ENSICAEN

ENSICAEN
ÉCOLE NATIONALE SUPÉRIEURE D'INGÉNIEURS DE CAEN
& CENTRE DE RECHERCHE
Spécialité Informatique
2ème année

PKI et Smartcards

MASSÉ Nicolas
LIMIN Thomas

2ème semestre 2005-2006

Nicolas MASSÉ & Thomas LIMIN

PKI et smartcards

ENSI de Caen

Introduction

Le premier objectif des systèmes de télécommunication fut de permettre la communication entre deux entités distantes. Une fois ce but réalisé, ces systèmes ont permis l'émergence de nouveaux moyens de communication, d'abord entre les experts, puis entre les entreprises et les administrations et impliquant finalement tout un chacun. Au fur et à mesure des nouvelles utilisations, le besoin en fiabilité et en sécurité s'est accru. Par fiabilité est entendu la disponibilité permanente du moyen de communication, l'absence de pannes ou de dysfonctionnements. Mais que représente la sécurité?

Dans le contexte des télécommunications, c'est à dire la communication de deux personnes (ou machines) qui ne se voient pas directement et qui sont souvent très éloignées, la sécurité regroupe les notions de confidentialité, d'authentification et de contrôle d'intégrité.

La première partie s'attachera à décrire les mécanismes rendant ces services, et particulièrement ceux faisant appel à la cryptographie asymétrique et aux infrastructures à clef publique. La seconde nous permettra de décrire en quoi l'introduction de smartcards simplifie l'utilisation d'un tel système tout en augmentant la confiance que l'on peut y placer.

Sommaire

1 - Infrastructures à clef publique

1.1 - La cryptographie asymétrique

Lorsqu'en 1976 Whitfield Diffie et Martin Hellman publient New Directions in Cryptography, ils proposent une nouvelle approche de la cryptographie, la cryptographie asymétrique, qui simplifie grandement l'échange de clefs (protocole de Diffie-Hellman) et ouvre la voie à de nouveaux mécanismes de signature. Le développement des algorithmes de cryptographie asymétrique ne tarda pas et 1978 voit la publication de RSA, très utilisé, et plus récemment (1985) est publié le cryptosystème ElGamal.

Les cryptosystèmes asymétriques reposent sur un concept simple. Chaque participant génère une paire de clef, une clef est publiée (la clef publique), l'autre est gardée secrète (clef secrète). Pour assurer la confidentialité de la communication, l'expéditeur d'un message utilise la clef publique du destinataire. En effet seule la clef secrète qui lui est associée et qui est la propriété exclusive du destinataire permet de déchiffrer le message. Pour s'assurer de l'identité d'un interlocuteur ou de la provenance d'un document, on utilise généralement un mécanisme d'authentification par signature. La personne qui désire s'identifier ou qui signe un message utilise sa clef secrète pour créer une signature. Cette signature peut ensuite être vérifiée par toute personne connaissant la clef publique du signataire.

1.2 - Le problème de l'authenticité des clefs

Dans le cas d'un cryptosystème fiable, toute la confiance que l'on peut lui accorder est assujettie à la confiance dans la validité des clefs publiques et de l'effectif secret entourant les clef secrètes. En effet, dans le cas du chiffrement, l'expéditeur peut être certain que la connaissance du secret est indispensable au déchiffrement du message, et que le décryptage du message est, du moins en un temps acceptable, impossible. Cependant, qu'en est il du secret de la communication si la clef publique utilisée pour chiffrer n'est pas celle du destinataire, mais celle d'une tierce personne, qui du coup, connaît la clef secrète associée? De même pour la signature: les cryptosystèmes permettent de s'assurer que la signature a été faite par quelqu'un connaissant le secret associé. Mais comment s'assurer que la personne détenant le secret est bien celle qu'elle prétend être?

La véracité de l'association entre une clef publique et une identité, que ce soit celle d'un serveur ou celle d'une personne, est un point essentiel sur lequel repose la sécurité des cryptosystèmes asymétriques. Les systèmes de distribution des clefs publiques doivent prendre en compte l'obligation d'en permettre la vérification.

1.3 - Le réseau de confiance

Plusieurs méthodes ont été développées pour valider les associations identité / clef. L'une d'elles, le réseau de confiance, ou Web of Trust, s'appuie sur un réseau de proches connaissances et sur la transitivité de la confiance. Ainsi si Alice connaît Bob et qu'ils s'échangent de manière sécurisée, par exemple de la main à la main, leur clef publique, chacun a une confiance maximale dans la validité de l'association identité / clef, et peut l'attester en apposant sa signature sur l'association identité / clef de son interlocuteur. Par ailleurs, si Bob fait de même avec Carole et authentifie en y apposant une signature

l'association entre l'identité de Carole et une clef publique, alors Alice, qui fait confiance à Bob, peut raisonnablement faire confiance à la clef de Carole si celle ci présente une signature de Bob. Ce système est efficace, mais complexe et demande de la part des utilisateurs une grande attention. En effet ceux ci ne devrait jamais signer une clef sans avoir auparavant scrupuleusement vérifié l'identité de son propriétaire, sans quoi le réseau de confiance se trouverait gravement affaibli. Dans la pratique cette méthode est utilisée par PGP, Pretty Good Privacy, un système de chiffrement et de signature d'e-mails et de documents, mais sa mise en oeuvre complexe et totalement décentralisée empêche son utilisation à grande échelle. En effet, hormis pour les clefs qu'Alice a personnellement signé, leur validité s'appuie sur une chaîne de signataires (Bob connaît Carole qui connaît Denis, qui lui même connaît Eric etc, chacun attestant de l'identité du suivant), les premiers pouvant être connu d'Alice, les suivants ne le sont certainement pas, mais elle doit tout de même s'en remettre à eux pour valider la clef de son interlocuteur. Même si Alice peut décider d'outrepasser la chaîne de signataires pour s'assurer elle même de la validité de la clef en organisant une rencontre, ce qui peut représenter une opération couteuse, elle ne pourra pas le faire pour tout ses interlocuteurs. Cette méthode impose un prérequis à toute communication faisant intervenir un nouvel interlocuteur, la rencontre "en personne", ce qui revient presque à la complexité de l'échange préalable d'un secret par un canal sécurisé avant les communications chiffrées symétriquement, le secret en moins. Pour résumer, le réseau de confiance est un moyen efficace d'authentifier les clefs d'un groupe relativement restreint d'utilisateurs éclairés, mais son manque de centralisation et sa complexité rende son exploitation "industrielle" délicate, voire dangereuse.

1.4 - Les infrastructures à clef publique

Une autre approche développée pour valider l'association identité / clef est la notion d'infrastructure à clef publique, apparaissant sous le sigle PKI (public key infrastructure) dans la littérature anglophone. Le but des PKI est d'authentifier, en tant que tiers de confiance, cette association, matérialisée sous la forme d'un certificat. Le rôle des PKI est la gestion de ces certificats, depuis leur génération à leur révocation, en passant par leur authentification. Une PKI peut être divisée en plusieurs entités, chacune ayant un rôle distinct.

- L'autorité d'enregistrement, RA comme Registration Authority, est l'organisme qui est chargé de vérifier les données relatives à un utilisateur, de générer une paire de clef et d'envoyer à l'autorité de certification la demande de certificat spécifiant les données qui y seront insérées, incluant la clef publique.
- L'autorité de certification, CA comme Certification Authority, est l'élément critique de l'ensemble. Son rôle est de signer les données propres à l'utilisateur, comportant sa clef publique. Une fois signées par le CA, ces données forment un certificat.
- L'autorité de dépôt, repository, stocke les certificats et les listes de certificats révoqués.
- L'autorité de séquestre, KE Key Escrow, a la charge, quand la législation l'impose, de mettre à disposition des autorités compétentes les données permettant le déchiffrement.

Le standard pour les certificats a été définis en 1988 par l'ITU (l'union internationale des télécommunications) sous le nom X.509, version 1, 2 ou 3.

L'utilisation de certificats permet d'ajouter un moyen simple de vérification de l'authentification des clefs à la cryptographie asymétrique. Cependant, il est inutile de se leurrer, les certificats et les PKI ne sont pas un moyen miraculeusement infalsifiable de s'assurer de l'identité de son interlocuteur. En effet, les certificats dont on désire vérifier l'authenticité sont certifiés par la signature du CA, que chacun peut contrôler grâce au certificat auto-signé du CA, dit certificat racine (root-certificate). La plupart de ces certificats racine sont inclus dans les logiciels utilisant la cryptographie asymétrique, les plus communs étant les navigateurs web. Mais qu'en est il de la validité de ces certificats racine? En effet aujourd'hui de nombreuses machines sont victimes de programmes malveillants qui, profitant de failles de sécurité ou d'une configuration le permettant, modifient le système à leur gré. A priori rien ne peut les empêcher de falsifier les certificats racine résidants afin qu'il permettent de valider de faux certificats par la suite. Dans cette perspective, le niveau de sécurité est réduit à néant.

Cependant le risque n'est pas cantonné à la falsification des certificats racine. Les PKI ne sont pas composées que d'algorithme de cryptographie réputés sûr, mais aussi de procédures administratives de vérification d'identité, le rôle des autorités d'enregistrement, sous la tutelle de personnes physiques, qui peuvent être abusées, ou corrompues. Dans un environnement critique, ce point n'est pas à négliger, ce qui impose aux autorités de certification de suivre des procédures complexes permettant d'éviter que de telles erreurs brisent la confiance. Un moyen parmi d'autres est de répartir les vérifications

1.5 - Remarques sur la sécurité des PKI

Les infrastructures à clef publique apportent un niveau de confiance important dans les clefs utilisées, grâce aux certificats, et sont plus facilement adaptées, de part leur centralisation, à une mise en place à grande échelle. Cependant l'utilisation de ces systèmes, qui assurent l'authentification des clefs publiques, n'assure en rien la sécurité des clefs privées, qui sont sous l'entière responsabilité de leur propriétaire. Ces propriétaires doivent être considérés comme des utilisateurs ne disposant pas de connaissances spécifiques en sécurité informatique, de sorte qu'il peut être beaucoup plus simple leur dérober une authentique clef privée pour signer à leur place que de forger une signature ou de falsifier le certificat associé. Il est donc d'une importance capitale d'assurer la totale confidentialité des clefs privées, en utilisant par exemple des dispositifs permettant leur utilisation tout en ne les divulguant pas. Ces dispositifs peuvent prendre la forme de carte à puces, appelées aussi smart cards.

2 - Smart cards

Lorsque les cartes de paiement ont commencé à se développer, elles utilisaient alors comme support d'information une bande magnétique. Ce support à l'avantage d'être simple, diminuant ainsi les coûts des technologies associées ; le revers de la médaille est qu'il n'est pas possible d'y stocker d'informations confidentielles (PIN, solde d'un porte-monnaie électronique) car elle sont lisibles et modifiables à volonté. De ce constat est né un besoin de sécurité et de contrôle d'accès aux informations, qui a été satisfait par l'arrivée des smart cards.

2.1 - Qu'est-ce qu'une smart card ?

Une smart card, aussi appelée "carte à puce" ou "carte à circuit intégré", est une carte de petit format ayant des circuits électroniques intégrés. Il existe deux grands types de cartes : les cartes à mémoire et les cartes à microprocesseur. Les premières ne contiennent qu'une mémoire non volatile et quelques circuits logiques destinés à assurer la sécurité. Contrairement aux cartes à mémoire, les cartes à microprocesseur possèdent en plus un microprocesseur. On notera, cependant, que couramment l'appellation "smart card" désigne uniquement les cartes à microprocesseur au format "carte de crédit" ou plus petit, ce sont sur ce type de cartes que nous nous focaliserons dans la suite de ce document.

2.2 - Communication

Parmi les smart cards (cartes à microprocesseur), on distingue deux grands types de cartes, suivant le mode de communication qu'elles utilisent : les cartes à contacts et les cartes sans contact. Les premières ont une série de 8 contacts normalisés par l'ISO sous la dénomination "ISO/IEC 7816" tandis que les dernières utilisent la technologie RFID (ISO/IEC 14443 et ISO 15693) comme moyen de communication. Il est à noter qu'il existe des cartes qui utilisent les deux modes de communication : ce sont des cartes hybrides.

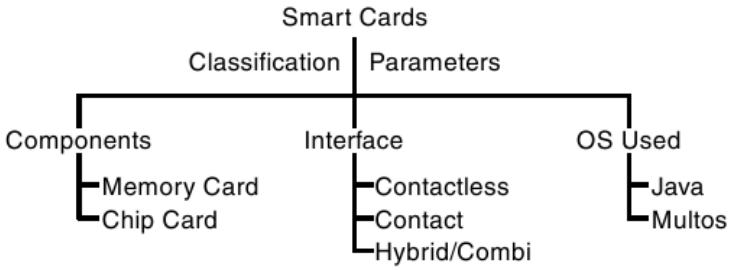

Illustration 1: Classification des smart cards

2.3 - Constitution

Une smart card est constituée de plusieurs éléments :

- une ROM qui contient le système d'exploitation de la puce (quelques kilo octets) ;
- une EEPROM qui contient le code des applications et leurs données (entre 2 et 32 ko) ;
- une RAM qui est utilisée par le processeur pour stocker des résultats temporaires (en général 256 octets) ;
- un microprocesseur (en général une architecture CISC 8 bits, à 5 MHz).

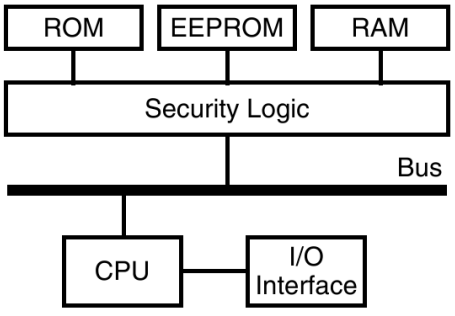

Illustration 2: Architecture d'une smartcard

2.4 - Caractéristiques

Les normes ISO relatives aux smart cards impliquent certaines caractéristiques telles que leur forme, la position de leurs contacts (s'il y a lieu), leur résistance électrique et physiques, etc.

2.4.1 - Forme

La forme d'une carte est normalisée : selon la norme ISO/IEC 7816 [1], une carte doit mesurer 53.98 mm de large et 85.6 mm de long. La position des contacts est également normalisée.

2.4.2 - Résistance physique

Les cartes se doivent de résister aux attaques répétées de l'environnement dans lequel elles seront utilisées : surtension, exposition à la chaleur, au froid, aux rayons X, torsions, et la liste n'est pas exhaustive ! À cela, il faut ajouter la résistance au démontage (« tamper résistance » en anglais) car, stockant des informations sensibles, il ne faudrait pas qu'il soit possible d'y accéder en démontant la puce et en y connectant un analyseur logique. Afin de se prémunir contre ce risque, les puces intègrent des protections matérielles (fusibles sensibles aux UV), et logicielles (somme de contrôle de la mémoire, production continuelle d'un bruit de fond, etc.).

2.5 - Applications

Les domaines d'application des smart cards sont très variés, on les trouve dans nos téléphones portables où elles assurent l'identification de l'abonné, stockent les messages courts (SMS), le répertoire téléphonique et hébergeront bientôt un serveur web (voir [2]) ; elles nous permettent également de payer : ce sont nos cartes bancaires ; on notera que de plus en plus de cartes de fidélité sont équipées de puces ; les sociétés de transports en commun utilisent ces cartes et deviennent parfois un standard de fait, comme c'est le cas avec la carte « Octopus » à Hong Kong (voir [3]), au début elle était réservée aux bus de la ville et maintenant de plus en plus de magasins l'acceptent comme moyen de paiement ; dans certains pays les permis de conduire sont en fait des cartes à puce, réduisant ainsi le risque de fraude ; les smart cards sont aussi utilisées comme moyen d'identification pour accéder à une zone confidentielle d'un bâtiment. Il existe cependant un domaine encore assez peu occupé par les smart cards : celui de la conservation de clés privées dans une infrastructure à clé publique.

2.6 - Smart cards et PKI

On définit en général la sécurité d'un système comme étant plus faible que le plus faible de ses éléments. Appliqué aux PKI, ce principe ne les met pas en valeur, car l'élément le moins sécurisé est le poste de travail (celui sur lequel est stocké la clé privée). La sécurité de cet élément est souvent délaissée par les éditeurs de logiciel, et quand bien même il serait conçu pour résister à toutes les attaques présentes et futures, la huitième couche du modèle OSI (elle se situe entre la chaise et le clavier) ne l'est pas : les pirates rivalisent d'ingéniosité pour exploiter la naïveté des utilisateurs dans le but de leur soutirer des informations confidentielles : mot de passe, code pin, clé privée, etc.

Afin de se prémunir contre tous ces risques il est possible d'utiliser des smart cards dans une infrastructure à clé publique. Le rôle de ces cartes est de stocker et d'assurer la confidentialité de la clé privée. Pour cela, la carte possède un coprocesseur cryptographique qui se charge d'effectuer des signatures électroniques (car le procédé de signature implique l'utilisation de la clé secrète). En pratique, lorsqu'une signature ou une procédure d'authentification est requise, plutôt que de communiquer le secret à un terminal quelconque, qui peut être (parfois très simplement) modifié dans le but de le divulguer à un tiers, on charge la carte de faire en interne, à l'aide de son coprocesseur cryptographie intégré, les calculs et de renvoyer uniquement le résultat.

Par précaution, on protège l'utilisation de la carte par un code confidentiel qui doit être fourni préalablement à son utilisation. Cette mesure permet de vérifier que la personne qui présente la carte connaît le code, et donc qu'elle peut raisonnablement être considérée comme l'utilisateur légitime. Ce code est bien entendu beaucoup plus simple à mémoriser et à fournir que le secret contenu dans la carte, de sorte qu'il puisse (et doive) être mémorisé par le porteur de la carte, sans qu'il lui soit nécessaire de le noter, pratique qui réduirais considérablement la sécurité de l'ensemble.

La carte à puce est conçue pour être inutilisable pour qui ne connaît pas le code confidentiel. Sans lui, le logiciel embarqué dans la carte refuse l'accès aux secteurs protégés. Et bien que le code qui, pour être mémorisable, est très court, il ne peut être découvert par recherche exhaustive, qui serait relativement simple, car la carte refuse de fonctionner après un nombre fixé de codes erronés présentés.

Grâce au smart cards, il est possible de confier à tout utilisateur un secret, la clé privée, tout en garantissant sa confidentialité présente et future. Le secret informatique, notion peu tangible pour le néophyte, est matérialisé sous la forme d'un élément physique crucial sans lequel rien n'est possible. De cette manière le rôle de l'utilisateur est considérablement simplifié. Sans carte à puce, il doit être garant de sa clé, de son support, des logiciels utilisés pour signer, du terminal, en bref, de toute la chaîne. Grâce à l'insertion du secret dans une puce capable de faire elle même les signatures, le rôle de l'utilisateur n'est plus que de garantir l'intégrité physique de la carte, c'est à dire empêcher qu'elle tombe entre de mauvaises mains, qui pourraient être équipées de divers instruments de torture propres à faire parler une smart card, aussi bien conçue soit elle.

La consigne que doit respecter l'utilisateur est simple: il ne doit jamais quitter la carte des yeux, (du moins tant qu'elle n'est pas sur lui), et ne pas divulguer son code confidentiel. C'est à la portée de tout le monde, et si cette consigne est directement mise en relation avec les risques que pourrait entraîner toute infraction, il est possible de compter sur la collaboration efficace de tous les porteurs de carte.

Conclusion

Les infrastructures à clé publique sont souvent présenté dans la presse spécialisée comme le remède à tous les maux, cependant la réalité n'est pas si simple: l'authentification de l'association entre une clé publique et une personne physique est loin d'être triviale et nécessite de s'appuyer sur des procédures administratives qui doivent être scrupuleusement suivies par les autorités d'enregistrement et de certification. De plus la confidentialité des secrets est difficile à obtenir de la part d'utilisateurs néophytes, ainsi que des autres, sans utilisation de dispositifs matériels comme les smart cards. La sécurité de ces smart cards repose en grande partie sur leur résistance au démontage (tamper resistance), mais cette résistance n'est finalement qu'apparente : plusieurs laboratoires on déjà réussi à extraire la puce d'une telle carte et à la faire fonctionner sous analyseur logique. Certes l'obtention et l'utilisation du matériel nécessaire à l'opération n'est pas à la portée du premier venu, mais on peut légitimement relativiser la sécurité de ces cartes de la même manière qu'on admet qu'un algorithme est cryptographiquement sûr tant qu'il n'existe pas d'attaques contre lui permettant un décryptage significativement plus rapide que par la recherche exhaustive.

Sans être un remède miracle, l'association PKI / smart card permet de s'affranchir de beaucoup de contraintes et de failles de la cryptographie asymétrique, ce qui la rend finalement utilisable commercialement pour un système relativement fiable de signature / authentification. Mais même si elle fait disparaître les points faibles du système, c'est pour les remplacer par d'autres failles propre aux nouveaux dispositifs ajoutés.

Prôner l'inviolabilité n'est qu'argumentation commerciale, que l'on pourrait presque qualifier d'abusive. Il serait plus judicieux d'affirmer que la fiabilité de tout système repose sur le rapport entre les moyens mis en jeux pour accroître la sécurité et les moyens rassemblés pour la mettre en défaut. Cet aspect doit être pris en compte lors de l'éventuelle prise en compte légale (droit de la preuve) d'une signature électronique et de l'évaluation de la fiabilité de la procédure de signature associée.

Bibliographie

1: ISO/IEC, 7816:1998(E) - Integrated circuit(s) cards with contacts, 1998

2: Scott Guthery, Roger Kehr, et al., GSM SIMs as Web Servers, 2000, http://www.dvs1.informatik.tu-darmstadt.de/publications/pdf/websim-isn2000.pdf

3: Wikipedia, Octopus card, , http://en.wikipedia.org/wiki/Octopus_card