Sécurité: 'Les besoins et les moyens ont évolué'

Deux grandes approches coexistent, s'agissant des procédures de sécurité d'accès: soit on acquiert ses certificats à l'extérieur, soit on décide de les produire soi-même.

Car on voit apparaître des solutions d'authentification forte, avec des clés publiques comme PKI ou FIM (*Federated identity management*). En préambule à la RSA Security Conférence (*), qui se tient à Amsterdam semaine prochaine, le directeur de la filiale France constate que le marché des clés d'authentification (comme la clé publique PKI) change. La reprise économique se pointe à l'horizon et les entreprises réamorcent leurs investissements en sécurité. RSA, qui s'inscrit dans la seconde logique (donc, permettre aux entreprises de produire elles-mêmes leurs outils et de les intégrer) voit l'avenir plutôt en rose (**). On a vu il y a quelques années, constate Olivier Caffin, l'installation d'infrastructures PKI sans qu'il existât des applications permettant de les gérer. A l'inverse, aujourd'hui, on suit un grand compte du secteur des transports qui a récemment intégré un support carte à puce avec les offres de PKI. Avantage: le client ne s'est pas borné à choisir une technologie; il a tenu à la replacer dans le contexte de l'application concernée, à savoir la protection de sessions sur poste de travail, à l'international. Ici, le système carte à puce intègre la signature et le contrôle d'accès Web pour des applications transactionnelles. On voit aussi apparaître de gros projets en matière de gestion fédérative de l'identité (*federated identity management*). **Horizon 2004: une belle progression** Sur ces deux thèmes, l'année 2004 devrait s'avérer plus florissante que 2003 pour l'ensemble des fournisseurs d'offres du marché. Olivier Caffin parle d'un *« véritable rattrapage »*. Explications? Un bon nombre d'entreprises doivent gérer le « nomadisme » grandissant de leurs cadres. **Tendances fortes:** Bref, l'administration des identités pour accéder aux services (*identity access management*) correspond clairement à un besoin formulé par les entreprises. Celles-ci « découpent » toutefois cette administration en plusieurs lots: – le « *e-provisioning* » : il permet à un individu transitant entre plusieurs entreprises d'un groupe ou changeant de fonction, d'avoir un accès à des applications différentes tout en conservant son identité – la gestion fédérative de l'identité: un système permettant une identification unique dans le cadre de Web services ou d'applications inter-entreprises. – une réflexion autour de l'annuaire: un thème sur lequel nous reviendrons. Car l'annuaire participe de plus en plus activement à la stratégie informatique de l'entreprise via son rôle central lié à l'administration et à la sécurisation du système d'information. _____ (*)RSA Conference, du 3 au 5 novembre, Amsterdam. Principaux thèmes: – Sécurité appliquée; développement d'applications sécurisées; piratage et menaces informatiques; mise en ?uvre de la sécurité; périmètre de défense; respect de la vie privée; lois et politique; sécurisation des Services Web. https://www.rsaconference.com/rsa2003/europe/agenda_body.html _____ (**) RSA se définit comme un spécialise de la gestion de l'identité et des accès. Ses compétences concernent les systèmes d'authentification forte mais aussi la signature électronique et la génération de certificats PKI. Dans le cas du contrôle d'accès, ses solutions permettent une supervision interne ou externe -vision globale intégrant des approches liées à l'utilisation d'annuaires et du processus de signature unique (*single sign on*). Un nouveau module, baptisé *Federated identity Management*, autorise, comme dans Passport de Microsoft, qu'une authentification effectuée dans un environnement soit renvoyée sur d'autres services, évitant ainsi à l'utilisateur de

justifier en permanence son identité lorsqu'il progresse d'un service Web à un autre. **Le cycle de vie de la sécurité des accès**

Il ne faut surtout pas croire qu'une infrastructure à clés publiques ne nécessite aucune administration. C'est en fait tout l'inverse puisque chaque certificat étant indivualisé, il est nécessaire que celui-ci suive la même « carrière » que son propriétaire et donc éventuellement disparaisse lorsque ce dernier quitte l'entreprise ou évolue vers des fonctions nécessitant un autre type d'accréditation. En règle générale, on distingue six grandes phases dans la vie d'un certificat 1- Enregistrement du certificat La naissance du certificat fourni par une autorité de certification se déroule en plusieurs étapes. – la demande de certificat auprès de l'organisme chargé de cette fonction ; – la vérification de l'identité du demandeur ; – la génération d'une paire clé privée/clé publique Nota : la façon dont ces différentes étapes sont accomplies et par quelle autorité peut varier d'une application à l'autre. 2 – Génération du certificat Une fois la demande d'enregistrement traitée par l'autorité de certification, celle-ci génère le certificat. Toutefois, pour que celui-ci ait force probante, il est indispensable que l'autorité de certification ait répondu à un certain nombre de critères de validation de son autorité, tant sur le plan de son mode de fonctionnement que sur celui des informations qu'elle doit impérativement demander au demandeur de certificat. Une fois la signature délivrée par l'autorité de certification, le document certifié et les clés ont valeur probante, notamment en matière de non répudiation. 3 – Publication du certificat Le certificat ayant désormais force probante, il convient de le publier ou de le diffuser. Là encore, la façon dont le certificat est distribué peut varier d'une application à l'autre. Dans la plupart des environnements PKI, le certificat sera délivré par la CA puis publié dans un répertoire. 4 – Révocation du certificat Le départ d'un employé, la compromission d'une clé, une fusion amenant à utiliser une application de certification d'un format différente sont autant de raisons pour procéder à la révocation d'un certificat. Le système PKI doit donc fournir les moyens nécessaires à cette révocation et permettre notamment de vérifier le statut et la validité des certificats d'autres entités. Les deux méthodes les plus couramment utilisées sont d'une part les listes de révocation de certificats via un annuaire LDAP et de l'autre le protocole OCSP (

Online Certificate Status Protocol). 5 – Expiration du certificat Les clés et les certificats se voient affectés une durée de vie donnée. Lorsque la clé arrive presque à échéance, il est nécessaire d'éditer une nouvelle paire clé privée/clé publique ainsi qu'un nouveau certificat (opération de mise à jour de la clé). Selon la règle procédurale mis en place, on lancera alors une des trois actions suivantes lors de l'expiration : – aucune action (la clé est définitivement expirée); – renouvellement de certificat (on utilise la même clé publique qui est placée dans un nouveau certificat ayant une nouvelle durée de validité); – mise à jour du certificat (la paire de clés ainsi que le certificat sont tout deux renouvelés et publiés). 6 – Archivage du certificat Enfin, outre les opérations précédemment mentionnées, il est aussi possible d'archiver les certificats à des fins d'audit ou pour permettre de résoudre certains litiges.