.

Par ailleurs, l'authentification peut aussi reposer sur un protocole d'authentification réseau, le protocole **Kerberos**, qui permet de sécuriser les mots de passe statiques lorsqu'ils sont transmis sur le réseau. Ce protocole, créé par le Massachusetts Institute of Technology (MIT), utilise la cryptographie à clés publiques.

1.2.2 Certificats de clés publiques

Comme nous venons de le voir, la cryptographie à clé publique peut être utilisée pour chiffrer des mots de passe. En outre, elle peut également être employée pour signer des données, qu'il s'agisse d'un contrat afin que les parties qui l'ont signé ne puissent pas en répudier le contenu a posteriori, ou qu'il s'agisse d'une valeur aléatoire pour assurer l'authentification.

En effet, les certificats de clés publiques sont l'une des techniques d'authentification les plus usitées à ce jour, certes loin derrière les mots de passe mais ce moyen d'authentification devient de plus en plus populaire.

La cryptographie asymétrique fait intervenir deux éléments qui sont mathématiquement liés entre eux : la clé privée et la clé publique.

La clé publique est :

- Disponible pour tout le monde.
- Utilisée par une personne qui souhaite authentifier l'émetteur d'un document électronique signé avec la clé privée. Le contrôle de la signature permet aussi de s'assurer de l'intégrité du fichier.
- Utilisée par une personne souhaitant chiffrer un message afin que ce dernier soit uniquement lisible par le possesseur de la clé privée associée.

La clé privée est :

- Conservée secrète par son possesseur.
- Utilisée par son possesseur pour signer un document électronique (message, contrat ou autre).
- Utilisée par son possesseur pour déchiffrer un message chiffré à son attention.

Connaissant la clé publique, il est impossible en un temps raisonnable, avec des moyens raisonnables (i.e. en une journée avec un seul PC), de deviner la clé privée associée. Mais avec des moyens conséquents et connaissant la clé publique, il est possible de retrouver la clé privée associée puisqu'en août dernier le défi RSA-155 proposé par la société américaine RSA Security Inc. a été relevé: une clé de 155 chiffres (ce type de clé est utilisé dans 95% des transactions de commerce électronique) a été cassée grâce à 300 machines en réseaux, ce qui est équivalent à 30 à 40 années de temps ordinateur (temps CPU). Ainsi, à ce jour, il est admis qu'en connaissant la clé publique il est impossible en un temps raisonnable avec des moyens raisonnables de deviner la clé privée associée : l'usage de clés asymétriques est jugée sûre.

L'Information Standard Organization (ISO) définit dans le standard ISO/IEC 7498-2 (Systèmes de traitement de l'information – Interconnexion de systèmes ouverts – Modèle de référence de base – Partie 2 : Architecture de sécurité), la signature numérique comme étant « des données ajoutées à une unité de données ou transformation cryptographique d'une unité de données permettant à un destinataire de prouver la source et l'intégrité de l'unité de données et protégeant contre la contrefaçon » (par le destinataire, par exemple).

Le principe de l'authentification de l'expéditeur d'un message grâce à l'usage de la signature numérique est le suivant : l'expéditeur calcule le *Message Authentication Code* ou MAC à l'aide d'une fonction « hash ». Puis, l'expéditeur signe le MAC avec sa clé privée. Le MAC signé est joint au message et l'ensemble est envoyé.

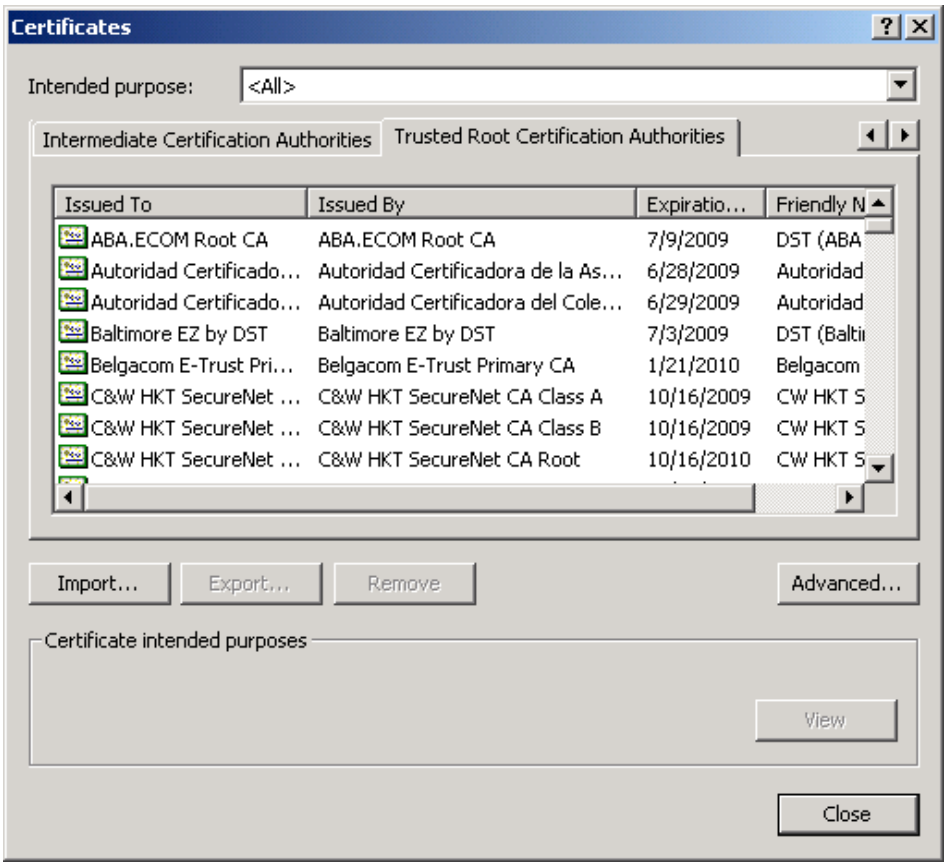
Le destinataire fait le « hash » du message reçu en utilisant le même algorithme que celui de l'expéditeur et compare ce MAC au MAC envoyé avec le message. S'ils ne sont pas égaux, cela signifie que le message a été altéré : la modification d'un seul bit pendant la transmission fait échouer le contrôle et permet d'alerter le destinataire. Plus qu'un mécanisme d'authentification de l'expéditeur d'un message, le MAC permet donc aussi de garantir l'intégrité du message.

La question qui nous assaille à cet instant c'est comment peut-on être sûr que cette signature (cf. modèle ci-dessous) est belle et bien celle de notre correspondant ?

```
BEGIN
SIGNATUREQCVAwUBMARe7gvyLNSbw6ZVAQF6ygP/fDnuvdAbGIDWaSMXUIs&»%k3MuNHYzdZOOcqkDh/Tc2+Dubu
Ea6GU03AgZY8K9t5r9lua34E68pCxegUz009b10cjNt6+o+704Z3j1yy9ijYM8BWNaSp9L2W4nUuWBdlWyel82Pj
jRVNZEtqtSRQuPEpJ2IHtx9tGevH10END SIGNATURE
```

Cette certitude naît de la relation de confiance liant l'expéditeur en question à son bi-clé (couple constitué d'une clé privée et d'une clé publique). Ce lien appelé certificat est, en fait, un fichier contenant les paramètres cryptographiques (algorithme utilisé, taille des clés, etc.) et les données d'identification de son possesseur, le tout signé par un tiers qui en a validé le contenu. Ce tiers est appelé autorité de certification (AC).

Maintenant que l'on peut avoir la garantie qu'une personne est bien celle qu'elle prétend être i.e. que la signature électronique de quelqu'un est bien de cette personne et que nous savons qu'il faut pour cela, vérifier le certificat X.509 (cf. RFC 2459 *Internet X.509 Public Key Infrastructure, Certificate and CRL Profile* pour plus de détails sur son contenu) associé à la clé de signature et/ou remonter la chaîne de certification jusqu'au certificat de l'AC racine (certificat auto signé), il reste à savoir où trouver ce(s) certificat(s). Dans les entreprises, les certificats de clés publiques sont stockés dans des annuaires **LDAP** (*Lightweight Directory Access Protocol)*. Pour un usage personnel de **MAC** ou autres applications utilisant la cryptographie asymétrique, les certificats des utilisateurs ainsi que de leur AC (et éventuellement, hiérarchie de certification jusqu'à l'AC racine) sont souvent stockés dans les **Navigateurs** (Microsoft Internet Explorer et Netscape Communicator). Ceux-ci comportent déjà par défaut un certain nombre de certificats d'AC racines (cf. Outils/Options internet/Contenu/Certificats).



Notons pour information, qu'une mesure de sécurité est d'effacer (*Remove*) ces certificats lors de l'installation et de ne rajouter que ceux autorisés par l'entreprise. Si vous souhaitez avoir vos propres

certificats d'authentification afin, par exemple, de faire des transactions en ligne, vous pouvez contacter un **Opérateur de Service de Certification (OSC)**. De nombreux OSC sont présents sur le marché français et européen.

1.2.3 Biométrie

Cf. article de P. Wolf dans la revue numéro 46.

1.2.4 Avantages et inconvénients des différentes techniques d'authentification

Le tableau suivant recense les principaux avantages et inconvénients de chacune des techniques d'authentification décrites précédemment :

	Avantages	**Inconvénients**
Mot de passe statique	+ peu coûteux + facile à mettre en œuvre + facile à utiliser	- vol du mot de passe en regardant par dessus l'épaule - oubli du mot de passe - peu robuste (facilement devinable ou « craquable ») - partageable, et trop souvent partagé - mot de passe rejouable par une personne malveillante
Mot de passe statique stocké dans une carte magnétique activée par code **PIN**	+ robustesse du mot de passe (possibilité de choisir un mot de passe aléatoire et comprenant des caractères spéciaux) + pas de nécessité de mémoriser le mot de passe	- vol, perte ou oubli de la carte - carte partageable - durée de vie du mot de passe souvent trop longue : nécessité de renouveler régulièrement l'enregistrement dans la carte - mot de passe rejouable
Mot de passe dynamique généré par un outil logiciel	+ robustesse du mot de passe (mot de passe souvent aléatoire et comprenant des caractères spéciaux) + confort d'utilisation pour l'utilisateur (absence de mémorisation du mot de passe)	- peu de confort d'utilisation (nécessité d'utiliser un logiciel à chaque nouvelle connexion) - protection de l'utilisation du logiciel par une personne non autorisée
Mot de passe dynamique généré par un outil matériel	+ confort d'utilisation pour l'utilisateur (absence de mémorisation du mot de passe) + robustesse du mot de passe (usage unique)	- vol, perte ou oubli du générateur de mot de passe - le générateur peut se désynchroniser avec le serveur qui contrôle la vérification du mot de passe
Certificat X.509 dans le navigateur de l'ordinateur	+ multi-usage + robustesse de la méthode d'authentification + confort d'utilisation pour l'utilisateur	- vol ou utilisation frauduleuse de l'ordinateur et copie de la clé privée associée au certificat
Certificat X.509 dans un token USB	+ multi-usage + robustesse de la méthode d'authentification + attitude similaire à la possession de clés (maison, voiture)	- vol, perte ou oubli du token

	Avantages	Inconvénients
Certificat X.509 dans une carte a puce	+ multi-usage + robustesse de la méthode d'authentification + attitude similaire à la possession d'une carte bancaire	- vol, perte ou oubli de la carte a puce
Biométrie et caractéristiques de référence dans une base de données en réseau	+ pas d'oubli ou de vol possible	- technologie encore immature - facilement falsifiable
Biométrie associée a une carte magnétique		- technologie encore immature - vol, perte ou oubli de la carte magnétique - coût élevé
Biométrie associée a un certificat X.509 dans un token USB	+ multi-usage + attitude similaire à la possession de clés (maison, voiture)	- technologie encore immature - vol, perte ou oubli du token USB - coût élevé
Biométrie associée a un certificat X.509 dans une carte a puce	+ multi-usage + attitude similaire à la possession d'une carte bancaire	- technologie encore immature - vol, perte ou oubli de la carte a puce - coût élevé

La **Qualité** d'une méthode d'authentification ne se mesure pas uniquement à ses avantages et inconvénients généraux ou à sa robustesse théorique face aux attaques mais avant tout à sa capacité à répondre aux besoins de sécurité de l'entreprise tout en prenant en considération le secteur d'activité dans lequel il est mis en place (son environnement) i.e. en tenant compte des risques mais aussi des contraintes techniques, organisationnelles, temporelles de même que financières et légales. En outre, le budget alloué à l'informatique en général et à la sécurité informatique en particulier, de même que la taille de l'entreprise et les compétences internes sont des facteurs très influents sur le choix de telle ou telle solution d'authentification. Comme toute solution de sécurité, le choix de la méthode d'authentification sera un compromis (parfois long à obtenir…).

L'authentification est l'un des domaines de sécurité qui engendrent le plus d'inquiétude au sein des entreprises, ce qui génère une réaction d'investissement afin de l'améliorer. Il est à noter que plus de la moitié des entreprises sont en train d'investir ou prévoient d'investir en 2003 dans le secteur de l'authentification (source IDC, 2002).

De manière générale, une des raisons principales des investissements des entreprises dans la sécurité informatique est guidée par le soucis de fournir aux utilisateurs un meilleur accès au réseau et un accès plus sécurisé car elles ont de plus en plus conscience de courir le risque d'être l'objet d'attaques de personnes malveillantes.

1.3 Protocoles d'authentification couramment utilisés

1.3.1 Protocole RADIUS

Le protocole **RADIUS** (Remote Authentication Dial-In User Service) développé par Livingston Enterprise et standardisé par l'IETF (cf. RFC 2865 et 2866) s'appuie sur une architecture client/serveur et permet de fournir des services d'authentification, d'autorisation et de gestion des comptes lors d'accès à distance.

Prenons le cas pratique d'un utilisateur nomade, souhaitant se raccorder via Internet au réseau interne d'une entité du CNRS par un canal protégé (circuit virtuel protégé CVP – *virtual private network VPN*). Le principe de l'authentification de cet utilisateur avec RADIUS est le suivant :

1. L'utilisateur exécute une requête de connection. Le routeur d'accès à distance (client RADIUS) récupère les informations d'identification et d'authentification de l'utilisateur (son identifiant et son mot de passe par exemple).
2. Le client RADIUS transmet ces informations au serveur RADIUS.
3. Le serveur RADIUS reçoit la requête de connexion de l'utilisateur, la contrôle, et retourne l'information de configuration nécessaire au client RADIUS pour fournir ou non l'accès au réseau interne à l'utilisateur.
4. Le client RADIUS renvoie à l'utilisateur un message d'erreur en cas d'échec de l'authentification ou un message d'accès au réseau si l'utilisateur a pu être authentifié avec succès.

1.3.2 Protocole SSL

Le protocole **SSL** (Secure Socket Layer) développé par Netscape Communications Corp. avec RSA Data Security Inc. permet théoriquement de sécuriser tout protocole applicatif s'appuyant sur TCP/IP i.e. HTTP, FTP, LDAP, SNMP, Telnet, etc. mais en pratique ses implémentations les plus répandues sont LDAPS et HTTPS.

Le protocole SSL permet non seulement de fournir les services d'authentification du serveur, d'authentification du client (par certificat à partir de SSL version 3) mais également les services de confidentialité et d'intégrité.

Le principe d'une authentification du serveur avec SSL est le suivant :

1. Le navigateur du client fait une demande de transaction sécurisée au serveur.
2. Suite à la requête du client, le serveur envoie son certificat au client.
3. Le serveur fournit la liste des algorithmes cryptographiques qui peuvent être utilisés pour la négociation entre le client et le serveur.
4. Le client choisit l'algorithme.
5. Le serveur envoie son certificat avec les clés cryptographiques correspondantes au client.
6. Le navigateur vérifie que le certificat délivré est valide.
7. Si la vérification est correcte alors le navigateur du client envoie au serveur une clé secrète chiffrée à l'aide de la clé publique du serveur qui sera donc le seul capable de déchiffrer puis d'utiliser cette clé secrète. Cette clé est un secret uniquement partagé entre le client et le serveur afin d'échanger des données en toute sécurité.

Afin d'éviter des attaques, il est recommandé d'utiliser la double authentification c'est-à-dire non seulement l'authentification du serveur mais également celle du client, bien que l'authentification du client avec SSL soit facultative.

Le protocole **TLS** version 1.0 (Transport Security Layer) est la version normalisée de SSL version 3.0 (cf. RFC 2246 de l'IETF). Les versions de TLS sont amenées à évoluer, au moins au fur et à mesure que de nouvelles attaques apparaissent. En Février dernier, une faiblesse majeure a été identifiée dans le protocole SSL : des chercheurs de l'Ecole Polytechnique de Lausanne ont montré qu'il est possible en moins d'une heure de trouver le mot de passe d'un internaute connecté à un service d'eCommerce. Que l'**URL** (*Uniform Resource Locator*) soit « sûre » ou pas, c'est-à-dire qu'une société dont la réputation n'est plus à faire héberge ce site Internet ou bien qu'il s'agisse d'une compagnie dont la sécurité des transactions n'est pas une priorité, la faille de sécurité basée sur une usurpation d'identité était bien présente pour les plates-formes Linux, Unix, Solaris et dérivés. L'information a été rapidement transmise à l'organisation OpenSSL afin de mettre à jour le protocole et développer une nouvelle **Version** de SSL qui résiste à cette attaque (cf. le site www.openssl.org pour les différentes mises à jour).

1.3.3 Protocole WTLS

Le protocole **WTLS** (Wireless Transport Layer Security) est la transposition du protocole TLS dans le monde des réseaux sans fil. Cependant, les négociations entre le client et le serveur ont été adaptées afin de

répondre aux contraintes du réseau « wireless ». Ainsi le nombre d'en-têtes du protocole WTLS est réduit par rapport au protocole SSL et le taux de compression est supérieur pour le protocole WTLS puisque la bande passante est plus faible.

Le principe d'une authentification utilisant WTLS est le suivant :

Les données échangées entre la passerelle WAP et un serveur Web sont codées en utilisant le protocole SSL ou TLS. La passerelle WAP gère la conversion entre WTLS et SSL/TLS. Cette étape de conversation est considérée comme critique car les données au format SSL/TLS sont décodées par la passerelle WAP qui les code ensuite au format WTLS. Les données entre le terminal mobile (PDA, téléphone GSM, etc.) et la passerelle WAP sont codées au format WTLS.

La passerelle WAP étant le cœur des échanges, il est essentiel d'en garantir la sécurité non seulement sur le plan logiciel mais également physique.

1.3.4 Protocole 802.1X-EAP

Le protocole 802.1X-EAP crée une structure standardisée pour l'authentification mutuelle entre un poste client et un élément du reseau tel qu'un commutateur réseau (hub), un point d'accès sans fil, etc. en s'appuyant sur un serveur d'authentification (souvent de type RADIUS) et l'un des protocoles EAP (*Extensible Authentication Protocols,* RFC 2284 et 2716) possibles. Après mutuelle authentification entre le client et le serveur, une clé est dérivée pour le chiffrement de la communication. Comme une nouvelle clé est dérivée par 802.1X pour chaque nouvelle session entre le client et le serveur, cela s'apparente à une gestion dynamique des clés.

1.4 Conclusion

Les systèmes d'authentification à base de certificats **X.509** semblent moins facilement attaquables et donc plus robustes que les systèmes basés sur les mots de passe. Mais un système jugé sûr aujourd'hui peut révéler des failles ou faiblesses demain. Nous nous souvenons de la chronique qui a fait la une de nombreux journaux en Fevrier 2000 racontant comment un informaticien a fabriqué une fausse carte à puce, appelée « **Yes card** », capable de tromper un automate distribuant des tickets de métro et mettant ainsi en exergue une vulnérabilité dans le système d'authentification du porteur de carte bancaire. Il est donc primordial de garder à l'esprit qu'une méthode d'authentification avec **Zéro défaut** n'existe malheureusement pas. La sécurité absolue est une utopie. Cependant il est possible de réduire à un degré tolérable le niveau de risque lié à une authentification permissive d'une personne non-autorisée à accéder au système d'information en mettant en place des solutions d'authentification forte. Toutefois, il est à noter que quelque soit la robustesse de la méthode d'authentification employée, la sécurité du système d'information ne doit pas uniquement reposer dessus. En effet, la sécurité est un tout et d'autres mesures de sécurité doivent compléter une méthode d'authentication forte, comme la mise en place de séances de sensibilisation à la sécurité informatique, la diffusion aux utilisateurs de la politique de sécurité du laboratoire ou de l'entreprise, le cloisonnement de certains réseaux, etc. (De nombreux exemples sont présentés dans l'article sur les tableaux de bord de la sécurité du système d'information du numéro 45 de la revue).

2 Mot de la fin

Bien qu'ayant adopté une approche de l'authentification allant de A à Z par le biais de mots clés, cet article n'est nullement exhaustif. Les avancées technologiques autorisent à penser que de nouveaux produits et de nouveaux protocoles d'authentification vont fleurir dans les mois à venir, notamment dans le monde du sans fil (Wi-Fi) où l'authentification (802.1X-EAP) devrait être un facteur clé de développement et de réussite. A suivre donc…

3 Références

3.1 Livres

1. « Authentication » par Richard Smith (Edition Addison Wesley)
2. "Sécuriser ses échanges électroniques avec une PKI - Solutions techniques et aspects juridiques" par Thierry Autret, Marie-Laure Oble Laffaire et Laurent Bellefin (Edition Eyrolles).

3.2 Article

« Smart card vs. Password » disponible sur http://www.scmagazine.com/scmagazine/2003_09/feature_1 (2eme article de la page)

3.3 Sites Internet

1. http://www.ietf.org/rfc
2. http://www.openssl.org
3. http://web.mit.edu/kerberos/www/

4 L'auteur

Caline Villacres – caline.villacres@ey.com

Ernst & Young LLP - Security & Technology Services

200 Clarendon Street, Boston MA 02116, USA