SÉCURITÉ INFORMATIQUE

numéro 24 avril 1999

SÉCURITÉ DES SYSTÈMES D'INFORMATION

Libéralisation de l'utilisation de la cryptologie…

éditorial

L'annonce faite, le 19 janvier dernier, par le Premier ministre, de la libéralisation de l'usage de la cryptologie, a été saluée de manière quasi unanime tant en France qu'à l'étranger. Chacun se réjouit en effet de pouvoir choisir librement son procédé cryptologique parmi ceux qui affichent, exprimée en nombre de bits, la clef la plus longue.

Aujourd'hui, l'utilisateur est seul maître de son choix, lorsqu'il en existe un, et seul responsable de l'usage qu'il fait de la cryptologie.

Si pour des organismes parfaitement rompus à l'utilisation de ces techniques, conscients des contraintes qu'elles imposent, des pièges qu'elles recèlent et de la limite de leur efficacité, cette tâche et cette responsabilité ne posent guère de problèmes, qu'en est-il pour le profane qui a découvert la cryptologie dans *Que sais-je ?* ou même dans le livre de Bruce Schneier ? Ce cryptologue reconnu internationalement n'a-t-il pas avoué lui-même, après avoir révélé une multitude de malfaçons dans les produits des plus grands éditeurs, que le drame est que rien ne ressemble plus à un bon procédé cryptologique qu'un mauvais ! et que, finalement, il regrettait d'avoir vulgarisé des notions de cryptologie laissant croire qu'on a tout compris au moment où tout se complique.

Nous savons que la cryptologie n'est pas la panacée à tous les maux. Ensuite, qu'elle n'est pas simple à mettre en œuvre. Enfin, que la force d'un procédé cryptologique ne se résume pas à la longueur de sa clef…

La sélection d'un tel dispositif, s'intégrant dans un système défini et répondant à ses besoins réels, exige un travail rigoureux et un niveau d'expertise élevé. Sinon, gare à ceux qui vous vendront du pseudo 128 bits, à la portée d'un pirate débutant ! Mais gare, également, aux produits plus finement affaiblis offrant un accès réservé à quelques privilégiés.

Certains l'ont déjà compris. C'est pourquoi le SCSSI est, d'ores et déjà, très sollicité par des utilisateurs qui cherchent leur voie à travers ce nouveau champ de liberté.

Général Jean-Louis Desvignes
Chef du Service central de la sécurité des systèmes d'information (SCSSI)

CENTRE NATIONAL DE LA RECHERCHE SCIENTIFIQUE

De l'usage de la cryptologie

La plus grande partie des transactions qui sont faites en vis-à-vis, ou par le support du papier, le seront bientôt par le truchement des médias électroniques. La facilité d'emploi, de transmission et de traitement des informations électroniques va en augmenter l'usage dans tous les domaines. Pour l'instant, la consultation de sites Internet et le courrier électronique sont les applications les plus répandues – et déjà un besoin de protection se fait sentir.
Que ce soit pour échanger des informations sur un brevet avant qu'il ne soit déposé ou pour accéder à une banque de données médicales, on exige un certain secret. Pour envoyer un ordre ou un bon de commande numérique, il est essentiel que l'identité de l'émetteur soit garantie. Quand le porte-monnaie électronique nous permettra de régler tous nos achats, pour respecter la vie privée, c'est-à-dire, ici, l'anonymat dans la vie courante, il faudra empêcher que toutes les opérations ne soient liées à une personne.
Tous ces besoins, donnés à titre d'exemple, sont essentiellement couverts par une partie bien spécifique de la sécurité des systèmes d'informations : la cryptologie.

Que recouvre la cryptologie ?

La cryptologie est à la fois une science et une technologie. Science, dont les principes les plus récents sont encore l'occasion de nouvelles découvertes. Technologie, utile et nécessaire dans l'industrie de la sécurité et pour tous ceux qui veulent protéger leur information.
La cryptologie couvre couramment quatre grandes fonctions de sécurité :

1. L'authentification

Il s'agit de garantir l'origine d'une information. En général, on utilise la signature numérique avec un couple de clés dont celle permettant de créer les signatures est gardée secrète, et dont l'autre permettant de vérifier la signature

suite page 2

suite de la page 1

est rendue publique. Le courrier électronique, un bon de commande transmis en ligne, un acte administratif peuvent être signés pour prouver leur origine et engager le signataire, à l'identique d'un paraphe sur le papier.
La signature numérique n'a réellement pris son sens qu'avec la découverte des systèmes de cryptologie dit «asymétriques». On peut diffuser largement le moyen de vérifier une signature sans risque de donner le moyen d'en contrefaire. Cependant les principes mathématiques employés sont récents, et si l'utilisation de la signature numérique est maintenant techniquement possible, l'édifice juridique et les usages courants ne sont pas encore adaptés à son utilisation. Divers travaux internationaux au sein de la Communauté européenne ou de l'OCDE tentent d'amorcer une évolution favorable à la reconnaissance juridique universelle des signatures numériques.

2. L'identification

Il s'agit de garantir l'identité et la qualité d'une personne qui souhaite accéder à des informations ou à des ressources matérielles. En général, on utilise le contrôle d'accès par mot de passe. Pour consulter son courrier électronique, pour se connecter à un ordinateur distant, ou pour entrer dans un lieu protégé, on peut ainsi s'assurer de l'identité du demandeur.
Ce problème est souvent négligé. En particulier, on voit encore trop de mots de passe circuler en clair sur les réseaux. Lors d'une ouverture de session ftp, ou telnet, **vous êtes-vous déjà demandé comment est protégé le mot de passe que vous entrez sur l'ordinateur en local ?** Dans la majorité des cas, il est simplement envoyé au serveur, risquant sur son trajet d'être attrapé par un «renifleur» et de finir dans la base de mots de passe d'un pirate qui se fera un plaisir de l'utiliser pour toutes sortes d'accès illégaux. Il conviendrait d'améliorer rapidement les méthodes de contrôle d'accès, mais, paradoxalement, c'est un des domaines de la sécurité où l'évolution est des plus lentes. Pourtant il existe des solutions, qu'il serait bon de valider au plus vite. Des techniques de cryptologie relativement simples, comme le défi réponse, permettent de ne pas diffuser l'information clé réutilisable, que cela soit un mot de passe ou une clé plus complexe sur un support physique.

3. La confidentialité

Il s'agit de garantir le secret de l'information transmise ou archivée. En général, on utilise le chiffrement au moyen d'une clé symétrique (*cf.* page 5 : «La révolution de la cryptologie asymétrique»). Tout, du courrier électronique aux commandes d'administration d'un ordinateur à distance, peut être ainsi protégé sous une forme chiffrée.
Trop souvent, la cryptologie est limitée dans les esprits à cette fonction de protection de la confidentialité. Sans doute des raisons historiques ne sont pas étrangères à cette confusion. En effet, pendant des siècles, c'est à peu près le seul usage qui en était fait. Déjà au Moyen Age, les grands stratèges et l'église utilisaient des formes élémentaires de chiffrement, dans le dessein de cacher le contenu de messages qui traversaient les lignes ennemies ou transitaient sur des terres hostiles.

4. L'intégrité

Il s'agit de garantir l'intégrité, c'est-à-dire l'absence de modification d'un message ou d'un document. On peut utiliser la signature numérique sous sa forme symétrique ou asymétrique, ou encore le chiffrement. Il est particulièrement important que, dans toute négociation et accord contractuel, on puisse vérifier qu'aucune modification du document électronique n'a été faite.
La cryptologie s'intéresse aussi à d'autres problèmes dont l'importance va croissant, comme la non-répudiation – garantissant que l'auteur d'un message ou d'un document ne peut pas nier l'avoir écrit et, le cas échéant, transmis –, l'anonymat (ou la non-traçabilité). La technologie peut rendre nombre de services, mais il lui est aussi possible de protéger l'individu de ses propres abus (*cf.* en encadré «Illusion de l'anonymat»).

Illusion de l'anonymat

Certains semblent penser que la large diffusion de la cryptologie suffira à la protection de la vie privée. Ce n'est malheureusement pas aussi simple. Certes le chiffrement peut cacher des informations, mais la signature, elle, ajoute une identification claire de l'émetteur d'un document, par exemple d'un courrier électronique. Les protocoles sécurisés de commerce électronique portent inévitablement des références des vendeurs et acheteurs, plus ou moins bien protégées. D'autres protocoles permettent, sans en casser la sécurité, d'obtenir des détails sur les interlocuteurs.
Toutes ces informations transitant sur les réseaux peuvent énormément simplifier la collecte et le traitement des données concernant un individu particulier. Si certains s'interrogent sur le droit à l'anonymat, d'autres pensent que chacun a le droit d'acheter un livre ou un journal sans être référencé pour autant dans une base de données. Si l'on veut dans l'avenir permettre des transactions à la fois sûres et anonymes – en particulier dans le commerce électronique –, il faudra faire appel à des principes cryptologiques d'une complexité bien supérieure au simple chiffrement. ■

Plus qu'un ensemble de principes mathématiques, un savoir-faire

Pour assurer correctement l'ensemble de ces fonctions de sécurité, il ne suffit pas de mettre les uns à côté des autres des algorithmes sans réflexion préalable particulière. La diffusion d'une certaine connaissance cryptologique dans le domaine public, et en particulier sur Internet, a donné l'illusion de la facilité. Le livre de Bruce Schneier *Applied cryptography* en est le meilleur exemple. Se voulant, dans un premier temps, le chantre de la liberté de diffusion de l'information, Bruce Schneier a rassemblé dans son livre une somme de connaissances sur les algorithmes cryptologiques, donnant leur description, leurs conditions d'utilisation, leur limite connue de solidité… Son aspect relativement linéaire et simple tend à faire croire à la lecture que l'implémentation de tous ces principes est simple. Il est intéressant de savoir que depuis, lors de certaines de ses conférences, Bruce Schneier avoue lui-même avoir fait plus de mal que de bien à la sécurité, créant cette illusion de facilité. Il décrit de manière imagée mais fort juste qu'il existe deux types de cryptologie : celle qui empêche votre petite sœur d'accéder à vos fichiers, et celle qui empêche les services étrangers d'écouter et de manipuler vos informations. La vraie difficulté est de passer du premier au deuxième type de cryptologie. Dans ce contexte, le défi, que nous rencontrons chaque jour au SCSSI, est d'aider la France à entrer dans la société de l'information avec un bon niveau de sécurité.

Petit Glossaire

Le vocabulaire de la cryptologie pose parfois quelques problèmes, en particulier à cause des anglicismes qui ont pu s'y glisser. Voici quelques termes :

➨ *CHIFFRER :*
transformer à l'aide d'une convention secrète, appelée clé, des informations claires en informations inintelligibles pour des tiers n'ayant pas la connaissance du secret ;

➨ *DÉCHIFFRER :*
retrouver les informations claires, à partir des informations chiffrées en utilisant la convention secrète de chiffrement ;

➨ *DÉCRYPTER :*
retrouver l'information intelligible, à partir de l'information chiffrée sans utiliser la convention secrète de chiffrement.

Par contre, crypter ou encrypter n'ont pas de sens clairement défini, mais sont parfois utilisés à tort comme synonymes de chiffrer. ■

Quelle que soit la fonction de sécurité recherchée à travers l'utilisation de la cryptologie, il convient de faire appel à des outils sûrs et adaptés.
Pour assurer la confidentialité, la simple observation de la longueur de la clé n'est pas suffisante. L'étude de l'algorithme utilisé, c'est-à-dire sa cryptanalyse, est indispensable. Les exemples sont nombreux de méthodes inattendues d'attaque d'algorithmes jugés dans un premier temps comme sûrs. Citons pour l'exemple RC3, algorithme de chiffrement, qui, «cassé» en interne, n'est jamais sorti de RSA Data Security, Safer, algorithme de chiffrement de Massey pour Cylink, dont une cryptanalyse réaliste a été présentée en 1997, et SHA, standard de condensation américain, qui a été modifié après sa diffusion pour compenser une erreur de conception. Quand on a acquis une confiance raisonnable en la solidité d'un algorithme, il faut encore s'assurer de sa bonne utilisation dans un produit, logiciel ou matériel. Il convient de définir précisément les parcours de l'information secrète, la gestion des clés, les protocoles d'échanges dans les cas de transmissions…
Il est simple, en oubliant la question de l'interface homme-machine, de faire un logiciel chiffrant des fichiers sur un ordinateur en local. Il est, à l'opposé, très difficile de mettre au point une infrastructure permettant de certifier, distribuer et gérer dans le temps les clés de milliers de personnes qui doivent échanger des messages avec un bon niveau de confidentialité et d'authentification. La moindre faille peut compromettre l'ensemble des secrets des intervenants. La question de ces grandes infrastructures de gestion de clés est un des défis des quelques années à venir.
Même pour l'identification, les principes retenus doivent être adaptés au besoin. Un simple code de quatre chiffres suffit pour déverrouiller un GSM ou une transaction de paiement par Carte Bleue. En revanche, l'administration à distance d'un gros calculateur ou d'un pare-feu devrait faire appel à des méthodes d'une autre robustesse, où la possession d'un support physique – comme une carte à puce – et d'un mot de passe est indispensable. Malheureusement, la grande majorité des connexions dans le monde Unix et Internet n'utilisent que la protection par mot de passe envoyé au serveur encore trop souvent en clair.
Enfin l'intégrité est assez souvent prise en compte au titre de la sûreté de transmission plus qu'en terme de sécurité. On se contente alors d'utiliser des codes correcteurs d'erreur dont la finalité n'est que de contrer certaines erreurs aléatoires et involontaires de transmission sur des supports physiques de qualité inégale. Mais, dans certains cas, il faut aussi se garantir contre les modifications volontaires, par exemple lors de la transmission de montants financiers ou de commande d'une centrale électrique.
Ces exemples montrent qu'au-delà des algorithmes utilisés, il faut faire appel à un vrai savoir-faire pour concevoir et réaliser des produits de sécurité, quelles qu'en soient les fonctions attendues. On est loin d'une simple classification en fonction du nombre de bits d'une clé. **L'architecture est essentielle.** Selon le cadre d'utilisation, les protocoles sont plus ou moins adaptés. Même le séquencement des opérations peut être déterminant pour la sécurité d'un édifice cryptologique. Doit-on identifier d'abord le correspondant, ou négocier les fonctions cryptologiques utilisées ? Doit-on avoir un mode dégradé en cas d'échec de négociation ? Des questions de fond se posent à chaque moment de la conception des produits, et cette réflexion doit accompagner l'ensemble du cycle de développement.

Comment trouver le bon produit de cryptologie ?

S'il apparaît qu'il n'est pas si facile de faire un bon produit de cryptologie, malheureusement il est aussi très difficile de distinguer les bons produits des mauvais. En l'absence d'informations précises, il est même impossible à l'expert de se prononcer. Il faut en faire une analyse poussée tant au niveau des principes et objets cryptologiques utilisés qu'au niveau de leur mise en œuvre pratique. La garantie d'un savoir-faire, mais aussi une grande ouverture et transparence de la part du concepteur sont des conditions essentielles de la réussite de ce processus de sélection en connaissance de cause.
Être connu et reconnu ne suffit pas. Dans les produits que l'on peut facilement trouver sur le marché, bon nombre ne méritent

Quelques adresses utiles :

On retrouve un certain nombre d'explications ainsi que le discours intégral du Premier ministre, à l'adresse du site gouvernemental : http://www.internet.gouv.fr/francais/frame-actualite.html#Regulation

La page donnant la liste des derniers décrets et arrêtés sur la cryptologie ainsi que les liens vers les documents complets à : http://www.internet.gouv.fr/francais/commerce/textesref.htm#1
ou http://www.internet.gouv.fr/francais/textesref/cryptodecret99199.htm

Décret n° 99-200 du 17 mars 1999 définissant les catégories de moyens et de prestations de cryptologie dispensées de toute formalité préalable :
http://www.internet.gouv.fr/francais/textesref/cryptodecret99200.htm

Un article très instructif de Bruce Schneier A LIRE ABSOLUMENT, à l'adresse :
http://www.counterpane.com/pitfalls_french.html. ■

pas forcément la confiance que semble créer leur notoriété. Voyons quelques cas typiques :

Lotus Notes

Ce logiciel, outre ses fonctionnalités de «*groupware*» qui en font un des leaders du marché, était censé assurer un chiffrement avec une clé de 64 bits. Les fonctionnaires suédois avaient trouvé cela suffisant pour certaines de leurs informations. Quelle ne fut pas leur déconvenue quand ils apprirent que 24 bits étaient disponibles sans effort pour les autorités américaines qui n'avaient plus qu'à chercher par examen exhaustif les 40 autres bits.

SSH

Voulant adapter ce protocole de connexion sécurisée pour en rendre l'utilisation libre avec une clé de 40 bits, Bernard Perrot de l'IN2P3 a revu l'ensemble du code standard de SSH, pour en tirer SSF. Il y a trouvé des failles, dont une importante. (*Cf. Sécurité Informatique* n° 23, février 1999). Personne avant lui ne l'avait relevée. Comme quoi, même la possibilité d'avoir accès au code d'une application sur Internet ne prouve rien si l'on ne l'examine en confiance, de façon systématique et complète (évaluations de sécurité).

PGP

Ce produit a longtemps été un symbole de la cryptologie libre incassable même par les grandes puissances. Toutefois la multiplication des versions, dont certaines sont dites internationales, et la complexité du code rendent difficile, si ce n'est impossible, un examen systématique et poussé. La plupart des personnes qui font confiance à PGP n'ont jamais revu le code source et encore moins recompilé l'exécutable. De plus, quelle que soit la qualité de l'implémentation, la certification des clés en anneau est modérément sûre. Enfin certains virus spécialisés semblent être capables de faire fuir sur Internet la clé privée d'un utilisateur de PGP.

Dans ce flou qui ne fait que grandir avec l'offre, des instructions interministérielles régissent la sélection et l'usage de produits de cryptologie pour les emplois gouvernementaux, c'est-à-dire dans toutes les parties de l'administration. Que cela soit pour le classifié de Défense ou pour les informations sensibles, comme certaines données financières ou personnelles, le circuit d'approbation technique et administrative est défini. Il ne s'agit pas d'empêcher l'utilisation de cryptologie, comme certains tendent à le faire croire, mais bien d'en favoriser un déploiement le plus efficace possible. Nous avons besoin de protéger nos informations, il s'agit de notre richesse. Si la définition du besoin et des objectifs de sécurité associés est un problème complexe, s'assurer de la qualité d'un produit de cryptologie ne l'est pas moins. Le développement de relations étroites entre les entités étatiques et les industriels permettra de faire croître le savoir-faire et la connaissance du besoin des utilisateurs, et donc de générer une offre de qualité. Alors seulement pourra-t-on obtenir la seule chose recherchée à travers la cryptologie : **la confiance.**

Jean-Séverin Lair
Chef de la Division Chiffre - SCSSI

Pour en savoir plus

Pour toute question complémentaire, contacter le SCSSI, 18, rue du Dr-Zamenhof 92131 Issy-les-Moulineaux. Tél. : 01 41 46 37 00. ■

Les Infrastructures de Gestion de Clés

Le besoin

Les nouveaux types d'applications (commerce électronique, messageries électroniques transitant sur des réseaux ouverts), les nouvelles configurations de réseaux (réseaux ouverts, apparition de matériels tels que des routeurs, firewalls, etc.) ont fait évoluer les besoins de sécurité des systèmes d'information.

Aujourd'hui, les utilisateurs mettent en œuvre des opérations de plus en plus complexes à partir de leur propre poste de travail et souhaitent voir la sécurité au plus près de leurs applications.

La cryptographie est une science qui répond aux besoins de sécurité des systèmes d'information. La cryptographie symétrique, qui implique une gestion contraignante de secrets appelés clés, s'adapte difficilement aux réseaux ouverts où un utilisateur ne connaît pas forcément son interlocuteur, utilise un canal de communication publique, ou échange des informations avec une communauté d'utilisateurs importante. La cryptographie asymétrique, quant à elle, facilite la gestion des clés puisqu'elle permet de sécuriser des communications sans qu'aucun échange de secret préalable ne soit nécessaire.

En effet, le principe de la cryptographie asymétrique consiste à utiliser un couple de variables cryptographiques appelées clés. Ce couple, appelé bi-clé, est composé d'une première clé dite privée qui doit rester secrète et dont seul son propriétaire a la connaissance et l'usage. La clé publique, quant à elle, peut être publiée mais doit impérativement rester intègre.

Ainsi dans un modèle d'intégrité, la fonction de sécurité est mise en œuvre par l'initiateur de l'échange par signature d'un document grâce à sa propre clé privée, de sorte que son interlocuteur puisse vérifier la signature en utilisant la clé publique correspondante. Dans un modèle de confidentialité, un premier correspondant utilise la clé publique de son interlocuteur de sorte que seul cet interlocuteur puisse déchiffrer le message sécurisé grâce à sa propre clé privée.

Grâce à ces systèmes asymétriques, divers types d'applications peuvent être sécurisés, comme, par exemple, la messagerie électronique, le commerce électronique, l'accès à des serveurs d'informations (Web), la gestion d'infrastructures réseaux (routeurs, chiffreurs…), etc.

Une infrastructure de confiance

Selon l'utilisation faite de la cryptographie asymétrique, il est possible d'assurer des fonctions de sécurité d'authentification de l'origine d'un message, de détection de perte d'intégrité, de non-répudiation d'une action et de protection de la confidentialité. Mais ces fonctions de sécurité ne peuvent être garanties que si l'auteur est bien le seul détenteur du secret qu'est la clé privée.

…… *suite page 5* ……►

suite de la page 4

De même, la sécurité du système fait appel à la confiance dans la relation qui lie l'utilisateur à un bi-clé. Un bi-clé est caractérisé par des paramètres cryptographiques (longueur de clé, période de validité, algorithme) tandis que l'utilisateur dispose d'une identité propre, d'une fonction, etc. pour une période donnée. L'ensemble de ces paramètres relatifs au bi-clé et à l'utilisateur est contenu dans un fichier appelé certificat de clé publique.
Pour que la relation entre l'utilisateur et le bi-clé soit de confiance, il est indispensable que le certificat soit signé par un tiers qui cautionne la véracité des informations contenues dans le certificat. Cette autorité est appelée autorité de certification (notée AC) et signe avec sa propre clé privée le certificat de clé publique.

Qu'est-ce qu'une infrastructure de gestion de clés ?

L'ensemble des ressources mises en œuvres pour sécuriser des bi-clés par la génération et la gestion complète de certificats de clés publiques est appelé infrastructure de gestion de clés (noté IGC).

Une IGC est un système distribué constitué de :
– ressources informatiques (matérielles, logicielles, réseau),
– ressources cryptographiques,
– ressources humaines (personnels de l'infrastructure).

Ces ressources agissent pour le compte d'utilisateurs finaux pouvant être des personnes, des organismes, des matériels ou d'autres composantes d'une infrastructure. Différents types de composantes tels que des autorités de certification, des autorités d'enregistrement, un service de publication, éventuellement un horodateur, interagissent pour offrir aux utilisateurs finaux des services de confiance. Au sein d'une infrastructure, la confiance se transmet par héritage, de composante à composante.
Les prestations réalisées par une IGC sont l'enregistrement d'un utilisateur, la génération de certificats, la publication et la révocation de certificats, ainsi que d'autres services qui peuvent varier selon les besoins.
L'enregistrement, service rendu par une autorité d'enregistrement, consiste en la vérification d'informations propres au demandeur de certificat, avant la génération de son certificat.

Après l'enregistrement, le gabarit d'un certificat est transmis pour signature à l'autorité de certification. Cette dernière génère le certificat et le transmet au service de publication, afin de le rendre disponible aux utilisateurs potentiels de la clé publique qu'il contient.
Les certificats sont publiés par le biais d'un vecteur de publication pouvant être une disquette, un document papier, un serveur d'information ou un annuaire.
Lorsqu'un utilisateur perd ou divulgue sa clé privée ou que les informations contenues dans son certificat sont ou deviennent fausses (falsification de l'identité, perte d'intégrité de la clé publique contenue dans le certificat), alors le certificat n'est plus de confiance et son utilisation ne peut plus garantir aucune fonction de sécurité. Il est alors révoqué par l'autorité de certification et son nouveau statut est transmis au service de publication.
Un utilisateur n'accorde sa confiance à une signature numérique que s'il a confiance dans le certificat qu'il utilise pour la vérifier et, par extension, dans le générateur de certificat, c'est-à-dire à l'ensemble de l'infrastructure.

Les enjeux

Toute la problématique des IGC réside dans :
– L'adéquation des services rendus par l'IGC aux besoins réels des utilisateurs.
Les spécification techniques doivent couvrir les besoins des applications sécurisées grâce à l'IGC et répondre aux attentes des utilisateurs finaux.
D'autre part, les solutions opérationnelles mises en œuvre doivent tenir compte de l'existant et proposer des solutions réalistes du point de vue des coûts et des ressources humaines disponibles.
– Le niveau de confiance généré par l'IGC et la possibilité de fournir des indicateurs de confiance aux utilisateurs finaux et aux partenaires de l'infrastructure.

En tant que générateur de confiance, une IGC doit disposer des procédures de fonctionnement interne, de politiques de certification, de déclarations quant aux services effectivement rendus et de spécifications techniques précises. Ces informations caractérisent l'infrastructure et fournissent des indicateurs sur le niveau de confiance à accorder à l'infrastructure. Cette confiance doit être démontrée aux utilisateurs des ser-

suite page 6

La révolution de la cryptologie asymétrique

Jusqu'à la fin des années soixante-dix, la cryptologie ne connaissait que les systèmes que l'on appelle maintenant «à clé symétrique». Il s'agit de systèmes où la clé de chiffrement identique à la clé de déchiffrement doit rester absolument secrète. C'est le cas par exemple de l'algorithme DES.
Mais, en novembre 1976, W. Diffie et M.E. Hellman ont émis l'idée de systèmes à clé non-symétrique (1). Il s'agissait là d'une révolution conceptuelle, dont l'exemple le plus connu est l'algorithme RSA, du nom de ses auteurs Rivest, Shamir et Adleman (2). Dans ces systèmes, comme le nom l'indique, les clés de chiffrement et de déchiffrement sont différentes. Plus précisément, la connaissance de l'une ne doit pas permettre en pratique de retrouver l'autre. Ces systèmes sont aussi appelés «à clé publique», une des deux clés pouvant être publiée sans nuire au secret de l'autre. Avec un tel système, n'importe qui peut envoyer à A un message chiffré. Il suffit pour cela d'utiliser la clé publique de A. Seul ce dernier, ayant sa clé privée, aura la capacité de le déchiffrer. Par ailleurs, si A veut signer un message, il lui suffit cette fois d'utiliser sa clé privée pour chiffrer un condensé du message. Alors toute personne pourra déchiffrer la signature à l'aide de la clé publique et vérifier qu'il s'agit bien du condensé du message signé.
Ces principes paraissent au premier regard quasi miraculeux, mais ils ont aussi un coût. Tout d'abord, les clés et les blocs élémentaires de chiffrement sont en général plus longs (environ 1000 bits) que dans les systèmes symétriques (environ 100 bits), même si des nouveaux algorithmes comme les courbes elliptiques tendent à faire disparaître cette différence. La complexité de calcul d'un chiffrement est beaucoup plus grande que dans les systèmes symétriques. De plus, les systèmes asymétriques reposent sur des problèmes mathématiques, comme la factorisation des grands nombres, où aucune solution radicale n'a été «encore» trouvée. Tout le problème est dans le «encore», car chaque jour la recherche mathématique fait des progrès dans ces domaines qui deviennent l'enjeu de compétitions.
Enfin la notion de clé publique ouvre d'autres horizons et appelle certaines questions dont la principale est : comment être sûr que la clé publique de A est bien celle que je trouve dans l'annuaire ? On arrive alors au problème épineux de la gestion, de la certification des clés dans les «Infrastructures de Gestion de Clés»…

(1) Diffie, W., Hellman, M.E. «New Directions in Cryptography». *IEEE-IT, 22*, n° 6, Nov. 1976.
(2) Rivest, R., Shamir, A., Adleman, L. «A Method for Obtaining Digital Signatures and Public-Key Cryptosystems». *Communication of the ACM*, vol. 21, n° 2, Feb. 1978, pp. 41-54. ■

J.-S. Lair

suite de la page 5

vices de l'IGC ainsi qu'à ses partenaires et aux autres infrastructures.
Pour cela, des documents tel que [PC2], [PP_IGC], [PP_OSM] doivent décrire l'IGC en termes opérationnels, techniques, organisationnels, ainsi qu'en termes de services rendus à l'utilisateur.
La reconnaissance de l'IGC par un organisme de confiance, un schéma d'accréditation national ou propre à une application représentent également un élément de confiance plus formel qui peut résulter d'une étude de l'ensemble des autres indicateurs.
Dans le cadre de communications entre infrastructures, des accords doivent être conclus, sous l'égide d'une autorité compétente. Cette autorité doit être capable de déterminer si les modalités de gestion mises en œuvre par deux IGC sont équivalentes et si leur coopération dans le cadre d'une ou plusieurs applications peut être envisagée.

Conclusion

Les infrastructures de gestion de clés sont des systèmes émergents qui répondent aux besoins de sécurité des systèmes d'information. Elles offrent des moyens techniques, organisationnels et humains au service de la génération de la confiance.
Des acteurs issus de domaines de compétences des plus divers (notariat, santé, commerce électronique, opérateurs Télécom, etc.) s'adonnent aujourd'hui à cette nouvelle activité de gestion de certificats, dans le but de sécuriser leurs applications. Ils se positionnent soit en tant qu'opérateurs de service, soit en proposant un produit matériel ou logiciel de déploiement d'IGC, soit en déployant une infrastructure au sein même de leur activité.
Les enjeux liés au développement des IGC désormais identifiés, les efforts commerciaux, nationaux et internationaux tendent aujourd'hui à se fédérer pour assister et accélérer le développement des IGC.

Virginie Taïch
Division Chiffre - SCSSI

Les textes légaux

L'usage de la cryptologie est régi par l'article 28 de la loi n° 90-1170 sur la réglementation des télécommunications modifiée en 1996.
Le 19 janvier 1999, le Premier Ministre, M. Jospin, annonçait une proche libéralisation de l'usage de la cryptologie. Voici un extrait de son discours :
« Nous avions, il y a un an, franchi un premier pas vers la libéralisation des moyens de cryptologie. J'avais annoncé alors que nous en franchirions un autre ultérieurement. Le Gouvernement a, depuis, entendu les acteurs, interrogé les experts et consulté ses partenaires internationaux.
Nous avons aujourd'hui acquis la conviction que la législation de 1996 n'est plus adaptée. En effet, elle restreint fortement l'usage de la cryptologie en France, sans d'ailleurs permettre pour autant aux pouvoirs publics de lutter efficacement contre des agissements criminels dont le chiffrement pourrait faciliter la dissimulation.
Pour changer l'orientation de notre législation, le Gouvernement a donc retenu les orientations suivantes dont je me suis entretenu avec le Président de la République :
– offrir une liberté complète dans l'utilisation de la cryptologie ;
– supprimer le caractère obligatoire du recours au tiers de confiance pour le dépôt des clefs de chiffrement ;
– compléter le dispositif juridique actuel par l'instauration d'obligations, assorties de sanctions pénales, concernant la remise aux autorités judiciaires, lorsque celles-ci la demandent, de la transcription en clair des documents chiffrés. De même, les capacités techniques des pouvoirs publics seront significativement renforcées et les moyens correspondants dégagés.
Changer la loi prendra plusieurs mois. Le Gouvernement a voulu que les principales entraves qui pèsent sur les citoyens pour protéger la confidentialité de leurs échanges et sur le développement du commerce électronique soient levées sans attendre. Ainsi, dans l'attente des modifications législatives annoncées, le Gouvernement a décidé de relever le seuil de la cryptologie dont l'utilisation est libre, de 40 bits à 128 bits, niveau considéré par les experts comme assurant durablement une très grande sécurité. »

Dans la suite logique de cette déclaration, les décrets n° 99-199 et n° 99-200 passant le seuil de 40 bits à 128 bits sont sortis le 19 mars 1999. Ils établissent, entre autres choses :
– que l'utilisation des produits «offrant un service de confidentialité mis en œuvre par un algorithme dont la clé est d'une longueur inférieure ou égale à 40 bits» est libre ;
– que l'utilisation des produits entre 40 et 128 bits est libre, sans condition dans le cas d'un usage purement privé, et après une unique déclaration du producteur, d'un fournisseur, d'un importateur ou même à défaut d'un utilisateur dans les autres cas.

Pour informations complémentaires, voir les sites :
www.premier-ministre.gouv.fr
www.legifrance.gouv.fr

Par ailleurs, au sein de l'administration, pour aider à un déploiement efficace des moyens de cryptologie, il existe aussi d'autres textes de régulation. En particulier, les instructions interministérielles n° 900/SGDN/DISSI/SCSSI/DR et n° 901/DISSI/SCSSI définissent la procédure à suivre pour protéger des informations classifiées de Défense ou sensibles non classifiées par des moyens de cryptologie.

Pour informations complémentaires, contacter robert.longeon@cnrs-dir.fr ou le SCSSI. ■

Références

[PC2] Procédures et politiques de certification de clés – Groupe Ad Hoc Messagerie Sécurisée de la Sous-Commission Chiffre de la Commission Interministérielle de la Sécurité des Systèmes d'Information (CISSI).
[PP_IGC] Profil de protection Infrastructures de gestion des clés – Groupe Ad Hoc Messagerie Sécurisée de la Sous-Commission Chiffre de la CISSI.
[PP_OSM] Profil de protection Outil de sécurisation des messages – Groupe Ad Hoc Messagerie Sécurisée de la Sous-Commission Chiffre de la CISSI. ■

SÉCURITÉ INFORMATIQUE
numéro 24 avril 1999
SÉCURITÉ DES SYSTÈMES D'INFORMATION

Sujets traités : tout ce qui concerne la sécurité informatique. Gratuit.
Périodicité : 5 numéros par an.
Lectorat : toutes les formations CNRS.

Responsable de la publication :
ROBERT LONGEON
Centre national de la recherche scientifique
Service du Fonctionnaire de Défense
c/o IDRIS - BP 167. 91403 Orsay Cedex
Tél. 01 69 35 84 87
Courriel : robert.longeon@cnrs-dir.fr
http://www.cnrs.fr/Infosecu

ISSN 1257-8819
Commission paritaire n° 3105 ADEP

Conseil et coordination : CNRS - DIST - Jacqueline Leclère • Conception et réalisation : La Souris 01 45 21 09 61