Towards a Secure Identity Management in Smartphone Environments

Maryline Laurent
CNRS Samovar Lab
Institut Mines-Télécom, Télécom SudParis
Evry, France
Maryline.Laurent@telecom-sudparis.eu

Samia Bouzefrane
Cedric Lab
Conservatoire National des Arts et Métiers
Paris, France
samia.bouzefrane@cnam.fr

Christophe Kiennert
LIP6 Lab
Université Pierre et Marie-Curie
Paris, France
christophe.kiennert@lip6.fr

***Abstract*— IDentity Management (IDM) is a hot topic today for mobile network operators and service providers, especially when the terminal is a smartphone. This paper addresses the encountered security issues of smartphones to support identity management. Then it proposes the original idea of an IDM applet remotely controlled by a trusted entity into the smartphone and performing secure identification and authentication of users to their service providers.**

Keywords- identity management; authentication; privacy; smartphone

I. INTRODUCTION

Mobile network operators are providing identification and authentication means to their subscribers through SIM-cards. However, the European regulation limits usage of this identity to the network provider perimeter, that is, to support mobile terminal localization, authentication and mobility management. As such, other digital identities are used for getting access to services offered by service providers, including mostly the login and password scheme. Hence, mobile terminals are hosting a number of digital identities for accessing Facebook / Google account, vendors web site, online games, etc. However, managing identities into a mobile terminal within the applications themselves are risky as terminals are very much vulnerable to passwords and ID thefts.

This paper is organized as follows. Section 2 presents the mobile terminal environment, and inherent vulnerabilities. Section 3 gives the reasons for defining a mobile identity management. Section 4 proposes a new IDentity Management (IDM) applet for users to use their smartphone as an Identity Management wallet to access to their online services. Section 5 concludes with some perspectives.

II. MOBILE TERMINAL ENVIRONMENT AND VULNERABILITIES

Mobile terminals host several distinct identities for users, included as configuration parameters of applications. Note that some great Internet actors like Facebook / Google offer their identity management service to Internet individuals and impose themselves as identity management systems for Internet individuals, but at the risk that users become too much dependent to these actors (which are known for not being respectful of privacy).

Mobile terminals like smartphones are made vulnerable due to several factors like: multiple connectivity interfaces (NFC, Wi-Fi, 3G), large choice of uncertified downloadable applications by users, OS configuration by users. As such, the terminals can be infected [3] by malicious applications or OS that can collect private data stored on the smartphones (preconfigured login/password, as well as agenda, directory, etc.). Some open connectivity interfaces to the smartphones can also cause leakage of private data information to malicious users. Data collections serve usually for later masquerading. So payments on Web sites are abusively charged to the legitimate user. As a consequence, it is not recommended to manage digital identities in the freely accessible user space in smartphones.

III. NEED FOR MOBILE IDENTITY MANAGEMENT

As explained in section 2, mobile terminals are improper to manage identity management functions as a user space application. However, the mobile terminal is very well introduced into the technology market due to its “always on” connectivity, but it is also considered now as a “personal data manager” by users making their agenda, their directory being automatically synchronized with their corporate or private data on their computer.

As such, there is a strong need and a huge market for mobile Identity management.

The regulation, especially in Europe, is currently revisiting several of its directives [1, 2] to build a more trustful electronic society where certified digital identities enable authentic services with data privacy preservation. The objective is to enforce secure enrollment of individuals into the IDM, so that next several qualified services can be built like digital signature service [4], electronic seal service, time-stamping service, etc. These services are considered as “qualified” as they can serve as valuable proofs to a court. In this context, investigating secure IDM into mobile environment is of high interest.

IV. PROPOSED MOBILE IDM APPLICATION

The idea is defining an IDM application in a Trusted zone of the mobile terminal as a Trusted Execution Environment (TEE). This IDM application is managing the digital identities and credential of the user. Identities and credentials can take the form of the binding login/password, or the login/private key/electronic certificate or a URI/WebID private key [7]. This application can be securely remotely managed by a Trusted Service Management (TSM) entity through the OTA (Over-The-Air) interface as illustrated in Figure 1. Referring to the classical identity management entities, the IDM application can play the role of the IDP (identity Provider).

This TSM entity can be ensured by network operators, banks or other financial institutions, or e-government services. Moreover, since the IDM application acts on behalf of the TSM, such architecture requires a trust relationship between the TSM and the IDM application. This trust relationship can be embodied, for instance, as a shared secret K.

There are several ways to design an embedded IDM application in order to address the security issues presented in the previous sections. For instance, [5] designed the IDM application as a local OpenID provider allowing the user to authenticate locally to this provider in order to access any website accepting OpenID authentication. The main advantage of this solution is to implement a very secure authentication since the credentials are not sent through the network. However, contrary to most identity federation standards, the OpenID protocol is not based on the circle of trust principle. Hence, service providers tend to be reluctant to rely on OpenID since the available OpenID IDPs are not always trustworthy. Moreover, it adds several constraints to solution deployment, since it only targets service providers proposing OpenID authentication, and since there has to be a permanent synchronization between an online OpenID proxy and the embedded OpenID provider.

The approach proposed in this paper mainly considers IDM functionality and does not aim to fit in identity federation standards. The principal idea is to let the user own a secure IDM wallet which he can access whenever authentication to a service provider is required. This application is installed in the TEE (Trusted Execution Environment) of the terminal, or in the SE (Secure Element) which is typically a secure micro component such as a smart card.

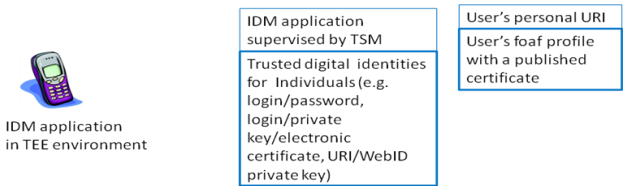

Figure 1. Entities for supporting the mobile IDM application.

Our solution is focused on two independent functionalities: IDM and user authentication. Figure 3 sums up the different interactions between all the entities of the solution. The blue arrows are related to IDM, and the green arrows are, in an entirely independent way, related to user authentication.

A. *Identity Management*

The user is able to perform the usual operations related to IDM (identity creation, modification, deletion) through the TSM which he can access on the network through a secure connection. This allows the user to access his personal folder containing his current identities. He can add any kind of identity as stated above, or he can modify the password associated to a login. In the case he stores a WebID along with a private key, the user's personal URI must contain the associated public key stored in a FOAF file. Whatever operation is performed by the user, the TSM shall update the user application through OTA with a HMAC taking the shared secret K as a parameter. By doing so, the identities stored in the Trusted zone of the user's terminal are all trusted, since the TSM is the sole entity able to modify the user's identities. The IDM applet stores all the identities in the non volatile memory according to the format represented in Figure 2, where the ID Type is a number identifying if the ID is a login/password, a URI/WebID private key, and so on. It also stores the number of currently stored identities as well as the relative address of the first byte of each identity, making the reply to a "Read all identities" command easy to compute.

ID Type	**Login Length L1**	**Secret Length L2**	**Login**	**Secret**
1 byte	2 bytes	2 bytes	L1 bytes	L2 bytes

Figure 2. Identity format as stored in the IDM application.

B. *User Authentication*

The identities and associated credentials stored in the application can be accessed by the user in a read-only mode through a local application running on the mobile terminal which interacts with the IDM applet via ISO 7816 commands (APDUs), and displays the available identities. The mobile application is only allowed access to the smart card applet upon entering a correct PIN code. It loads a user interface displaying all the logins of the identities stored in the smart card. The user does not need to enter any login or password, and only needs to select the identity he wishes to use. Then, he must select a pre-registered service provider URI or enter this URI himself. The credentials of the selected identity are then transmitted to the URI of the remote server where user authentication is performed.

Since the credentials associated to each identity are stored in a trusted environment, this application mitigates risks of identity theft in a very simple way. The main concern addressed by this application is personal or secret data leakage due to the traditional storage of such data in environments devoid of any physical and logical security countermeasures. With such an application, the whole IDM environment is entirely safe. However, the credentials are still sent over the network during the authentication step, and

the security issues regarding data eavesdropping, interception, or man-in-the-middle attacks are not addressed by this application. This is not necessarily problematic since this application is entirely flexible, and can be easily extended with several security features. These features could consist, for instance, in performing local authentication, as proposed in [5], or in exclusively managing X.509 certificates for mutual TLS authentication based on embedded TLS, as proposed in [6]. But such extensions have the notable inconvenient of considerably narrowing the deployment possibilities of the solution.

Although enforcing confidentiality during authentication cannot be part of the security claims of the solution proposed in this paper, it remains possible to enhance security by taking advantage of options commonly supported by service providers such as the HTTPS protocol, ensuring that a one-way TLS server authentication performed before the password is sent over an encrypted channel.

V. CONCLUSION

This paper presents the need for a trusted IDM solution for mobile network environment. It proposes a secure IDM approach for managing digital identities as a mobile application embedded in a secure component. This application manages to significantly improve the IDM security on mobile terminals without any hindrance regarding its deployment and scalability. This work shall be pursued with a full implementation of the solution and further thought about possible optimizations.

REFERENCES

[1] Proposition de règlement du Parlement Européen et du Conseil relatif à la protection des personnes physiques à l'égard du traitement des données personnel et à la libre circulation de ces données (règlement général sur la protection des données), COM(2012) 11, Bruxelles, 2012.

[2] Proposition de règlement du Parlement Européen et du Conseil sur l'identification électronique et les services de confiance pour les transactions électroniques au sein du marché intérieur, COM(2012) 238, 2012.

[3] A. Efrati, S. Thurm, and D. Searcey, Mobile-app makers face u.s. privacy investigation, 2011, Wall Street Journal.

[4] http://www.gsma.com/mobileidentity/wp-content/uploads/2013/03/Mobile-Identity-A-Regulatory-Overview-FINAL-Feb2013.pdf

[5] A. Leicher, A. U. Schmidt, Y. Shah, Smart OpenID: A Smart Card Based OpenID Protocol, IFIP Advances in Information and Communication Technology Volume 376, 2012, pp 75-86, 2012.

[6] P. Urien, C. Kiennert, E. Marie, A New Convergent Identity System Based on EAP-TLS Smart Cards, Conference on Network and Information Systems Security (SAR-SSI), 2011, pp. 1 - 6.

[7] WebID: http://www.w3.org/community/webid/participants

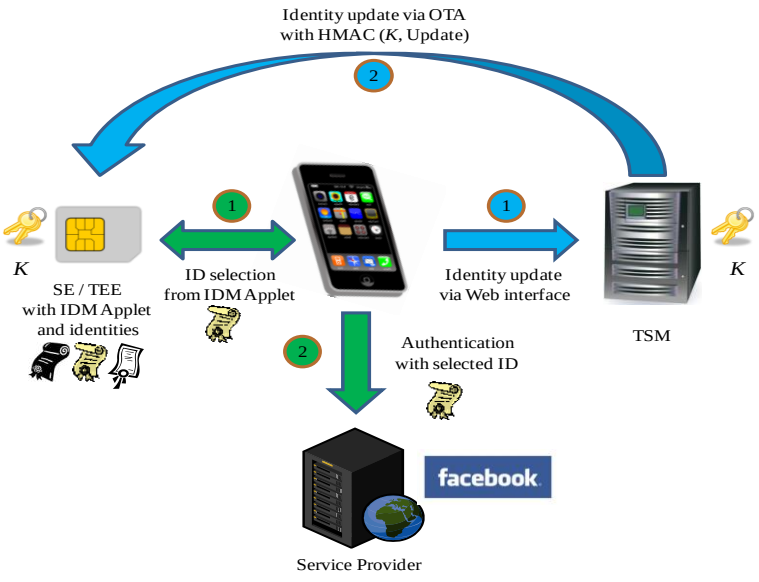

Figure 3. Interaction between different entities of the architecture.