Les principales méthodes d'authentification pour smartphones

12/05/2010

Jean-Philippe Blaise

Les principales méthodes d'authentification pour smartphone

Sommaire

I. Rappel du sujet : Authentification d'applications sur téléphones mobiles

Enseignants encadrants : Francine Herrmann, Yann Lanuel

Contexte

Dans le cadre d'un projet européen, nous mettons en place une chaine de certification d'images capturées par téléphones mobiles. Ces images sont en partie certifiées à l'aide des données GPS puis enregistrées sur un serveur.

L'objectif de ce projet est d'étudier les algorithmes et les méthodes qui permettront de garantir la robustesse de la chaine de certification. L'objectif est d'assurer que l'ensemble du processus de collecte des informations est certifié et qu'aucune falsification n'est possible en cours de transfert.

La difficulté est que les différents acteurs d'une application mobile ne disposent pas nécessairement d'une paire de clés publiques et privées permettant une authentification certifiée.

L'objectif sera donc de comparer différents algorithmes de construction de chaines de certification d'un point de vue théorique, fonctionnel et expérimental.

En particulier, on étudiera la possibilité d'utiliser, sur téléphone mobile Windows, des certificats numériques pour identifier un utilisateur et permettre l'accès à l'application de certification.

1 Objectifs

L'objectif de ce sujet de IR est :

- L'étude bibliographique complète dont l'article [1] proposé en annexe est un point de départ.
- La comparaison théorique de différents systèmes de certification d'applications pour téléphones mobiles.
- Eventuellement la proposition d'une nouvelle méthode utilisable dans le contexte de notre chaîne d'images capturées.

2 Etude bibliographique

Etat de l'art et comparaisons de chaines de certification de différentes applications

3 Référence Bibliographique

[1] Jong Sik Moon, Deok Gyu Lee and Im-Yeong Lee, Device Authentication/Authorization Protocol for Home Network in Next Generation Security, Lecture Notes in Computer Science, Springer Berlin, Volume 5576/2009, In Advances in Information Security and Assurance, 2009, Pages 760-768

II. Introduction

Ce sujet cherche à définir les méthodes de certification et d'authentification dans le cadre d'un projet européen permettant de certifier des images capturées par téléphone mobile.
Une étude de chaque méthode était impérative, les expliquant, pour pouvoir définir leur points faibles ou forts, et pouvoir les comparer les unes aux autres.

III. Définition de l'authentification

L'authentification est la procédure qui consiste, pour un système informatique, à vérifier l'identité d'une entité (personne, ordinateur...), afin d'autoriser l'accès de cette entité à des ressources (systèmes, réseaux, applications...). L'authentification permet donc de valider l'authenticité de l'entité en question. L'identification permet donc de connaître l'identité d'une entité alors que l'authentification permet de vérifier cette identité.

Le contrôle permanent de l'intégrité et de l'accès (usage, identité du destinataire, émetteur, propriétaire) à un contenu ou à un service constitue le fondement de la traçabilité des transactions. Ce contrôle permet :

- la protection des intérêts supérieurs de l'État et du patrimoine informatique des entreprises, donc de leurs intérêts commerciaux. Pour les entreprises, il s'agit de réduire le coût qui résulte d'attaques, de la perte de temps, de la perte d'informations, de l'espionnage, ou des fuites involontaires d'informations...
- le développement du commerce et des échanges électroniques. L'authentification contribue à la facturation des services et contribue à la confiance dans l'économie numérique, condition indispensable du développement économique.
- la protection de la vie privée. Les données personnelles véhiculées dans les systèmes d'information sont des données sensibles à protéger.

Les techniques d'authentification font partie des technologies clés. En France, elles sont identifiées comme telles dans le rapport sur les technologies clés 2010 (voir site sur les technologies clés 2010). Les efforts entrepris par les constructeurs et fournisseurs de services Internet (Ebay, Yahoo, PayPal, etc.) pour mettre en œuvre des systèmes d'authentification, notamment d'authentification forte, nous montrent clairement que l'authentification est un des enjeux majeurs pour le futur.

Dans le cas d'un individu, l'authentification consiste, en général, à vérifier que celui-ci possède une preuve de son identité ou de son statut, sous l'une des formes (éventuellement combinées) suivantes :

- Ce qu'il sait (mot de passe, numéro d'identification personnel).
- Ce qu'il possède (acte de naissance, carte grise, carte d'identité, carte à puce, droit de propriété, certificat électronique, diplôme, passeport, carte Vitale, Téléphone portable, PDA, etc.).
- Ce qu'il est (photo, caractéristique physique, voire biométrie).
- Ce qu'il sait faire (geste, signature).

Quatre propriétés importantes dans l'authentification et qui seront utilisées plus tard :

- La confidentialité : seul le destinataire (ou le possesseur) légitime d'un bloc de données ou d'un message pourra en avoir une vision intelligible ;
- L'authentification : lors de l'envoi d'un bloc de données ou d'un message ou lors de la connexion à un système, on connaît sûrement l'identité de l'émetteur ou l'identité de l'utilisateur qui s'est connecté ;
- L'intégrité : on a la garantie qu'un bloc de données ou un message expédié n'a pas été altéré, accidentellement ou intentionnellement ;
- La non-répudiation : l'auteur d'un bloc de données ou d'un message ne peut pas renier son œuvre.

La phase de vérification fait intervenir un protocole d'authentification. On en distingue deux sortes « familles » :

- L'authentification simple : l'authentification ne repose que sur un seul élément ou « facteur » (exemple : l'utilisateur indique son mot de passe).
- L'authentification forte : l'authentification repose sur deux facteurs ou plus.

Les différentes méthodes qui existent pour garantir l'authentification sont les certificats, les PKI, Kerberos, la clé-USB (ou carte mémoire), la biométrie et les mots de passe. Ceux-ci font partis de la famille des authentifications fortes.
Nous allons les voir dans la suite de ce rapport.

IV. Définition d'un certificat

Un certificat électronique est une carte d'identité numérique dont l'objet est d'identifier une entité physique ou non-physique. Le certificat numérique ou électronique est un lien entre l'entité physique et l'entité numérique. L'autorité de certification fait foi de tiers de confiance et atteste du lien entre l'identité physique et l'entité numérique. Le standard le plus utilisé pour la création des certificats numériques est le X.509. **(1)**

Il existe 4 types de certificats en fonction du niveau de sécurité:

- classe 1 : adresse électronique du demandeur requise;
- classe 2 : preuve de l'identité requise (photocopie de carte d'identité par exemple);
- classe 3 : présentation physique du demandeur obligatoire.
- classe 3+ : identique à la classe 3, mais le certificat est stocké sur un support physique (clé USB à puce, ou carte à puce; exclut donc les certificats logiciels)

Tel qu'on l'utilise en cryptographie et en sécurité informatique, un certificat électronique est un bloc de données contenant, dans un format spécifié, les parties suivantes :

- un numéro de série;
- l'identification de l'algorithme de signature;

- la désignation de l'autorité de certification émettrice du certificat;
- la période de validité au-delà de laquelle il sera suspendu ou révoqué;
- le nom du titulaire de la clé publique;
- l'identification de l'algorithme de chiffrement et la valeur de la clé publique constitués d'une paire de clés asymétriques (comme par exemple RSA);
- des informations complémentaires optionnelles;
- l'identification de l'algorithme de signature et la valeur de la signature numérique.

Un certificat électronique est géré tout au long de son cycle de vie (Certificate revocation list (CRL), Protocole de vérification en ligne de certificat) avec une infrastructure à clés publiques (PKI pour Public Key Infrastructure).

V. La PKI

La PKI, ou Public Key Infrastructure est un ensemble de composants physiques, de procédures humaines et de logiciels en vue de gérer le cycle de vie des certificats numériques ou certificats électroniques. **(2) (3)**

A. Description

Une PKI délivre des certificats numériques. Ces certificats permettent d'effectuer des opérations cryptographiques, comme le chiffrement et la signature numérique qui offrent les garanties suivantes lors des transactions électroniques :

- La confidentialité
- L'authentification
- L'intégrité
- La non-répudiation

B. Principe

1. Les acteurs de la PKI

- Le détenteur d'un certificat, l'utilisateur possède une clé privée, le certificat qui contient cette clé
- L'utilisateur d'un certificat, un serveur par exemple, récupère le certificat et utilise la clé publique dans sa transaction avec le détenteur

- Une autorité de certification (AC), souvent une entité juridique, doit être capable de :
  - Générer des certificats
  - Elle les publie publiquement pour être utilisé de tous.
  - Elle gère la liste des certificats révoqués, ainsi que les archives d'anciens certificats.

2. Fonctions d'un PKI

Les fonctions d'une PKI sont les suivantes :

- Elle doit pouvoir émettre des certificats à des entités préalablement authentifiées.
- Elle est capable de révoquer des certificats, ou les maintenir.
- Elle doit aussi établir, publier et respecter des pratique de certification afin d'établir un espace de confiance
- Les certificats pourront être mis à disposition du public.

3. Création d'un certificat

Pour créer un certificat, les étapes suivantes sont effectuées :

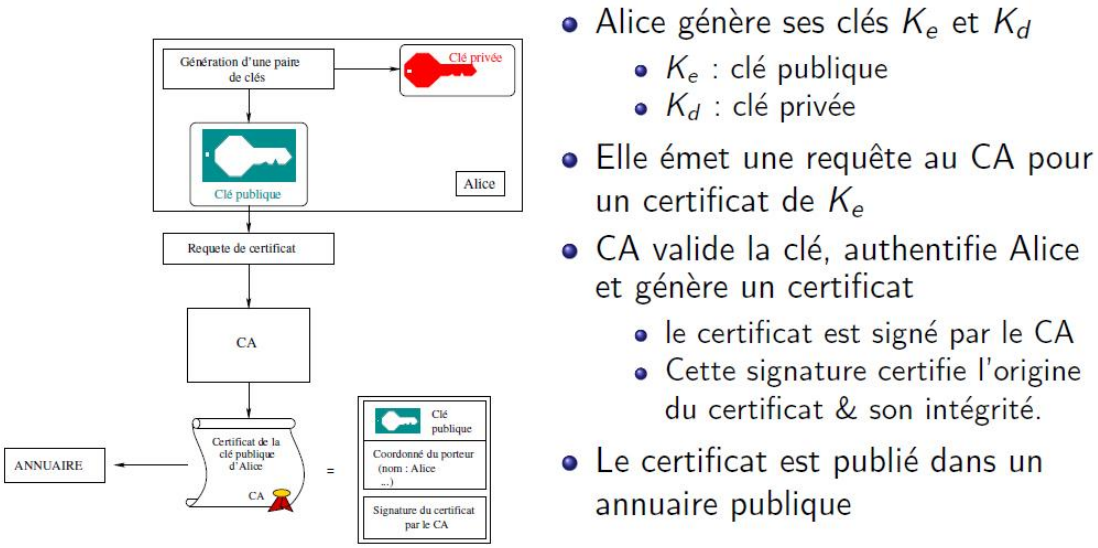


Figure 1 : Exemple de création d'un certificat

4. Emission d'un certificat

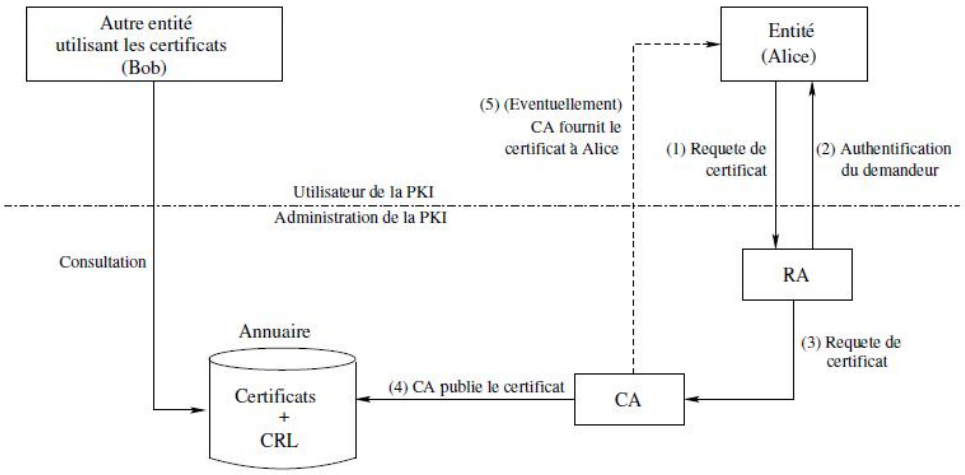


Figure 2 : Emission et utilisation d'un certificat

Alice demande un certificat auprès d'une autorité d'enregistrement (RA) qui valide la clé publique d'Alice et génère un certificat. L'autorité de certification reçoit le certificat d'Alice, et le publie dans l'annuaire de certificat. Une fois ceci fait, n'importe qui peut consulter le certificat d'Alice.

C. Utilisation dans le domaine mobile

L'utilisation de PKI pour téléphone mobile existe, et est appelé Wireless PKI (WPKI). **(4)** Ce protocole a été créé en 2000, mais ne fonctionnait que sur très peu de téléphones. Aujourd'hui tous les smart phones sont capables de gérer ce protocole. Il faut cependant une carte SIM compatible, capable de générer une paire de clé publique/privée et de générer des signatures.

1. Son fonctionnement :

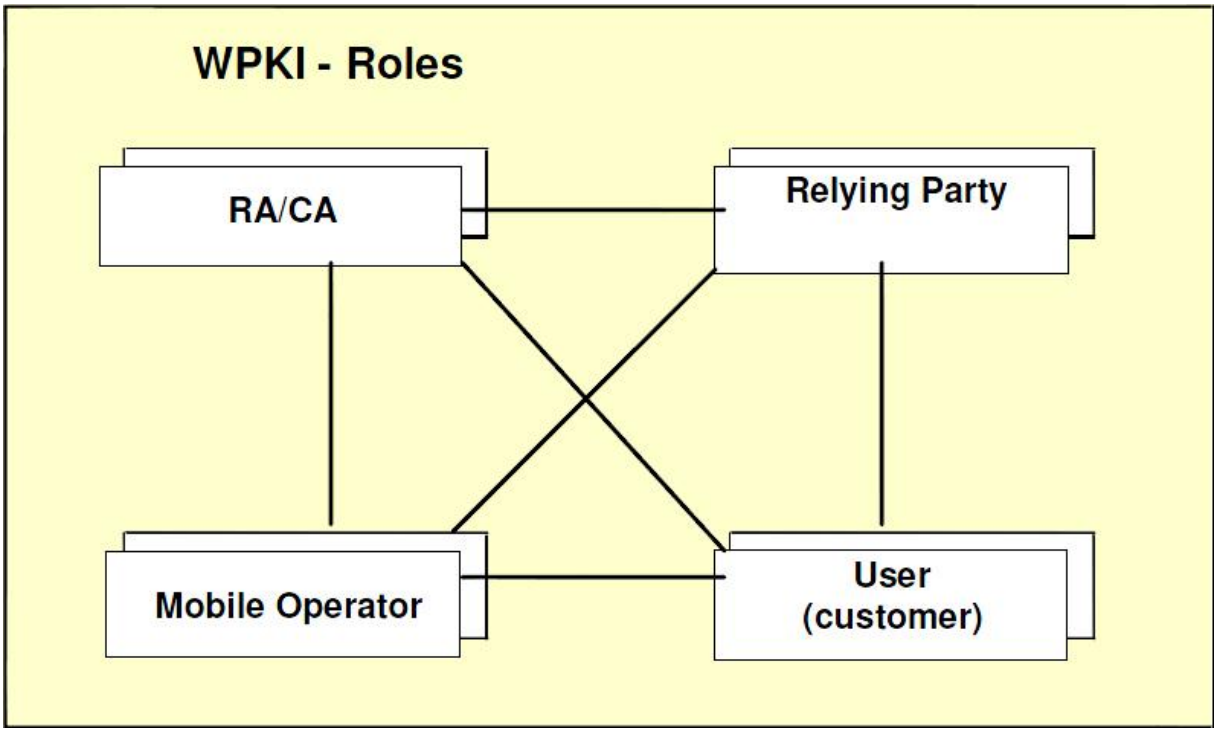


Figure 3 : Schéma des rôles du protocole WPKI.

- Opérateur mobile (MO):

L'opérateur mobile propose un accès mobile, répondant à la carte SIM ayant les fonctionnalités de la WPKI et est responsable de la distribution des demandes de signature à l'utilisateur et reçoit des signatures de réponse de l'utilisateur.

- Autorité d'enregistrement / Certificate Authority (RA / CA):

La RA / CA identifie l'utilisateur et enregistre son Mobile e-ID.

- Relying Party (RP):

La Relying Party offre le service à l'utilisateur en utilisant la structure WPKI.

- Utilisateur:

L'utilisateur utilise le service offert par la Relying Party.

L'opérateur mobile propose une interface pour le RA / CA pour obtenir les clés publiques correspondantes aux clés privées et vérifie les conditions préalables pour l'inscription. Lorsque l'utilisateur a une carte SIM compatible, il prouve son identité en entrant le code d'activation d'inscription prévues dans le processus d'identification ci-dessus et y appose sa signature pour prouver l'existence et la possession d'une clé privée.
Sur la base de ces informations, la RA / CA publie une paire de certificats d'utilisateur final. La RA / CA est aussi responsable de la fonctionnalité de révoquer les certificats d'utilisateur. La RA / CA conclut des accords avec les parties se fiant que l'authentification vous pouvez acheter et services de signature de la RA / CA.

2. Prérequis :

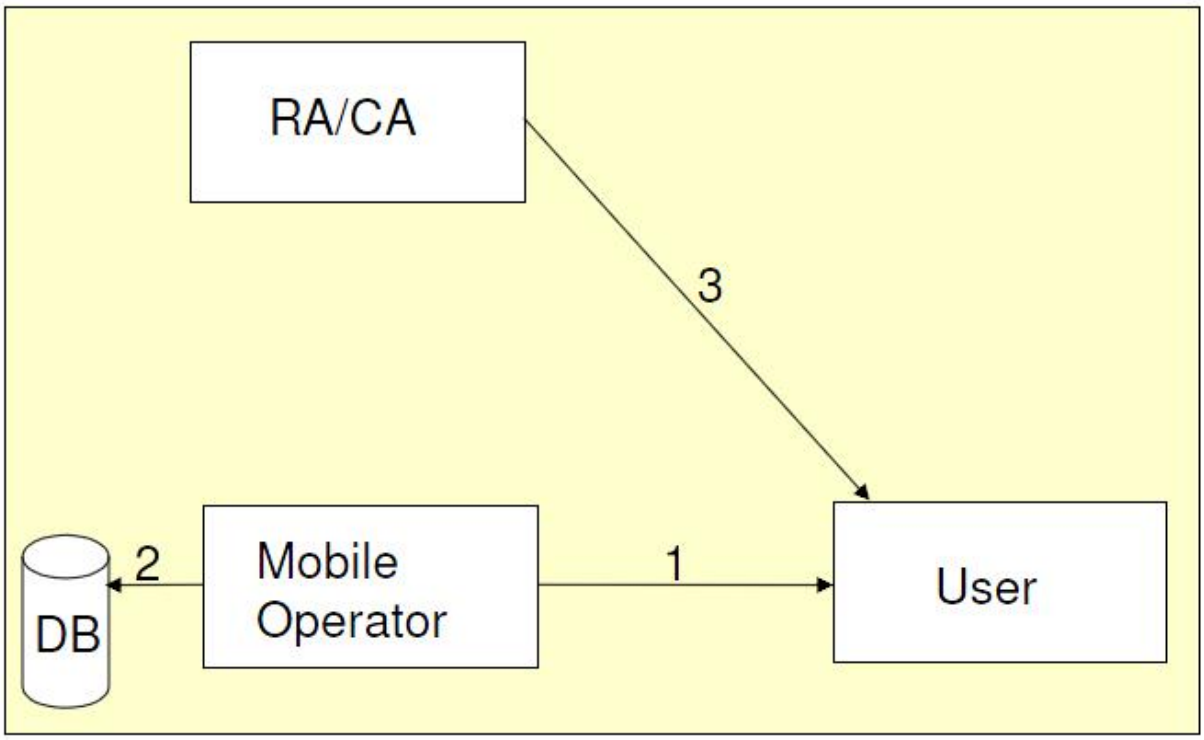


Figure 4 : Schéma du prérequis pour le protocole WPKI.

1) L'opérateur fourni la carte SiM compatible.
2) Si les clés privées sont déjà présentes sur la carte, elles sont placées dans une base de données par l'operateur.
3) La RA / CA effectue un processus d'identification pour identifier de manière sûre l'utilisateur. Le succès de l'opération engendre l'envoie d'un code d'activation d'inscription à l'utilisateur.

3. Inscription :

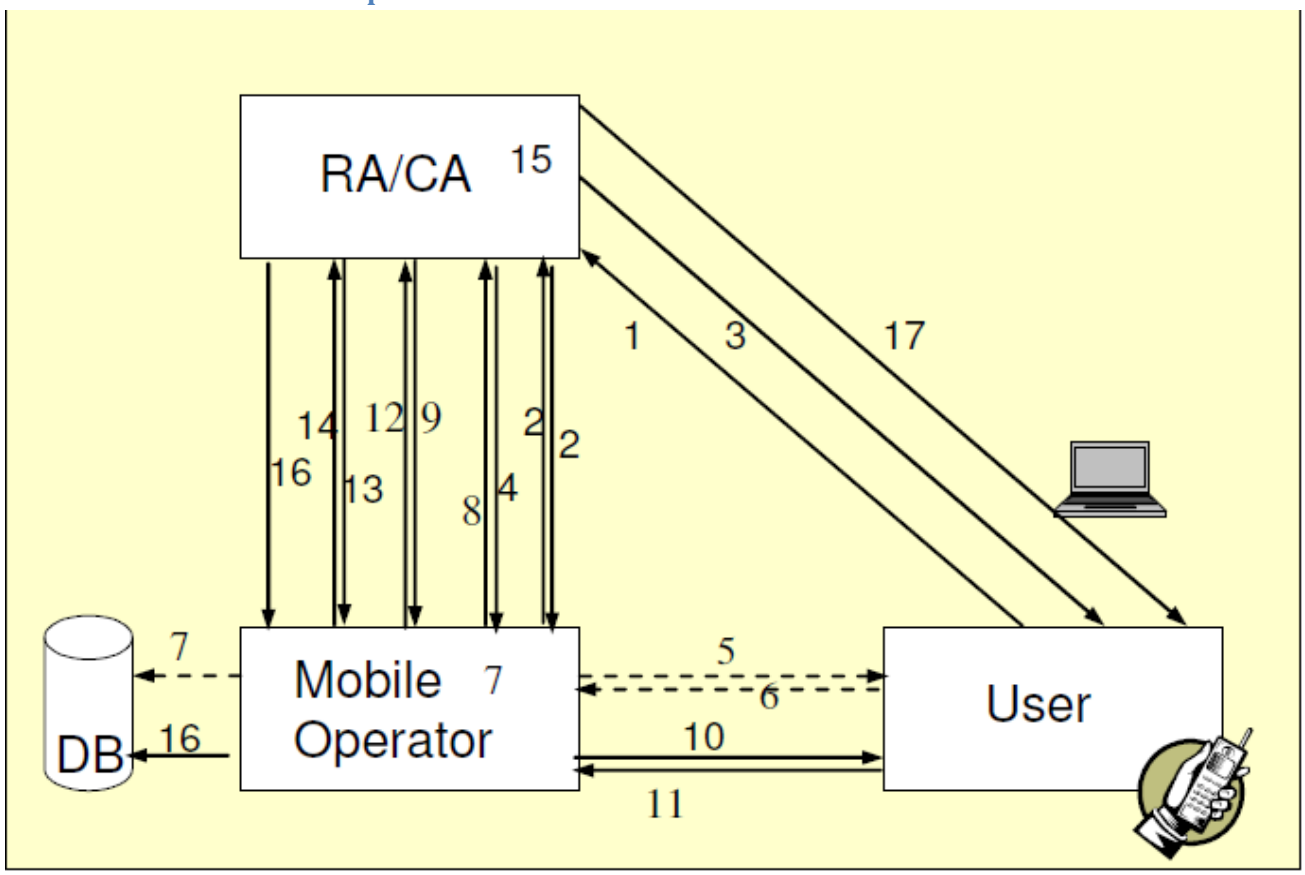


Figure 5 : Schéma d'inscription pour le protocole WPKI.

1) L'utilisateur contacte le RA/CA. Le RA/CA lui demande son numéro de téléphone, et identifie son opérateur mobile.
2) La RA / CA envoie un CAMO.control à l'opérateur pour vérifier si les conditions préalables à pour que l'utilisateur s'enregistre soit remplies. L'opérateur renvoie le résultat de la vérification.
3) Le RA/CA informe l'utilisateur sur la façon de s'inscrire.
4) Le RA/CA demande à l'opérateur d'inscrire l'utilisateur.
5) L'operateur vérifie si l'utilisateur a des clés utilisables. Dans le cas où elles sont absentes, l'operateur envoie une commande d'initialisation de clés.
6) Si les clés ont étés générées à l'étape 5, l'opérateur mobile récupère la clé publique de l'utilisateur.
7) Si les clés ont été générées à l'étape 5, l'operateur créé un certificat pour l'appareil et le stocke dans une base de données.
8) L'operateur envoie le certificat de l'appareil au RA/CA pour la non-répudiation.
9) Le RA/CA fait une demande auprès de l'opérateur d'une signature.
10) L'opérateur envoie un message à l'utilisateur avec la demande de signature du 9) et le code d'activation à signer.
11) L'utilisateur entre le code d'activation et le signe avec sa clé privée. Ce code est retourné à l'opérateur, puis au RA/CA.
12) Le RA/CA reçoit le code d'activation signé par l'utilisateur, et le compare avec le code qui a été donné pendant la phase de prérequis.
13) Le RA/CA se connecte auprès de l'opérateur et demande les clés publiques.

14) L'opérateur mobile lui répond en envoyant le certificat de l'appareil signé.
15) Le RA/CA utilise ces informations pour produire des certificats qui seront stockés, accompagnés d'informations telles que le numéro de MSISDN et l'opérateur mobile de l'utilisateur.
16) Le RA/CA demande une connexion « business » à l'opérateur. L'opérateur enregistre des informations comme le RA/CA qui communique avec lui et les clés.
17) Le RA/CA informe l'utilisateur que l'inscription s'est correctement déroulée.

4. Utilisation :

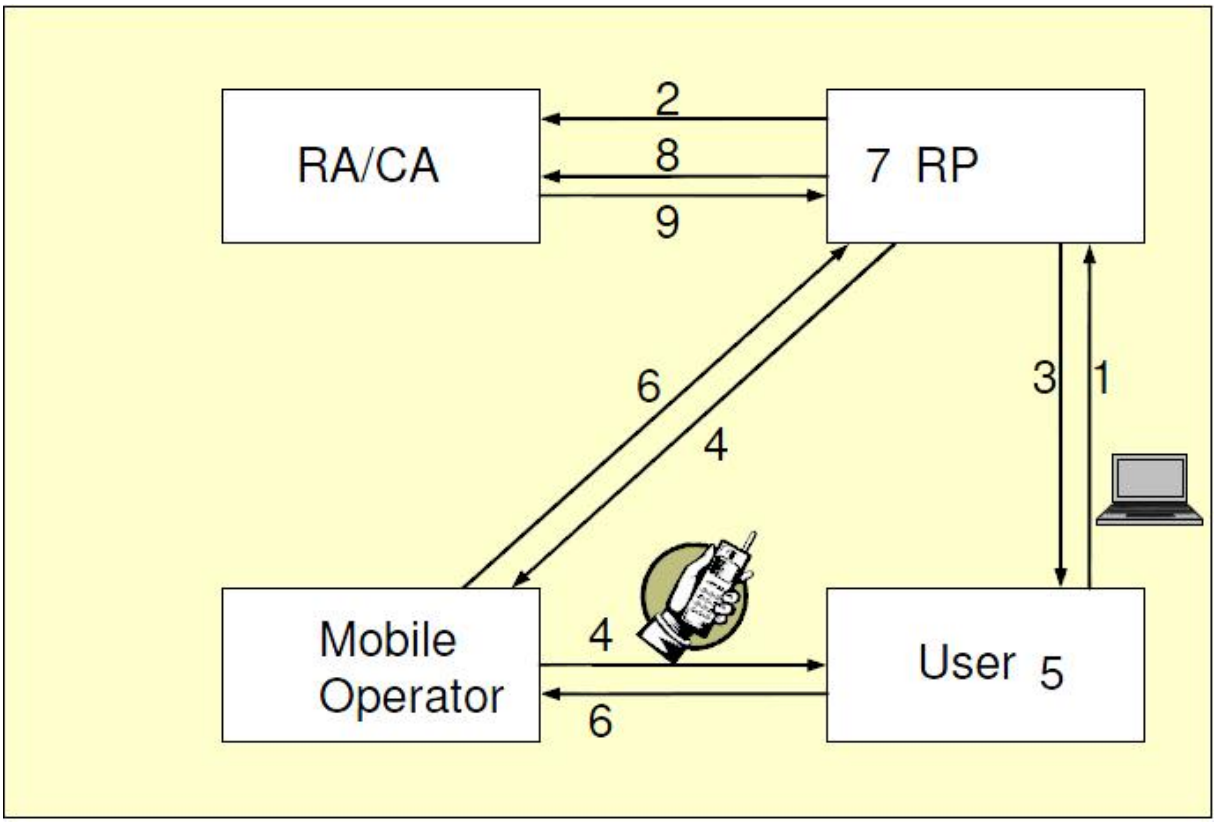


Figure 6 : Schéma d'utilisation du protocole.

Les étapes ci-dessous sont valables pour le cas où l'utilisateur utilise séparément un tunnel d'information et un tunnel de sécurité mais aussi lorsque l'utilisateur utilise le même tunnel pour l'information et la sécurité.

1) L'utilisateur se connecte au RP sur le tunnel d'information. Quand l'utilisateur veut s'authentifier ou créer une signature, la RP demande lui demande des informations à propos de son téléphone portable, pour l'identifier et récupère son MSISDN (Mobile Station ISDN Number est le numéro « connu du public » de l'usager GSM).
2) On utilise alors le MSISDN de l'utilisateur comme identifiant, la RP récupère le certificat de l'utilisateur utiliser pour la vérification de la signature et l'URL vers laquelle la demande de signature doit être envoyé, La RA / AC doit renvoyer uniquement des certificats valables. Si l'utilisateur a de multiple certificats il faut se mettre d'accord sur le certificat à utiliser pour la transaction.

3) La RP utilise le canal d'information pour afficher les informations que l'utilisateur doit signer sur le canal de sécurité. Le RP envoie également un code de contrôle et demande à l'utilisateur d'entrer le code de contrôle sur le terminal mobile et signer les informations avec sa clé privée.
4) La RP envoie une demande de signature à l'opérateur mobile pour accéder au canal de sécurité du terminal mobile de l'utilisateur.
5) Si un code de contrôle est utilisé, l'utilisateur entre le code de contrôle sur son mobile. Le code de contrôle est ajouté aux données à signer (DTBS). Le TTBS est affichée à l'utilisateur qui la signe en entrant la clé privée à six chiffres PIN.
6) Le message signé est renvoyé à l'operateur qui restructure la signature pour être conforme à une norme et la transmet au RP.
7) La RP peut ainsi vérifier la signature et valider le certificat de l'utilisateur.
8) LA RP valide le certificat auprès de la RA.
9) La RA répond par son accord.

D. Première mise en œuvre

Une équipe de 3 chercheurs, Marko Hassinen, Konstantin Hyppönen, and Keijo Haataja de l'Université de Kuopio, a réalisé, en 2006, un système de paiement sur mobile, via une PKI. **(5)** Pour leurs tests, ils ont utilisés une PKI fournie par le centre d'enregistrement finlandais.
Les clés privées ne sont stockées que dans la carte SIM, la carte n'étant pas falsifiable, les clés privées ne peuvent pas être « capturées ». Les clés publiques des utilisateurs sont disponibles dans une base de données et peuvent être téléchargés.
Chaque personne se voit attribuer un unique certificat par le centre d'enregistrement. La carte SIM est capable de signer des informations, alors que pour le cryptage/décryptage se fait par le téléphone en lui-même.

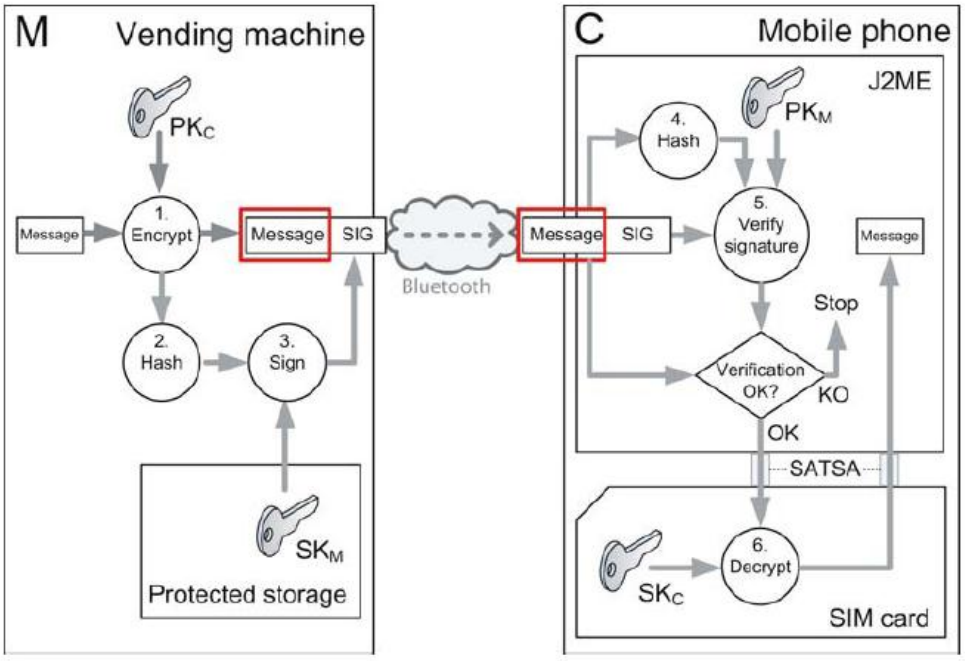


Figure 7 : Un exemple d'échange de message sécurisé

Voilà un schéma montrant le fonctionnement de leur authentification. Une machine en ligne (banque, vente à distance, etc.) crypte son message, et le signe. Le message est ensuite envoyé. Le téléphone mobile vérifie la signature, si elle est correcte, le téléphone consulte la clé privée stockée dans la carte SIM, et décrypte le message.

Pour la suite de l'explication, on note :

- C est le client
- M est le marchand
- B est la banque
- ID_x est l'identité de X
- SK_x est la clé secrète de X
- PK_x est la clé publique de X
- $Cert_x$ est le certificat de X, contenant la clé publique de X
- $\{m\}_k$ est la méthode de cryptage du message m avec la clé K
- SIG_{XY} est la signature numérique généré par X, qui vérifie Y
- H est une fonction de hachage, utilisant le protocole SHA-1

Le paiement fonctionne comme suit.

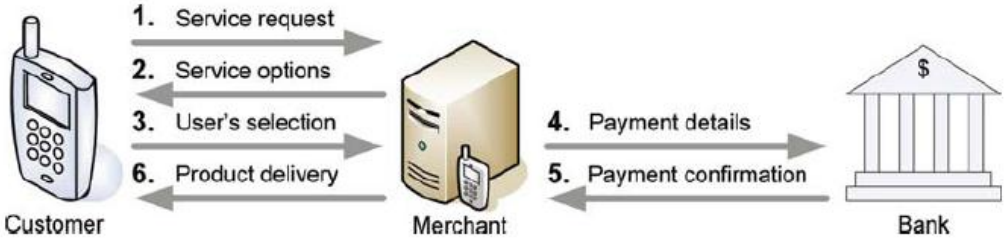


Figure 8 : Modèle de paiement virtuel

1) Le client initialise le protocole avec le marchant.

$$C \xrightarrow{\text{Service request}} M$$

2) Le marchand envoie une liste d'option sur le mobile. Cette liste contient de brèves descriptions des produits et leurs prix. Le certificat du marchand est attaché à cette liste.

$$M \xrightarrow{\text{Service options}|\text{Cert}_M} C$$

3) Le client est invité à sélectionner les produits qu'il veut. Ces informations sont envoyées au commerçant. Le tout est signé par la clé privée du client.

$$C \xrightarrow[\text{SIG}_{C_B}=\{H(TS_C|ID_M|AM)|H(PD|N_C)\}_{SK_C}]{\text{MSG}=\left\{PD|N_C|TS_C|\{H(PD|TS_C)\}_{SK_C}|ID_B|\text{SIG}_{C_B}\right\}_{PK_M}} M$$

4) La demande de paiement. Les informations de paiement sont signées à l'aide de la clé privée du commerçant et chiffre avec la clé publique de la banque.

$$M \xrightarrow[\mathrm{SIG}_{M_B}=\{H(ID_M|ID_C|TS_C|AM|H(PD|N_C))\}_{SK_M}]{\mathrm{MSG}=\{ID_M|ID_C|TS_C|AM|H(PD|N_C)|\mathrm{SIG}_{M_B}|\mathrm{SIG}_{C_B}\}_{PK_B}} B$$

5) La confirmation de paiement. Le montant indiqué est transféré du compte client au compte du commerçant. Un message de confirmation est envoyé au commerçant. Ce message est signé avec la clé privée de la banque, et est crypté avec la clé publique du commerçant.

$$B \xrightarrow{\mathrm{MSG}=\{H(ID_M|ID_C|TS_C|AM|H(PD|N_C))\}_{SK_B}} M$$

6) La livraison du produit. Apres que le commerçant ai vérifié les informations reçues, et si le paiement a été effectué correctement, il délivre le produit au client. Le client reçoit alors un message lui disant que le paiement a bien été effectué, et que le produit a été livré.

$$M \xrightarrow{\mathrm{MSG}=\{H(ID_M|ID_C|TS_C|AM|H(PD|N_C))\}_{SK_B}} C$$

E. Deuxième mise en œuvre de PKI sur mobile

Une seconde mise en œuvre, faite par Jong Sik Moon, Deok Gyu Lee, and Im-Yeong Lee de l'Université d'informatique et d'ingénierie de Soonchunhyang, en 2009. La méthode proposée est chiffrée en utilisant la méthode basée sur des clés publiques pour sécuriser des attaques extérieures pendant les déplacements et la communication. Ces clés sont fournies avec une signature empêchant la falsification des données. Cette méthode permet d'accéder au réseau domestique via des réseaux externes, de pouvoir recevoir un service continu d'authentification avec les tickets et valeurs d'itinérance. L'authentification est rapide, basé sur les tickets d'itinérance. Même en utilisant des serveurs externes, les communications sont sécurisées. **(6)**

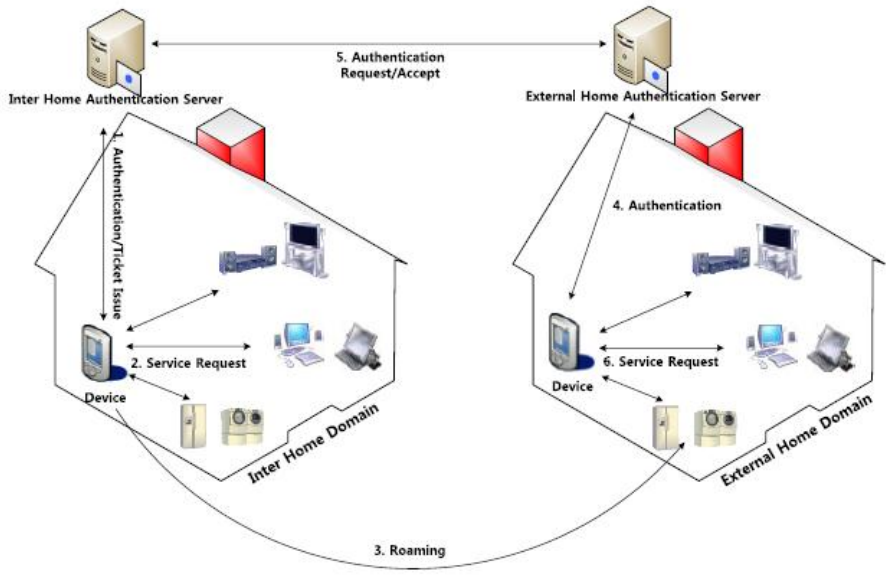


Figure 9 : Schéma du dispositif d'authentification.

Ce protocole est constitué d'une phrase d'authentification dans le réseau local avec l'émission d'un ticket et une phrase d'authentification avec génération de clés symétriques et la synchronisation des valeurs entre l'appareil qui veut se connecter et le serveur d'authentification du réseau domestique.

- L'authentification et l'émission de ticket dans le réseau domestique

Cette phase est découpée en 5 étapes. Lors de ces étapes, l'appareil demande au serveur d'authentification une authentification. Le serveur délivre un ticket d'itinérance si la validité de l'appareil est validée.

1) l'appareil qui veut se connecter et le serveur génèrent tous les 2 une clé publique et une clé privée.
2) l'appareil crypte le mot de passe et la valeur du compteur avec la clé publique du serveur et le transmet au serveur avec son ID.
3) le serveur décrypte le message transmis, génère le mot de passe, et vérifie qu'il est bien identique à celui reçu. Si c'est le cas, l'appareil est authentifié auprès du serveur.
4) Si l'authentification a réussie, le serveur génère une valeur d'itinérance et un ticket d'itinérance. Le serveur crypte ensuite le billet et la valeur d'itinérance avec la clé publique de l'appareil et lui transmet le message crypté.
5) L'appareil décrypte le message, génère la valeur d'itinérance, et la compare avec celle reçue.

VI. Kerberos

A. Description

Kerberos est un protocole d'authentification réseau créé au Massachusetts Institute of Technology (MIT). Kerberos utilise un système de tickets au lieu de mots de passe en texte clair. Ce principe renforce la sécurité du système et empêche que des personnes non autorisées interceptent les mots de passe des utilisateurs.
L'ensemble repose sur des clés secrètes (chiffrement symétrique).

B. Principe

Dans un réseau simple utilisant Kerberos, on distingue plusieurs entités :

- le client
- le serveur de services
- le service d'émission de tickets (TGS pour *Ticket-Granting Service)*
- Le service d'authentification (AS pour Authentication Service)
  (Ces deux services réunis forment le KDC (*Key Distribution Center*)

Le client veut accéder à un service proposé par le serveur de services. **(7)**

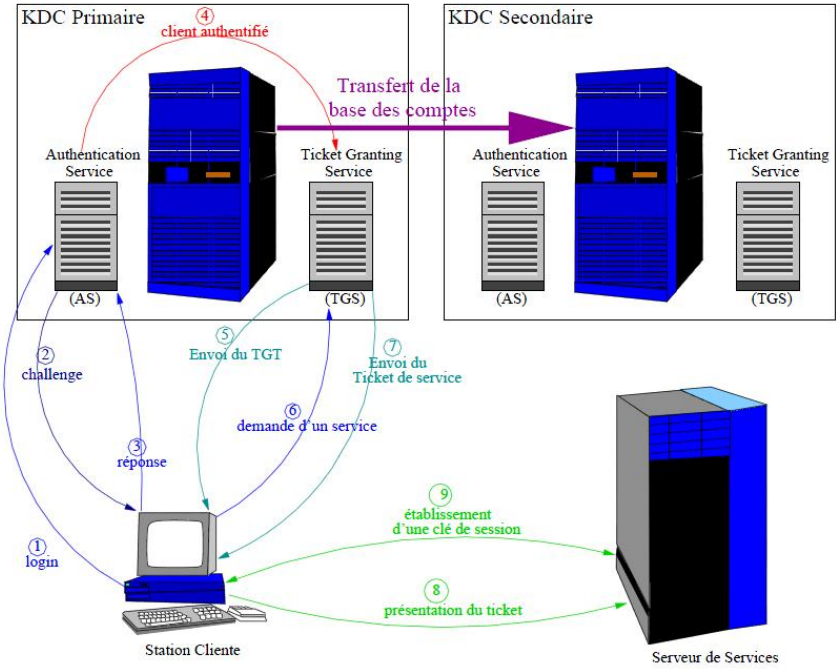


Figure 10 : Schéma du fonctionnement de Kerberos

Lorsque le client veut accéder au serveur, il envoie au KDC un message contenant son identifiant, son adresse réseau et un horodatage (pour éviter les attaques basées sur le temps). Le serveur d'authentification lui fournit alors des informations, cryptées avec la clé du client. Ces informations contiennent entre autre un ticket de session (TGT), crypté avec la clé du TGS. Le client ne peut en aucun cas décrypter ce ticket.

Une fois cela fait, il peut demander l'accès au serveur B. Pour cela, il envoie son TGT au serveur d'émission des tickets (TGT). Si le client est authentifié, le TGS lui envoie un ticket de service crypté avec la clé du service. Il contient également une clé de session qui sera utilisée entre le client et le serveur qui offre le service.
Une fois ce ticket reçu, le client le déchiffre et utilise le ticket de session pour contacter le service. Le service, déchiffre à son tour le ticket.
Le client est authentifié auprès du service.

C. Utilisation dans le domaine mobile

Kerberos existe pour appareil mobile, notamment très utilisé chez Apple, les librairies pour développer une application utilisant le protocole sont incluses dans le SDK de l'IPhone. Cependant il n'existe pas d'application sur le store officiel, mais on peut trouver une application s'appelant Kerberos, développé par saurik (développeur underground), utilisable avec un IPhone jailbreak, permettant d'utiliser ce protocole. **(8)**

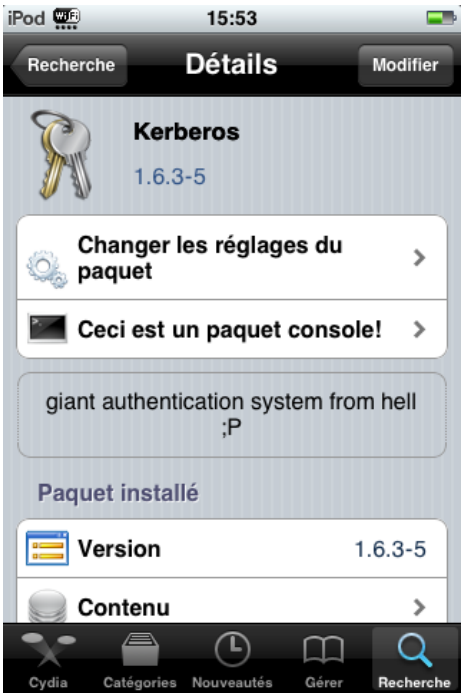


Figure 11 : Application Pour IPhone

Il est possible de l'utiliser sur Windows mobile depuis la version 5. Cependant il parait très gourmand. En effet il faudrait 15 secondes pour que l'appareil reçoive le ticket initial.

D. Mise en œuvre

Windows mobile intègre depuis la version 5 le protocole d'authentification Kerberos. Sur iPhone il est impossible de l'utiliser de manière « légale ». Kerberos est codé en langage C, le code est disponible pour Windows et pour Mac sur le site de Kerberos. **(9)**

Une équipe de l'Université d'Australie occidentale a utilisé le protocole Kerberos dès 2007 pour s'authentifier sur un réseau Ad-Hoc. **(10)** Ils l'ont appelé Kaman. Ils sont partis du principe que :

- Tous les utilisateurs ont une clé secrète ou un mot de passe connu uniquement d'eux même.
- Tous les serveurs connaissent les mots de passe utilisateur hachés
- Tous les serveurs se partagent une clé secrète entre eux.

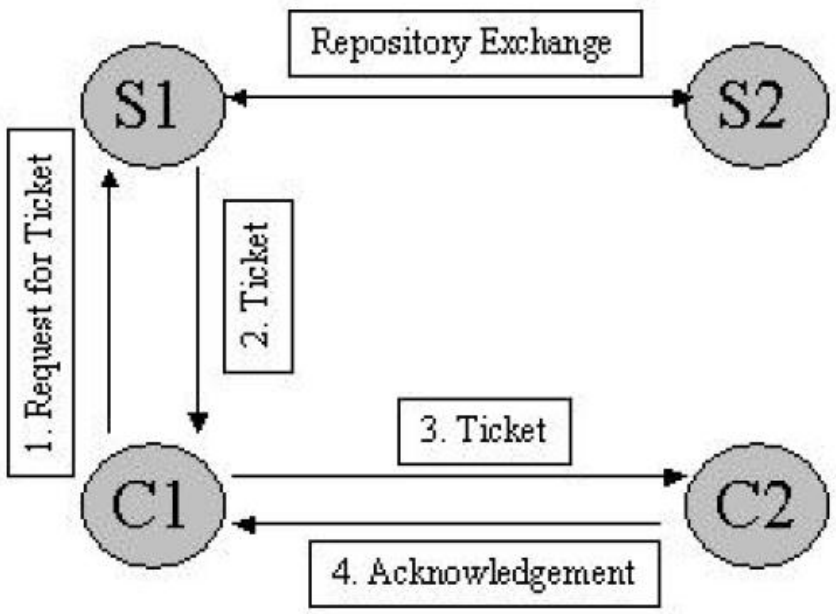


Figure 12 : Schéma de fonctionnement de Kaman

6) Dès qu'un client C1 veut accéder au client C2 il doit faire une requête au serveur Kaman S1.
   - (Options, ID_{C1}, ID_{C2}, Times, Nonce)
7) Le serveur crée un ticket qui contient la clé de session et l'envoie à C1.
   - (ID_{C1}, $Ticket_{C2}$, {$K_{C1,C2}$, Times, Nonce, ID_{C2} }K_{C1})
8) Le client C1 envoie à son tour le ticket à C2.
   - Options, $Ticket_{C2}$, $Authenticator_{C1}$
9) Le client C2 reçoit le ticket et établie une session sécurisée entre les deux clients en utilisant la clé de session préalablement fournie par le serveur.
   - {TS, Subkey, Seq# }$K_{C1,C2}$

$Ticket_{C2} = \{Flags, K_{C1,C2}, ID_{C1}, AD_{C1}, Times\}K_{C2}$

Néanmoins, ce protocole est comme nous l'avons dit prohitif du fait de la consommation nécessaire en temps de calcul.

VII. Clé USB – Carte mémoire

A. Description

La clé USB est utile dans de nombreux domaines. On peut aussi l'utiliser pour s'authentifier. Par exemple si la clé USB est connectée à l'appareil (ordinateur par exemple), l'utilisateur va alors pouvoir utiliser

l'appareil. La clé sert donc de login et de mot de passe pour s'authentifier sur la machine. De la même manière, la carte mémoire peut servir d'authentifiant.

B. Principe

La clé USB contient les données d'authentification d'une personne. Celle-ci veut s'identifier sur sa machine. Le simple fait d'insérer la clé USB dans la machine, va authentifier l'utilisateur, qui va pouvoir utiliser la machine normalement. Ce système existe sous Linux, via le logiciel Pam-USB.
Le principe de ce logiciel est qu'il contrôle le port USB continuellement. Si la clé est présente, la machine peut fonctionner. Dans le cas où l'utilisateur enlève la clé, la session se verrouille, rendant l'ordinateur inutilisable.
Il est possible d'utiliser un mot de passe permettant d'utiliser la clé USB, ce qui empêcherai un potentiel voleur de pouvoir s'authentifier et utiliser la machine juste avec la clé USB.

Sur téléphone mobile, on utilise des cartes mémoire. Le procédé est identique. En ayant la carte insérée dans le téléphone, l'identification peut être réalisée.

L'avantage de ce système, est que la carte mémoire peut être utilisée par plusieurs appareils, comme un téléphone, un ordinateur, un PDA etc.

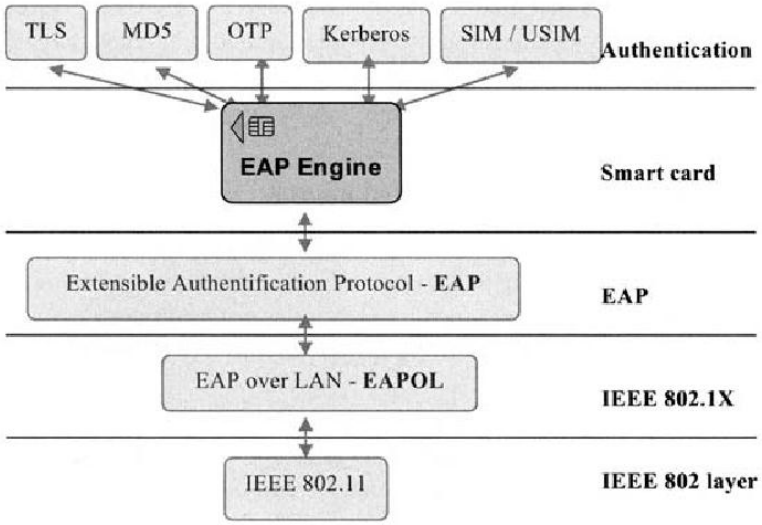
Figure 13 : Utilisation d'une carte mémoire.

C. Utilisation dans le domaine mobile

Trois français ont imaginés un protocole d'authentification par carte mémoire. Elle s'appuie sur une authentification par EAP **(11).** Ce protocole d'authentification extensible est un protocole d'authentification qui supporte de nombreuses méthodes d'authentification, telles Kerberos, les mots de passe à usage unique, les PKI, et les carte mémoire.
Pour leur protocole, il se base sur EAP/TLS. C'est un système de certificat, de la même manière que les

PKI. Un certificat est généré par un serveur, validé par lui-même, et stocké dans la carte mémoire. C'est plus puissant qu'un simple protocole PKI, car si l'utilisateur est révoqué, l'accès au réseau est aussi révoqué.

D. Mise en œuvre



La méthode d'authentification, quelle qu'elle soit est intégrée dans la carte mémoire. Puis le protocole EAP prend la relève, et authentifie le téléphone. Ainsi, le téléphone est connecté.

VIII. La biométrie

A. Description

La biométrie est la science qui permet d'identifier automatiquement un individu en se basant sur ses caractéristiques physiologiques ou comportementales. Généralement, on distingue deux catégories de méthodes d'authentification biométrique: les méthodes basées sur les caractéristiques physiques telles que visage, voix, iris, rétine, pouce, forme de la main et de l'oreille, ADN, et celles basées sur les caractéristiques comportementales comme la signature, la manière de marcher ou de taper sur un clavier.

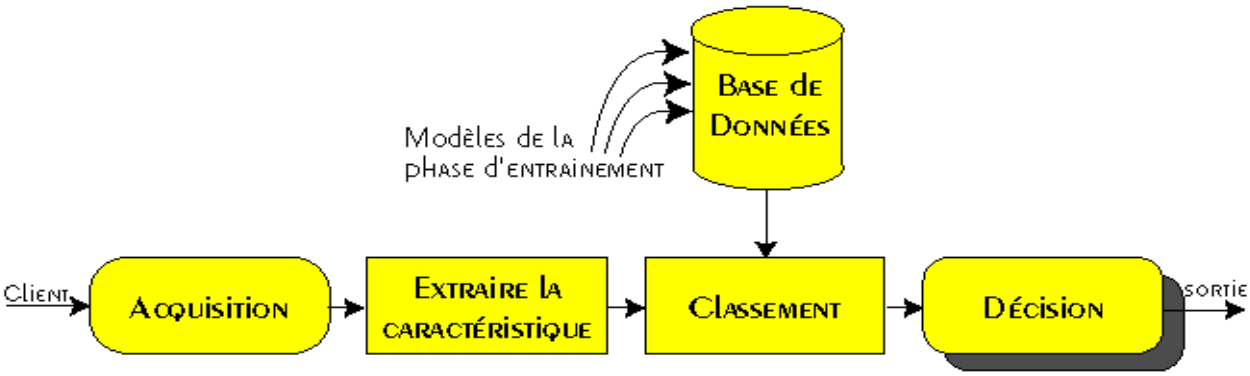


Figure 14 : Schéma du fonctionnement de la biométrie.

L'authentification se fait en 4 étapes.

- L'acquisition : un système d'acquisition équipé d'un capteur est utilisé pour acquérir une caractéristique spécifique de l'utilisateur, par exemple: une caméra ou un microphone dans le cas de la voix.

- L'extraction : Ayant une image ou une voix en entrée**,** une étape de segmentation permet d'extraire la caractéristique dont le processus d'authentification a besoin. Par exemple: extraire le visage du fond d'une image dans le cas de l'identification de visage.

- La classification : En examinant les modèles stockés dans la base de données, le système collecte un certain nombre de modèles qui ressemblent le plus à celui de la personne à identifier, et constitue une liste limitée de candidats. Cette classification intervient uniquement dans le cas d'identification car l'authentification ne retient qu'un seul modèle (i.e. celui de la personne proclamée).

- La décision : Dans le cas de l'identification, il s'agit d'examiner les modèles retenus par un agent humain et donc décider. En ce qui concerne l'authentification, la stratégie de décision nous permet de choisir entre les deux alternatives suivantes: l'identité de l'utilisateur correspond à l'identité proclamée ou recherchée ou elle ne correspond pas.

Il existe plusieurs méthodes d'authentification biométrique.

Les empreintes digitales est le premier procédé utilisé. La formation des empreintes dépend des conditions initiales du développement embryogénique, ce qui les rend uniques à chaque personne et même à chaque doigt. L'image d'empreinte est prise soit selon le mode traditionnel qui est un scanning du doigt couvert d'encre.

Le visage est une technique très populaire. Elle reste la plus acceptable puisqu'elle correspond à ce que les humains utilisent dans l'interaction visuelle. Les caractéristiques jugées significatives pour la reconnaissance du visage sont: les yeux, la bouche et le tour du visage. Le nez ne présente pas de particularité pour la vue de face. La méthode d'authentification du visage est sensible à la variation de l'éclairage et le changement de la position du visage lors de l'acquisition de l'image. De plus, il est recommandé d'utiliser le même type de caméra dans plusieurs applications.

La voix utile dans certain cas. La reconnaissance d'un locuteur offre l'avantage d'être bien acceptée par l'utilisateur, quelle que soit sa culture. De plus, s'il s'agit de sécuriser une transaction téléphonique, la voix est la seule information disponible. La phase d'apprentissage utilise généralement plusieurs modèles du locuteur pour tenir compte de la variabilité de son discours. La phase de reconnaissance consiste à segmenter le signal de parole en unités qui sont ensuite classées. Ces unités peuvent être des mots ou des phonèmes. La performance est sujette à la qualité du signal, qui dépend de la variabilité de la voix du locuteur dans le temps comme dans le cas de maladie, des états émotionnels et de l'âge, des conditions d'acquisition de la voix telles que le bruit et la réverbération, de la qualité des équipements tels que le microphone, sans oublier le fait que différentes personnes peuvent avoir des voix similaires.

La rétine, la méthode utilisée dans les films. Il a été montré que chaque œil possède en sa rétine un arrangement unique des vaisseaux sanguins. La technique basée sur la rétine utilise la texture de ces vaisseaux. Cette technique est relativement ancienne, et a été utilisée essentiellement dans des environnements de haute sécurité, comme l'accès aux sites nucléaires militaires. Cette méthode requiert une collaboration étroite de la part du sujet, car il doit placer son œil extrêmement près de la caméra. Cette caractéristique a limité le développement d'applications grand public.

L'iris. Si la couleur, la forme et l'apparence générale de l'iris est déterminée génétiquement, sa texture détaillée est propre à chaque individu, voire même à chaque œil. De plus, cette texture est stable et ne peut être modifiée sans perte importante des capacités visuelles. L'incorporation de techniques de localisation de l'œil permet de relaxer la contrainte à laquelle l'utilisateur est soumis, et son utilisation est envisagée dans les distributeurs de billets de banque et pour l'accès sécurisé à Internet.

Enfin la main. La silhouette de la main est une caractéristique de chaque individu. La forme de la main est acquise par un scanner spécialisé, généralement à infrarouge. Des paramètres tels que la longueur des doigts, leur épaisseur et leur position relative sont extraits de l'image et comparés à la base de données. Cette biométrie est toutefois sujette aux modifications de la forme de la main liées au vieillissement.

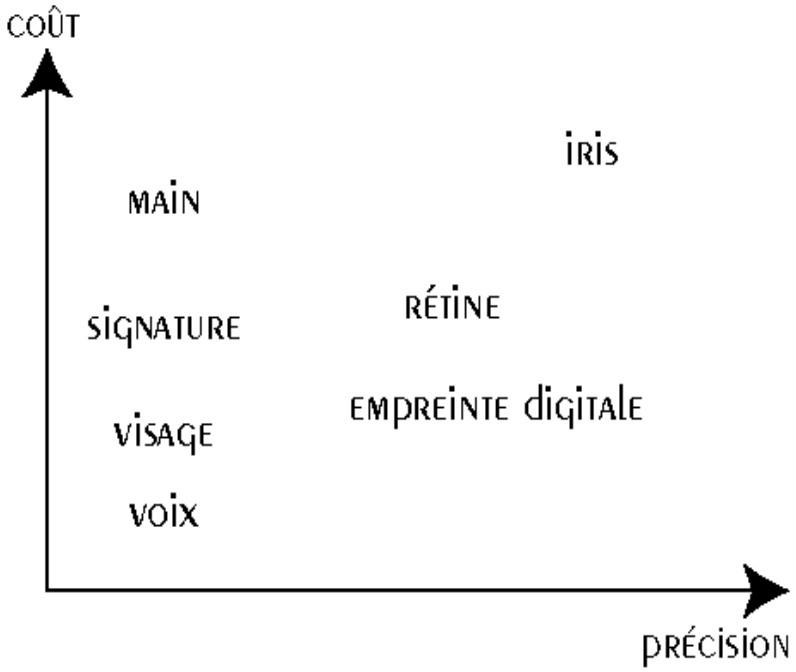


Figure 15 : Graphique distinguant les types d'authentification biométrique.

Voilà un graphique montrant les différentes méthodes citées plus haut, en fonction de leur précision et de leur cout.

D'autres méthodes sont en développement comme la biométrie basée sur la géométrie de l'oreille, les odeurs, les pores de la peau et les tests ADN.

B. Utilisation dans le domaine mobile

Que ce soit sur Windows mobile, Androïd ou sur L'iPhone, il existe des applications permettant de sécuriser des données ou de verrouiller le téléphone par empreinte digitale.

Quelques applications existent sur IPhone. Le problème étant que l'écran ne capte que le fait d'être touché. De ce fait il lui est impossible de capturer des données précises sur un doigt. En juillet 2009 Apple a déposé un brevet pour la reconnaissance digitale sur son téléphone.

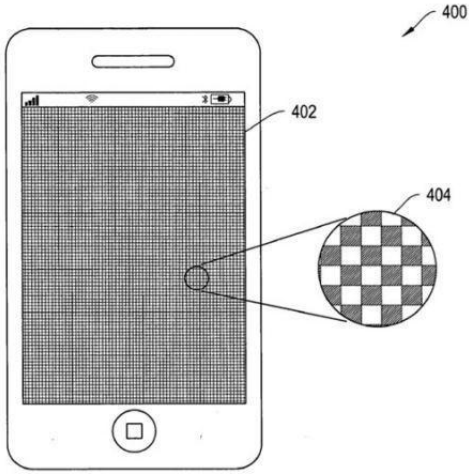


Figure 16 : Schéma du prototype du futur écran de l'IPhone.

Cette photo ci-dessus nous montre des petits pigments sur la surface de l'écran. Cette nouveauté est pour le moins très intéressante. En effet, ces pigments servent à donner du relief, chacun étant mobile, l'association de ces derniers à l'environnement affiché sur l'écran donnerait une sensation de relief et cela aurait également l'avantage de ne pas être statique, ce qui signifie que l'écran pourrait se modifier en fonction de ce qu'il affiche. Le premier brevet déposé par Apple concernant cette technologie avait pour but d'identifier l'utilisateur afin qu'aucun mot de passe ne soit requis sur l'écran de verrouillage. **(12)**

Il en va de même pour les appareils fonctionnants sous Windows Mobile. Les écrans ne sont pas capables de capturer d'informations précises. Certains téléphones sont ainsi équipés d'un lecteur d'empreinte, notamment le Toshiba G500.

Pour ce qui est d'Androïd, Sagem et Upek, spécialiste du contrôle d'identité par empreinte digitale, travaillent ensemble pour créer un mobile basé sur Androïd**,** dont les caractéristiques comprennent la capacité de reconnaître des empreintes digitales. Il sera présenté en fin d'année. **(13)**

IX. Mots de passe

A. Description

Le mot de passe est souvent employé pour réaliser l'authentification d'une personne.
La méthode d'authentification par mot de passe MD5 reste le plus courant.

B. Principes

Entités requises :

- Un client
- Un serveur générant et connaissant les mots de passe
- Un point d'accès

Le serveur génère un login et un mot de passe pour ses clients. Ces logins et mots de passe sont envoyés au client qui lui correspond.
Si un client veut accéder à une ressource, comme par exemple un réseau Wifi, il va devoir s'authentifier auprès du point d'accès. Pour ce faire, le client communique au point d'accès son login et mot de passe. Le point d'accès va alors le transmettre au serveur d'authentification. Celui-ci va comparer les données qu'il a reçues, avec celles qu'il avait déjà en mémoire. Si les deux correspondent, alors le client est authentifié.

C. Utilisation dans le domaine mobile

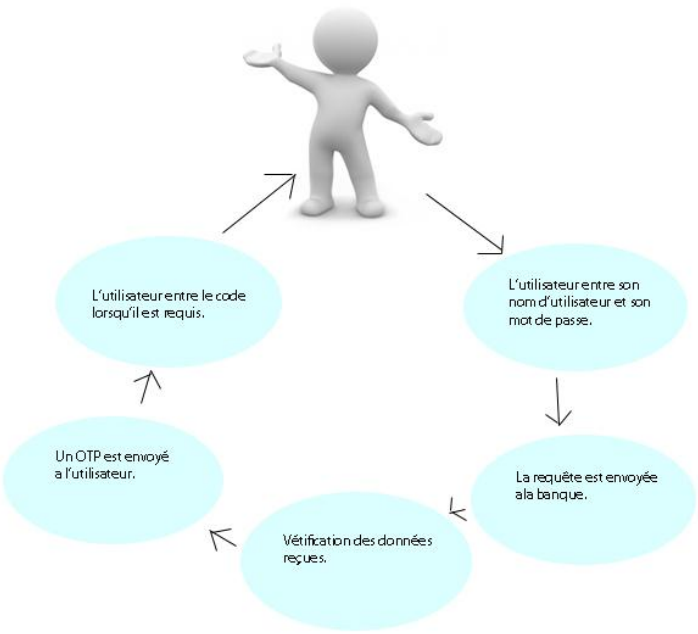


Figure 17 : Utilisation d'un OTP par SMS.

Cette méthode est très fréquemment utilisée. Notamment si l'on veut accéder à un site sécuriser. Le site en question envoie un SMS (Short Message Service) à l'utilisateur, contenant le mot de passe à usage unique (One Time Password OTP). Celui-ci a une durée très limitée pour l'utiliser et s'authentifier. **(14)**

D. Mise en œuvre

Ces mots de passe générés sont calculés à partir de trois données :

- Une donnée publique (mot ou phrase courte par exemple), choisie par l'administrateur. On appelle cela aussi la semence, ou seed en anglais.
- Un numéro de séquence : C'est un nombre relatif au numéro de connexion. C'est un compteur, tout simplement. C'est ce paramètre qui rend le mot de passe unique : L'OTP de la connexion n°587 n'est pas le même que la connexion n°586 ou 588.
- Un mot de passe utilisateur, connu de lui seul, qui servira à l'authentifier.

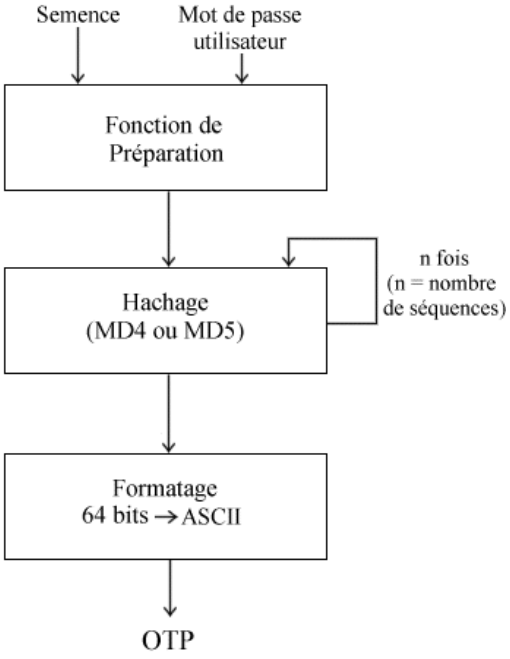


Figure 18 : Calcul des mots de passe à usage unique.

X. VPN

A. Description

Le réseau privé virtuel (Virtual Private Network en anglais, abrégé en VPN) est vu comme une extension des réseaux locaux et préserve la sécurité logique que l'on peut avoir à l'intérieur d'un réseau local. Il correspond en fait à une interconnexion de réseaux locaux via une technique de « tunnel ». On parle de VPN lorsqu'un organisme interconnecte ses sites via une infrastructure partagée avec d'autres organismes. **(15)**

B. Principe

Un VPN repose sur un protocole, appelé protocole de tunnelisation, c'est-à-dire un protocole permettant aux données passant d'une extrémité à l'autre du VPN d'être sécurisées par des algorithmes de cryptographie.

Lorsqu'un système extérieur à un réseau privé (client nomade, agence ou travailleur à domicile) souhaite se connecter au réseau de son entreprise :

- Les paquets (qui contiennent les données) sont chiffrés par le client VPN (selon l'algorithme décidé par les deux interlocuteurs lors de l'établissement du tunnel VPN) et éventuellement signés
- Ils sont transmis par le biais du réseau transporteur (internet en général)
- Ils sont reçus par le serveur VPN qui les déchiffre et les traite si les vérifications requises sont correctes

C. Utilisation dans le domaine mobile

Le VPN existe sur mobile, et s'appelle tout simplement VPN mobile **(16)**, et qui fonctionne sur Windows Mobile.
C'est un logiciel qui pratique la solution de VPN IPSec (IPSec est un protocole d'authentification et de chiffrement des données sur un canal sécurisé entre deux entités), et permet aux utilisateurs d'établir des connexions sécurisées avec le réseau de l'entreprise via internet. Il permet entre autre de pouvoir se connecter en Wifi, GSM, GPRS, EDGE, et est capable de d'utiliser des canaux sécurisés par cryptage DES, 3DES, AES.

D. Mise en œuvre

La mise en œuvre est possible sur mobile qui fonctionne avec Windows, via le logiciel décrit plus haut, et un logiciel tel OpenVPN qui permet de faire un serveur. Sous Androïd les connexions VPN sont possibles depuis la version 1.6. **(17)** L'iPhone permet aussi d'utiliser des réseaux VPN**. (18)**

XI. Comparaison fonctionnelle et expérimentale

	PKI	Kerberos	Carte mémoire	biométrie	mot de passe
Matériel requis pour le client	Un téléphone et une carte sim compatible wpki	Un téléphone	Un téléphone et une carte mémoire	Un téléphone avec lecteur biométrique	Un téléphone
Matériel requis pour le serveur					
Utilisation	Taper toujours le même mot de passe d'authentification	Taper toujours le même mot de passe d'authentification	L'insertion de la carte entraine l'authentification	Faire glisser son doigt sur le lecteur	Taper un mot de passe different a chaque utilisation
Adresse des codes à télécharger pour faire fonctionner la méthode côté serveur	http://www.openssl.org/source/	http://web.mit.edu/kerberos/dist/index.html#krb5-1.8	-	-	-
Disponible pour Windows Mobile ?	Oui	Oui depuis la version 5	Oui	Oui	Oui
Disponible pour Iphone ?	Oui	Oui via une application disponible non officiellement	Non, aucun port	Non	Oui
Coût (coté serveur, CA)	1 serveur capable de créer des certificats	2 serveurs (Le gestionnaire de ticket, et le serveur d'authentification	-	1 serveur avec 1 base de données	1 serveur de gestion de mot de passe

Figure 19 : Tableau comparatif des différentes méthodes d'authentification pour smartphone.

XII. Bibliographie

1. **Wikipedia.** *Certificat électronique.* Wikipedia. 2010. http://fr.wikipedia.org/wiki/Certificat_%C3%A9lectronique.

2. **Wikipedia** *. Infrastructure à clés publiques.* Wikipedia. 2010. http://fr.wikipedia.org/wiki/Infrastructure_%C3%A0_cl%C3%A9s_publiques.

3. **Benjada, Mustapha.** *PKI (Public Key Infrastructure).* SecuriteInfo.com. http://www.securiteinfo.com/cryptographie/pki.shtml.

4. **WPKI Non-Profit Association.** *WPKI Main Specification.* WPKI Main Specification. 2009.

5. **Hassinen, Marko, Hyppönen, Konstantin et Haataja, Keijo.** *An Open, PKI-Based Mobile Payment System.* Lecture notes in computer science. Freiburg : Germany, 2006. Vol. 3995, Page : 86 - 100.

6. **Moon, Jong Sik, Lee, Deok Gyu et Lee, Im-Yeong.** *Device Authentication/Authorization Protocol for Home Network in Next Generation Security.* Lecture Notes In Computer Science. 2009.Vol. 5576, Pages : 760 - 768.

7. **Bouillon, Emmanuel.** *Kerberos et la Sécurité*. Kerberos et la Sécurité. Bruyères-le-Chatel : France, 2008.

8. **Jay Freeman (saurik).** *iPhone AppTrackr.* Kerberos. 2008. http://iphoneapptrackr.com/app/krb5/.

9. **The MIT Kerberos Team.** *MIT Kerberos Distribution Page.* Kerberos V5 Release 1.8.1. http://web.mit.edu/kerberos/dist/index.html#krb5-1.8.

10. **Pirzada, Asad Amir et McDonald, Chris.** *Kerberos Assisted Authentication in Mobile Ad-hoc Networks.* Proceedings of the 27th Australasian conference on Computer science. Dunedin, New Zealand : s.n., 2004. Vol. 56, Pages: 41 - 46.

11. **Gaiti, M Loutrel - P. Urien - D.** *Authentification dans les réseaux radioélectriques : état de l'art et intégration avec la carte à puce.* Annals of Telecommunications. 2004.

12. **Alban.** *Les nouveaux brevets signés Apple.* iPhoneCoffee.com. 2009. http://www.iphonecoffee.com/les-nouveaux-brevets-signes-apple.html.

13. **unwiredview.com.** *Sagem to launch Android phones with fingerprint identity capabilities from UPEK.* Sagem to launch Android phones with fingerprint identity capabilities from UPEK. 2010. http://www.unwiredview.com/2010/02/05/sagem-to-launch-android-phones-with-fingerprint-identity-capabilities-from-upek/.

14. **Arnaud Jacques.** *Les mots de passe à usage unique : One Time Password.* SecuriteInfo.com. http://www.securiteinfo.com/cryptographie/otp.shtml.

15. **Wikipedia.** *Réseau privé virtuel.* Wikipedia. 2010. http://fr.wikipedia.org/wiki/R%C3%A9seau_priv%C3%A9_virtuel.

16. **TheGreenBow, Sistech SA.** *VPN Mobile.* TheGreenBow.com. 2010. http://www.thegreenbow.fr/mobile.html.

17. **Kallenborn, Gilbert.** *Android 1.6 supporte les VPN.* 01net.com. 2009. http://pro.01net.com/editorial/506255/android-1-6-supporte-les-vpn/.

18. **Apple.** *iPhone et iPod touch : configuration d'un VPN. C*onfiguration d'un VPN. http://support.apple.com/kb/HT1424?viewlocale=fr_FR&locale=fr_FR.

19. **Moon, Jong Sik, Lee, Deok Gyu et Lee, Im-Yeong.** *Device Authentication/Authorization Protocol for Home Network in Next Generation Security.* Lecture Notes In Computer Science. Vol. 5576, Pages : 760 - 768.