NOTE DE LA FRS

n° 17/2008

Sécurité des Systèmes d'Information : l'infrastructure de gestion des clefs publiques à la portée de tous…

GCA (2S) Michel Asencio, Chercheur associé

(15 septembre 2008)

Les technologies de l'information et de la communication (TIC) ont envahi notre quotidien et notre vie sociale au travers de l'Internet et des Intranet d'entreprises. En 2006, il y avait plus d'un milliard et demi d'internautes à travers le monde et les échanges dématérialisés se généralisent et croissent de manière exponentielle. Comme le souligne le *Livre blanc sur la défense et la sécurité nationale*, de nouvelles menaces apparaissent avec ces nouvelles pratiques de travail et les échanges entre particuliers qui nécessitent un besoin de sécurité recouvrant la disponibilité, l'intégrité, l'authentification voire la confidentialité des échanges et de leurs contenus. La généralisation de cette dématérialisation des échanges va obliger à recourir de plus en plus souvent aux infrastructures de gestion de clés publiques (IGC). Le but de cette note est de rendre compréhensible au non spécialiste le concept IGC et le système des clés asymétriques.

Introduction

En cryptographie, il faut distinguer 2 systèmes :

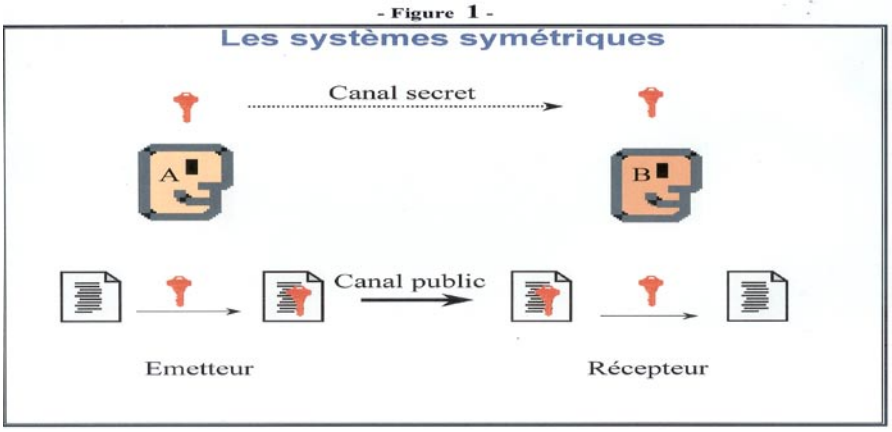
- les systèmes à clé symétrique également nommée « clé secrète » ;
- les systèmes à clé asymétrique connue sous le vocable « clé publique ».

Les systèmes à clé secrète utilisent une même clé pour chiffrer et déchiffrer un seul message secret. Les systèmes à clé publique utilisent une clé pour chiffrer et une autre clé pour déchiffrer. Ces deux clés sont indissociables et constituent le « bi-clé ».

Les systèmes symétriques

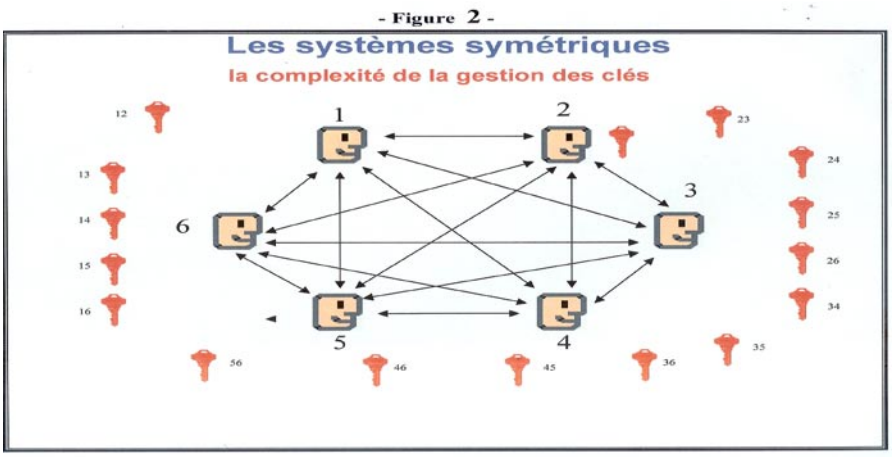
Les systèmes symétriques utilisent une clé unique par couple émetteur-récepteur. Ce couple est seul à partager ce secret. Il y a symétrie complète et unicité de la clé pour les deux opérations de chiffrement et de déchiffrement, comme l'indique la figure 1.

- Figure 1 -



Ce sont des systèmes rapides (quelques dixièmes de secondes pour un message d'un mégaoctet) et bien adaptés pour la confidentialité. Par contre la gestion de ces clés devient très vite compliquée et inextricable avec l'augmentation des couples émetteurs-récepteurs, c'est-à-dire des abonnés, comme l'illustre la figure 2.

- Figure 2 -



Les systèmes asymétriques

Dans ces systèmes asymétriques, chaque clé possède deux moitiés qui se correspondent, l'une dite « clé publique », l'autre étant nommée « clé privée ». Mais il y a une asymétrie forte dans ces deux types d'opérations :

- la première consiste en un chiffrement et une génération de signature avec la clé privée de l'émetteur (représenté par A dans la figure 3) ;

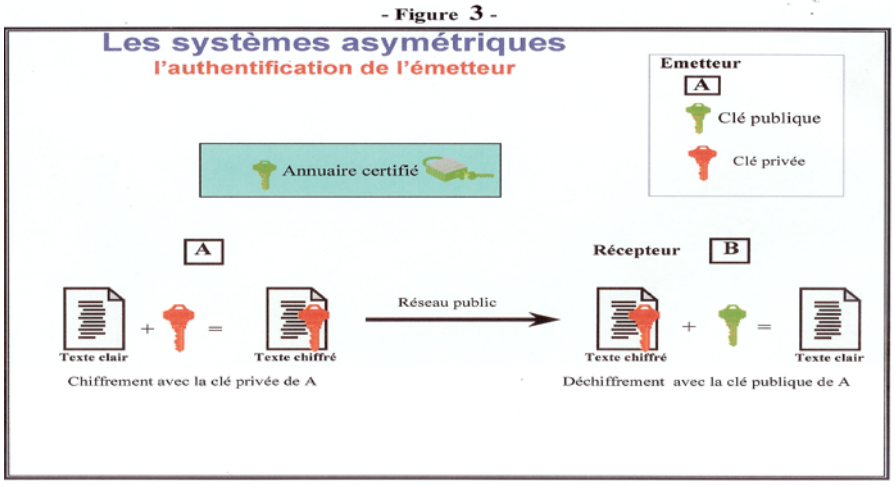
- la seconde tient en un déchiffrement et une vérification de signature par le récepteur (représenté par B dans la figure 3).

Les systèmes asymétriques contrairement aux systèmes symétriques sont plus lents (de l'ordre de 1 à 1 000, soit quelques minutes au plus) mais offrent, lorsqu'on évolue dans un monde de confiance, une gestion de clés facile même pour plusieurs milliers d'abonnés.

1. Le besoin d'authentification

La figure 3 illustre, à partir d'un annuaire centralisé et certifié, comment un récepteur B peut authentifier de manière certaine un émetteur A.

- Figure 3 -



Légende:

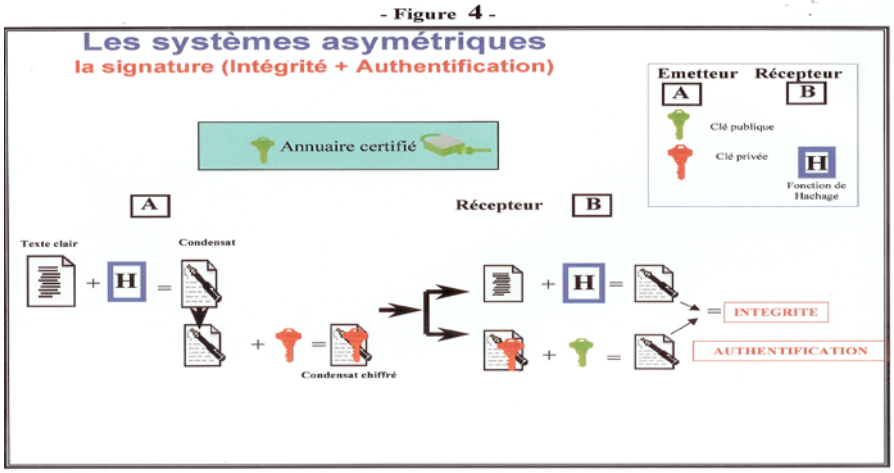
- l'émetteur A a chiffré un message à l'aide de sa clé privée.
- tout le monde a accès à la clé publique de A, grâce à l'annuaire certifié. Donc tout le monde peut lire le message émis par A, après l'avoir déchiffré à l'aide de la clé publique de A

Rappel: A est le seul capable d'émettre un message chiffré avec sa clé privée. Tous les récepteurs qui déchiffreront le message avec la clé publique de A savent que c'est A qui est l'émetteur et lui seul. L'authentification de A est donc acquise.

2. Le besoin de signature (authentification + intégrité)

La figure 4 illustre, elle, le besoin du récepteur B d'authentifier la signature de l'émetteur A mais aussi de vérifier que l'échange est resté intègre durant l'échange (pas de détournement, ni de modification du texte)

- Figure 4 -



Légende :

- La fonction de hachage est une opération cryptographique, non réversible, permettant d'obtenir une image (condensat) du texte clair. Toute modification du texte clair, aussi minime soit-elle, donnera en appliquant la fonction de hachage d'un nouveau condensat.
- L'émetteur A fait subir la fonction de hachage à son texte clair. Il obtient le condensat correspondant.
- Le condensat est chiffré avec la clé privée de A. Le condensat chiffré est transmis, par un canal public au récepteur B afin d'être déchiffré avec la clé publique de A, c'est l'opération d'authentification de l'émetteur A (cf. figure 3).
- Il s'agit ici d'être sûr de la signature de l'émetteur A, il n'y a pas de besoin de confidentialité. C'est pourquoi le texte clair et le condensat sont transmis simultanément, par un canal public, au récepteur B. Ce dernier, applique au texte clair la même fonction de hachage et obtient un condensat qu'il compare avec celui qu'il a reçu de l'émetteur A. L'équivalence des condensats démontre l'intégrité du document transmis en clair.

Les opérations décrites ci-dessus sont totalement transparentes pour les opérateurs.

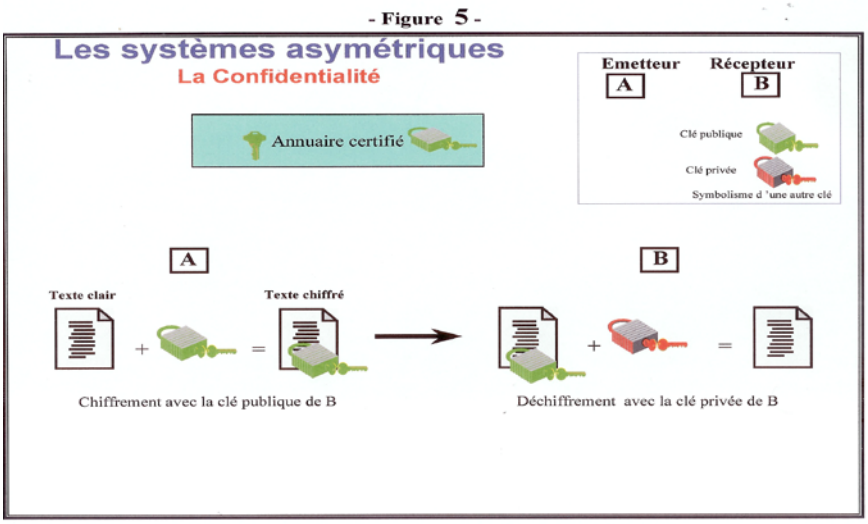
3. Le besoin de confidentialité

Les systèmes asymétriques permettent également d'assurer la confidentialité des échanges bien que cette fonctionnalité ne s'applique pas correctement à des textes ou échanges longs. Plusieurs mégaoctets représentent un texte d'une dizaine de pages environ et demandent avec les systèmes asymétriques quelques minutes alors que les systèmes symétriques chiffrent ces mêmes textes en quelques secondes. Dans le domaine de la confidentialité, on perd donc en performances par rapport aux systèmes symétriques.

L'explication est simple : les clés de chiffrement utilisées par les systèmes asymétriques sont très longues donc plus robustes par rapport à celles utilisées par les systèmes symétriques. Elles utilisent également des mécanismes mathématiques de chiffrement beaucoup plus complexes. Cette robustesse explique la lenteur de chiffrement (1 à 1 000) par rapport aux systèmes symétriques et la perte de performance.

La figure 5 illustre le principe de la confidentialité dans les systèmes asymétriques.

- Figure 5 -



Légende:

- tout le monde a accès à la clé publique de B. Seul B peut lire le message chiffré par A, car il n'y a que lui qui possède sa clé privée qui est l'autre « moitié » de sa clé publique.

En conclusion partielle de ces tentatives d'explications, il faut retenir que les systèmes symétriques offrent les avantages de la vitesse de chiffrement pour assurer la confidentialité mais que le nombre d'utilisateurs est forcément limité alors que les systèmes asymétriques, eux, offrent l'assurance de la signature par l'authentification de l'émetteur et l'intégrité du texte émis quel que soit le nombre d'utilisateurs mais ils sont plus lents.

Il est donc tout naturel de vouloir combiner ces deux types de systèmes, appelés systèmes mixtes, pour utiliser à la fois les avantages de la clé symétrique et ceux de la clé asymétrique.

Les systèmes mixtes

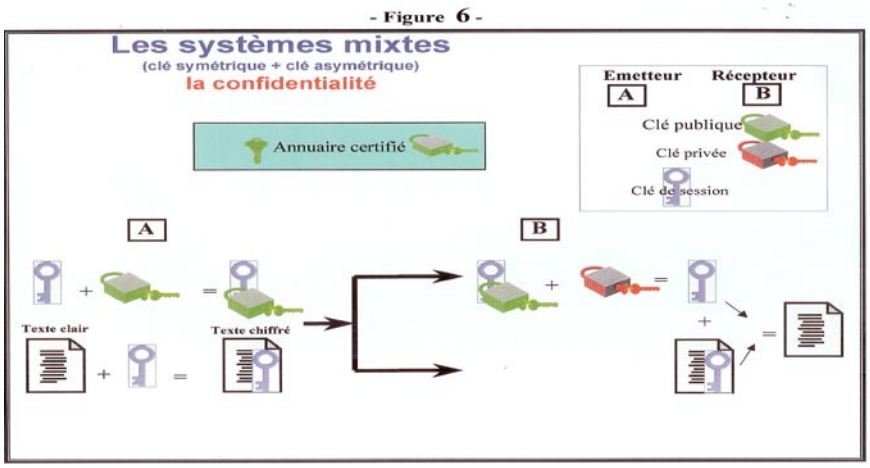
1. Le principe de confidentialité dans un système mixte

La confidentialité dans un système mixte fait appel à une clé de session de façon à gommer les lenteurs de chiffrement du système asymétrique. La clé de session est mise en œuvre par un algorithme de chiffrement symétrique donc très rapide. Une partie de l'opération consiste à transmettre au récepteur B cette clé secrète qui a permis de chiffrer (il faut rappeler que B doit avoir obligatoirement la même clé pour déchiffrer).

Le canal sûr pour transmettre cette clé de session est fourni par le chiffrement asymétrique qui vient « encapsuler » cette fonction confidentialité en un temps très court car il ne s'agit plus dans ce cas de chiffrer un texte clair mais de traiter une suite de 1 et de 0 ce qui est électroniquement plus rapide.

La figure 6 illustre le principe de confidentialité offert par un système mixte.

- Figure 6 -



Légende :

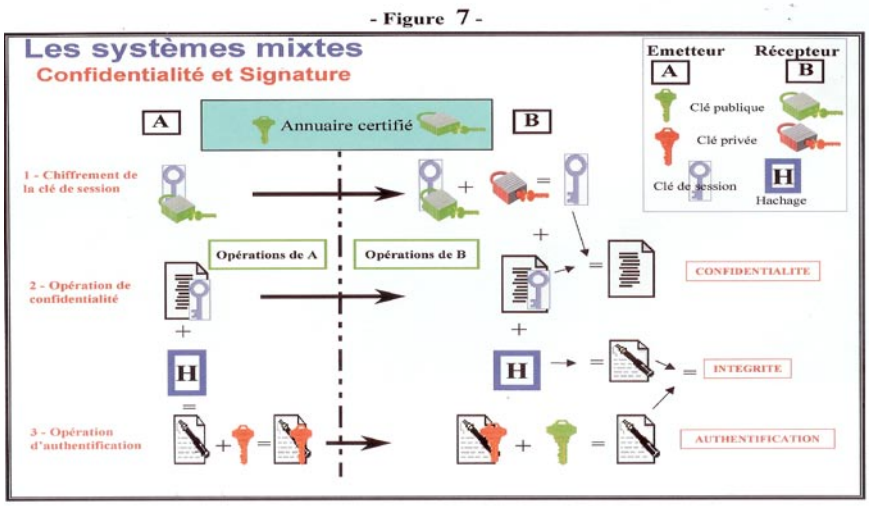
- la clé de session est le remplacement de l'ancien ruban perforé des machines de cryptographie. C'est une clé qui est générée aléatoirement à chaque opération de chiffrement donc différente à chaque message.
- le texte chiffré (avec la clé de session) et la clé de session (elle-même chiffrée avec la clé publique du récepteur B) sont transmis par un canal public au récepteur B. Ce dernier pourra déchiffrer la clé de session, car lui seul possède la clé privée correspondante. Il détient donc la clé de session qui permet de déchiffrer le texte envoyé par l'émetteur A.
- toutes ces opérations sont transparentes pour les utilisateurs.

2. L'offre de confidentialité et de signature d'un système mixte

Le but des systèmes asymétriques est de répondre aux besoins de disponibilité, d'intégrité, d'authentification c'est-à-dire de signature électronique tout en assurant une très grande confidentialité dans un espace de confiance, avec des outils simples d'emploi et totalement transparents pour l'utilisateur non spécialiste.

La figure 7 regroupe en une seule illustration les trois opérations assurant la confidentialité, l'intégrité et l'authentification d'un échange électronique. Ces opérations se déroulent simultanément et sans l'intervention de spécialistes.

- Figure 7 -



La sécurité des informations du futur...

Les communications quantiques exploitent l'envoi de photons intriqués[1], chacun transportant un bit d'information. Elles sont sûres car, si une personne intercepte les photons, l'intrication cesse en dévoilant l'intrus. Les bits reçus en sécurité sont utilisés comme clé pour crypter les communications. On a réussi à transmettre une clé quantique à 144 km, mais, pour des distances plus grandes, la transmission est difficile car l'atmosphère perturbe les états quantiques fragiles des photons. On vient cependant de démontrer à titre expérimental que les communications quantiques spatiales sont possibles à très longues distances.

Cette technologie permettant une sécurité à toute épreuve n'est pas encore disponible dans les applications courantes pour le commun des mortels. Les spécialistes en sont au stade de la réalisation de portes logiques quantiques et ils estiment qu'un ordinateur quantique ne sera pas disponible avant une quinzaine d'années...

Conclusions

Compte tenu de la multiplication des échanges électroniques en cours (et surtout à venir) et grâce à l'instauration du travail en groupe et à la transversalité autorisée par la connexion des réseaux, l'utilisateur des techniques numériques a besoin de plus de sécurité, de disponibilité et de fiabilité dans ses échanges électroniques.

Le *Livre Blanc* 2008 insiste longuement sur cette nouvelle menace d'intrusion dans les échanges numérisés et demande aux services gouvernementaux mais aussi aux entreprises privées de se prémunir contre ces risques : « *Les moyens d'information et de communication sont devenus les systèmes nerveux de nos sociétés, sans lesquels elles ne peuvent plus fonctionner. Or le « cyberespace », constitué par le maillage de l'ensemble des réseaux, est radicalement différent de l'espace physique : sans frontière, évolutif, anonyme, l'identification certaine d'un agresseur y est délicate.*

La menace est multiforme : blocage malveillant, destruction matérielle, neutralisation informatique, vol ou altération de données, voire prise de contrôle d'un dispositif à des fins hostiles. Dans les quinze ans à venir, la multiplication des tentatives d'attaques menées par des acteurs non étatiques, pirates informatiques, activistes ou organisations criminelles, est une certitude. Certaines d'entre elles pourront être de grande ampleur ».

[1] L'intrication (*quantum entanglement*) résulte de l'affinité quantique entre des particules par laquelle la mesure d'une propriété quantique d'une particule détermine automatiquement et instantanément la propriété correspondante de l'autre particule. On a pu intriquer des photons, des électrons et des atomes. Par exemple, des atomes sont intriqués en les forçant à agir dans un piège optique tandis que des photons sont intriqués dans un cristal. En informatique, les « qubits » sont liés par l'intrication.

Pour répondre à ces besoins les systèmes asymétriques devraient, dans les prochaines années, connaître un énorme développement à condition que les entreprises privées, les structures gouvernementales et les services mettent en place des infrastructures de gestion des clés publiques pour traiter correctement ce problème complexe Ces structures organisationnelles et techniques doivent prendre en compte les directives interministérielles émises dans ce domaine pour assurer un minimum d'interopérabilité même si la spécificité du ministère de la Défense doit également prendre en compte les travaux menés par l'OTAN et l'Union européenne, les demandes des industriels de l'armement et surtout la souplesse d'emploi et la maîtrise des matériels sur les théâtres extérieurs.

Ces structures respectent la nécessaire centralisation pour la certification des clés (registre ministériel et autorité de certification), l'archivage des clés de confidentialité qui est une obligation légale et réglementaire. Mais elles prennent aussi en compte l'autonomie des autorités d'enregistrement qui devront être au plus près des utilisateurs.

Le concept dans son application est encore relativement nouveau, les travaux restant à conduire tant en interne aux ministères intéressés qu'en interministériel sont encore très importants. Les premiers systèmes qui voient l'application de ce concept d'infrastructures de gestion des clefs sont les différents Intranet des structures ministérielles et des grandes sociétés pour ce qui concerne les échanges d'informations sensibles ou sécurisées. En attendant les communications quantiques et leur sécurité inviolable ... pour la génération prochaine.

Je tiens à remercier les spécialistes de la DGA et de la D4SIC pour les précisions qu'ils ont bien voulu me donner sur ce sujet extrêmement important.

Les opinions exprimées ici n'engagent que la responsabilité de leur auteur.

http://www.frstrategie.org

GCA (2S) Michel Asencio, Chercheur associé
m.asencio@frstrategie.org