

Comparaison fonctionnelle et expérimentale d'une PKI sur mobile et de Kerberos sur mobile. Mise en oeuvre et comparaison rigoureuse des résultats expérimentaux. Automatisation du déploiement.

Jean-Philippe Blaise, Willian Jouot

Master SSIC, Metz University,
Ile du Saulcy, 57045 Metz, France
jeanphilippe.blaise@umail.univ-metz.fr
william.jouot@umail.univ-metz.fr

Résumé De nos jours, les téléphones mobiles sont partout, et la population de smartphone est en plein essor. Ces types d'appareils peuvent faire de plus en plus de choses, et ainsi égaler nos ordinateurs. Ainsi en leur fournissant une multitude de moyens de communication, nous devons nous poser la question de la sécurité des données, telle que nous la connaissons pour nos ordinateurs. Les smartphones, étant de plus en plus puissant, peuvent parfaitement gérer un ou plusieurs protocole d'authentification. De ce fait, nous allons développer une solution de PKI et une solution Kerberos pour smartphones utilisant le célèbre Operating System de Google, Android. Dans cet article, nous allons comparer quelques solutions déjà existantes, puis proposer notre méthode.

Mots-clés : PKI, Kerberos, Android, mobile, mise en oeuvre, déploiement automatique

1 Problématique

A l'heure actuelle, les téléphones ainsi que les smartphones se démocratisent de plus en plus, et il y a donc de plus en plus de données qui transitent via ces appareils, que cela soit via le wifi, bluetooth, ou directement le réseau téléphonique. On commence ainsi à faire des achats directement depuis son téléphone, où encore envoyer des informations personnels, comme des mots de passe, ou des documents que l'on veut garder secret. Malheureusement, toutes ces données transitent plus ou moins en clair dans l'air, à la portée de n'importe qui. Il faut donc sécuriser les données. Quelles solutions existent ? Des systèmes comme PKI ont déjà fait leurs preuves sur nos ordinateurs, mais existe-t-il des solutions concrètes pour nos mobiles ?

2 Travaux existants dans la littérature scientifique

Il existe de nombreux travaux dans le domaine, notamment pour la PKI. Le premier article étudié[1], est très intéressant. Datant de 2007, cet article se pose une excellente question. Comment sécuriser des données transitant d'un téléphone mobile à un site

marchant ? Ainsi on peut trouver une solution assez intéressante, la création des clés d'authentification utilisées se fait en local, c'est à dire que le téléphone est capable de générer ses propres clés. C'est un bon point. Les auteurs utilisent la Crypto librairie[2] pour la signature de données transmises. Cependant cette solution connaît quelques faiblesses, que nous détaillerons plus tard.

Le second article[3] nous propose un autre systèmes de paiement sécurisé pour mobile via une PKI. Pour leurs tests, le centre d'enregistrement finlandais s'est chargé de leur fournir la PKI.

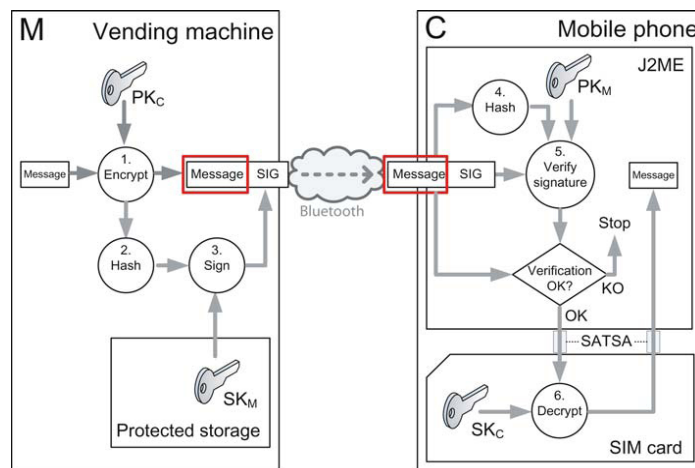


FIGURE 1. Exemple d'échange de messages sécurisés

Pour faire simple, les clés privées sont stockées dans la carte SIM. Etant infalsifiable, les clés privées ne peuvent pas être compromises. Chaque carte SIM se voit attribuer un unique certificat, délivré par le centre d'enregistrement finlandais. Cette carte SIM est capable de signer les données, mais le cryptage/décryptage se fait sur le téléphone. Un machine en ligne (banques, vente en ligne, etc.) crypte son message, et le signe. Le message est ensuite envoyé au téléphone mobile. Celui-ci vérifie la signature, dans le cas ou elle est correcte, le téléphone consulte sa clé privée, stockée dans la carte SIM, et décrypte le message.

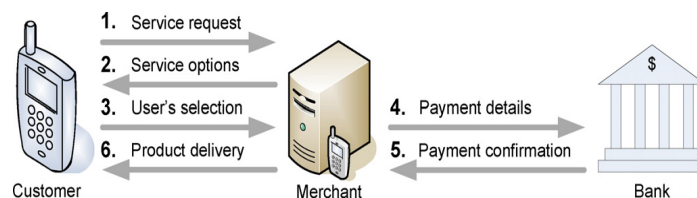


FIGURE 2. Modèle de paiement virtuel

Cette figure schématise le fonctionnement du paiement via téléphone mobile. 6 étapes sont nécessaires.

Le troisième article sur une PKI pour mobile [4]. Leur travail se reporte à d'anciens téléphones, avec très peu de mémoire vive et même un processeur très faible. Ainsi la génération de clés RSA leur est impossible. Ils décidèrent d'utiliser un autre algorithme de signature, plus adapté à leur type de téléphone, le ECDSA (Elliptic Curve Digital Signature Algorithm), avec des clés de 163 bits, équivalent à une clé RSA de 1024 bits, en terme de sécurité. De ce fait, les certificats ainsi générés sont eux aussi, plus petits.

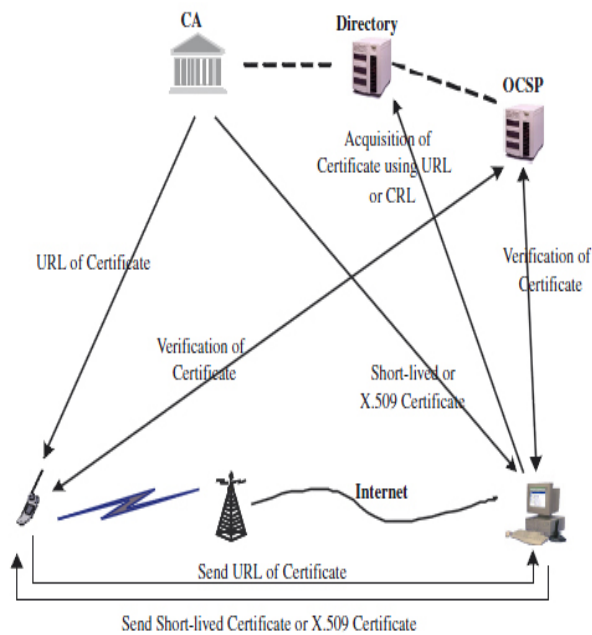


FIGURE 3. Schéma de leur système de PKI pour mobile

Pour le premier article, offrant une solution Kerberos [5], met en avant la non-répudiation, en utilisant une méthode de hachage fonctionnant plus rapidement que les algorithmes de signatures numériques. Leur procédé fonctionne exactement comme le protocole Kerberos que nous utilisons sur nos ordinateurs. Le téléphone mobile demande à s'authentifier auprès du centre d'authentification. Puis après quelques opérations, on fournit au téléphone un ticket, lui permettant d'accéder au service demandé au tout début. Cependant, il est possible de réutiliser un ticket pour accéder au même service, à plusieurs reprises. Au niveau de la sécurité, il n'est pas possible de créer un ticket, car la signature de l'autorité de certifications n'est pas falsifiable. Un attaquant ne peut pas utiliser ou modifier un ticket émis. Les clés symétriques, utilisées lors de l'authentification sont régénérées à chaque session.

Le second article offre lui une solution permettant à un téléphone ayant en sa possession un ticket d'itinérance, d'avoir accès aux services auxquels il veut avoir accès, sans communiquer avec le serveur d'authentification à chaque fois.

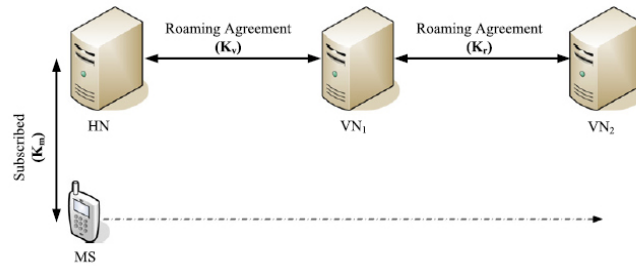


FIGURE 4. Représentation de l'itinérance

Pour ce faire, le téléphone s'authentifie auprès d'un réseau "visiteur", qui lui même authentifie le téléphone auprès de son home réseau.

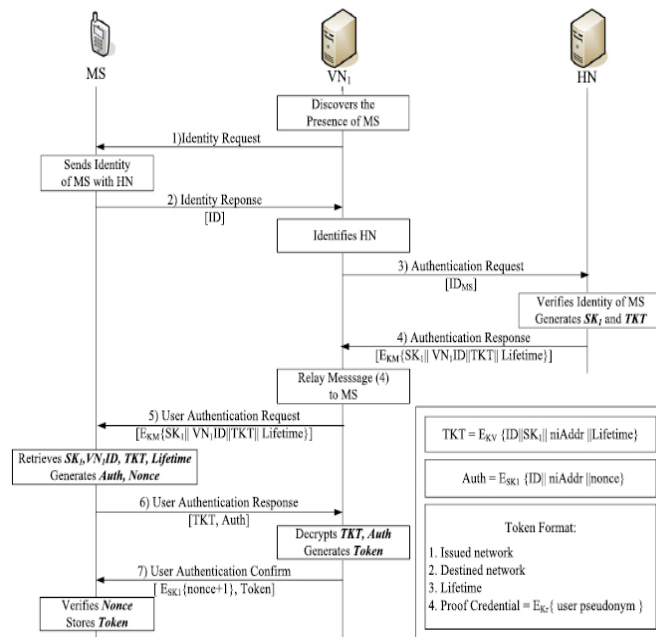


FIGURE 5. Authentification du téléphone auprès du réseau "visiteur"

3 Premières critiques des travaux existants

Premier constat, aucune solution de PKI ne supporte l'échange de données de téléphone à téléphone, seuls les échanges de données entre le téléphone et un serveur (banque, site de vente en ligne, etc.) sont gérés. D'un autre côté, les 3 solutions de PKI présentées, sont relativement complètes. Les systèmes de signatures sont réfléchis, les clés privées sont innaccessibles, même en cas de vol, puisque les clés sont stockées dans la carte SIM, qui elle même est protégée par un code PIN. De leur côté, les solutions Kerberos, présentées plus tôt ont eux aussi ce soucis de ne pas gérer les échanges entre deux téléphones.

Evidemment, chacune des techniques PKI ou Kerberos présentes des désavantages qui sont propres à leur fonctionnement. Par exemple, lors d'un système Kerberos, les mots de passe utilisateurs sont enregistrés sur le serveur de manière non hashé, car le serveur a besoin du mot de passe en clair pour crypter la réponse à envoyer au client. De plus, Kerberos, de part son fonctionnement un serveur, peut poser problème si pour une raison ou une autre le serveur d'authentification n'est pas accessible. Dans le cas par exemple où le serveur a planté.

4 Objectifs et perspectives du projet de synthèse

Notre objectif est d'implémenter le déploiement automatique d'un système de certification pour mobile. Pour cela, nous allons devoir implémenter une solution de PKI pour mobile, et une solution Kerberos pour mobile. Ainsi, nous pourrons comparer de manière fonctionnelle les deux systèmes et choisir le plus efficace. Dans le cas de Kerberos, le but est de créer un petit client, capable de se connecter à un centre d'authentification Kerberos pour ensuite avoir un ticket pour un service demandé.

5 Premiers essais

Nous avons commencé à implémenter une solution de PKI. Seules les méthodes de génération de clés, et de signatures sont pour le moment présentes.

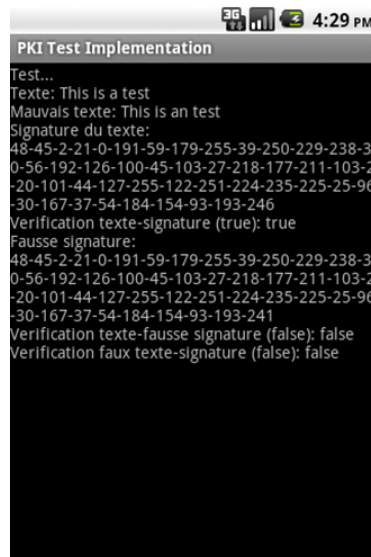


FIGURE 6. Début d'implémentation

Coté Kerberos, nous avons réussi à créer un serveur Kerberos, basé pour l'instant uniquement sur des utilisateurs créés manuellement, et à créer un client Java capable de se connecter sur ce serveur pour récupérer, après quelques échanges, un ticket de service. La prochaine étape est de, premièrement, convertir le projet pour qu'il fonctionne sur Android, et ensuite de créer un service, compatible Kerberos, comme par exemple une session SSH, pour que le téléphone puisse se connecter dessus.

Références

1. M. Assora, J. Kadirire, and A. Shirvani, "Using wpki for security of web transaction," *Lecture Notes in Computer Science*, 2007, vol. 4655, pp. 11–20, 2007.
2. *WMLScript Crypto API Library : WAP-161-WMLScriptCrypto-20010620*.
3. M. Hassinen, K. Hyppönen, and E. Trichina, "Utilizing national public-key infrastructure in mobile payment systems," *Electronic Commerce Research and Applications*, vol. 7, pp. 214–231, 2008.
4. Y. Lee, J. Lee, and J. Song, "Design and implementation of wireless pki technology suitable for mobile phone in mobile-commerce," *Computer Communications*, vol. 30, pp. 893–903, 2006.
5. Y. Lei, A. Quintero, and S. Pierre, "Mobile services access and payment through reusable tickets," *Computer Communications*, vol. 32, pp. 602–610, 2009.