SIM Card based Security and Trust Management

Dinesh Kumar[1], Ghankuntla Rana[2], Sevati Patel[3], Vijay Kumar Dewangan[4]

[1, 2, 3, 4]*(Department of Electronics and Telecommunication, kirodimal Institute of Technology, India)*

Abstract

This paper presents a solution how the position of a mobile device can be determined using the SIM card. These solutions require changes in the existing infrastructure of the GSM system in one way or another, and are based on information residing in the network. Sim card is integrated for providing basic services related to security, privacy, and trust. As the market for cellular telephones, and other mobile devices, keeps growing, the demand for new services arises to attract the end users. One topic that is being discussed throughout the world today is location-based services. How can a mobile device be located and in which way can a service be constructed to utilize this information.

Keywords- Mobile services, SIM card, Trust management, smart card

I. INTRODUCTION

In order to repeat the success of the WEB, mobile services of the future have to be simple to find, simple to use, simple to trust, and simple to set-up. In this paper, we mainly address the specification and implementation of mobile services that are “simple to trust”. Typical use cases for mobile services are travel scenarios. Security issues are important from both the end-user as well as from the service provider perspective. One goal for SMS is to enable individuals and small companies to become service providers (“simple to set-up”). Especially this clientele would benefit from easy-to-use and easy-to-build-in mechanisms helping them to provide secure services. Nowadays, the SIM establishes the security of mobile networks by authenticating Subscribers. Thereby, it provides an identity which is also used for further purposes as for Instance micro-payment which is carried out through the mobile network operator. As a security device for mobile networks, the SIM is also technologically capable of providing security, privacy, and trust functionality for mobile services.

II. WHAT IS A SIM CARD

A SIM card, also known as a subscriber identity module, is a subscriber identity module application on a smartcard that stores data for GSM/CDMA Cellular telephone subscribers. Such data includes user identity, network authorization data, personal security keys, contact lists and stored text messages.

III. WORKING OF SIM CARD

As described above the MS consists of two entities .The ME and the SIM card. Whereas the ME handles the radio communication, it’s the SIM card that provides all user subscription information and personalization. Without the SIM card the ME can’t log onto the system, and simply put the ME is just a nonoperational mechanical device.4 Since the SIM card holds all user information, it’s not tied to a specific ME but can be used in any ME and the owner of the SIM will be charged for the calls, not the owner of the ME. The SIM cards contain three different types of information that’s related to the user. The first type is information that is stored by the operator and can’t be changed, such as the International Mobile Subscriber Identity (IMSI) and the authentication key *Ki*. The IMSI identifies the subscriber within the GSM network, and the *Ki* is used for security purposes.The second type of information is temporary stored information, such as network information that changes over time. Examples of this are the Temporary Mobile Subscriber Identity (TMSI) or Location Area Identity (LAI). The TMSI is sometimes used instead of the IMSI to identify the user in the network, to increase security against actions such as monitoring of certain IMSI. The LAI identifies which LA the subscriber currently is registered in. The last type of information is service-related and can be language preferences, phonebook, short messages, call log and so on.To enhance the functionality of the SIM card it can be programmed with SIM Application Toolkit commands, which enables the card to interact with the ME [1].

IV. SIM CARD SECURITY SYSTEM

By combining stored evidence of identity (such as a key) with personal information only the user will know (a password, for example), it offers the same two-tier authorization provided by smartcards. It is becoming clear that the SIM --- a feature unique to the mobile world --- has applications far beyond those for which it was originally designed. The clue is in the name --- Subscriber Identity Module. It was created to remotely authenticate users to the network and to the billing systems that allow operators to generate revenues from voice traffic[3].The GSM standards as specified by ETSI requires authentication of a mobile subscriber through a secure device (the SIM card) Hierarchical PKIs as well as Web-Of-Trust Infrastructures can become very complex. The suggested solution is to use a Web-Of-Trust, but with a limited signature chain. If we only attend direct signatures, instead of three levels like in Open PGP [4], we are able to simplify the problem. Inspired by [5] we introduce a trust scoring calculation based on probabilistic argumentation for mobile service authentication where users are able to gradually rate the services. Trust values of signing entities together with the trust value of the entity itself can define an average service trust, based on a simple calculation algorithm: It must be further evaluated, if e.g. neutral trusted signatures are taken into consideration.

V. SIM BASED SERVICE TRUST MANAGEMENT

A couple of basic security services can be provided by the SIM. This includes management of sensitive user data, basic identity management, multi-id and multi-subscriber Management, basic cryptographic services like signing data and verification of signatures, And many others. Based on the architecture described in the previous sections, these Services can smoothly be integrated into composite services. The management of sensitive user data for instance should be only one component of the profile data management which also includes components for handling large non-sensitive data [2]. In the following, we present our proposal for on-card trust management in heterogeneous service infrastructures as an example for provisioning security, privacy, and trust services on the SIM.

A. On-Card Key Management

One of the basic concepts of our service trust management approach is that the attributes of

Services (including ratings resulting from previous service utilizations) are stored Individually for each user. Furthermore, we propose to securely store the data on the SIM Preventing.

B. Individual Trust Level Ranking

Every key in the key-ring application can be assigned with a discrete trust value to rank the individual service trust for the user of the service, e.g. a value between 0 and 1 as outlined in the table in Figure 5. We assume that this value will be adjusted automatically by dedicated system components that observe each usage of a service, or based on recommendations from friends or neutral organizations. Moreover, it is conceivable that Ranked public keys with trust values can be imported e.g. from an operator's database over

the air or from local kiosk terminals manipulation of service attributes by malicious software on the mobile phone.

C. Using Digital Signatures

Above we described the use of digital signatures and the management of a key-ring application on a SIM to proof the identity of a service. This is important e.g. during service discovery to determine the individual trustworthiness of services. In addition to this, we can find more aspects were digital signatures can be used a lot of mobile services are commercial oriented and the user might want to conclude some kind of commercial contract. To secure the process, the use of digital signatures could be helpful in order to make contracts accountable. This implies an even higher level of security than the usage of secure connections which is common in B2C internet shops, as the signature outlasts the conclusion of the contract. It is important that this signature is a digital signature method that takes place on the presentation layer of the OSI model. The user must be able to see what he signs and the signature must not be lost in any transport layer or omitted in later storage. A further use case is related to authorization. In general, authorization is determined within an application once the identity of the other party is confirmed by authentication and the access privileges are assigned. However, the SMS concept should include another way of authorization, allowing the user to perform certain actions or granting her certain rights that otherwise she would not have received, providing her with one-time (i.e. use only once, or time/event constrained) tokens. Several applications are possible. The user may for instance receive a time-constrained token during check-in at the airport, allowing him to buy in tax free shops**.**

VI. SIM INTEGRATION

Today, access to the SIM is rigidly regulated according to specifications of large international standardization bodies. For the future however, it can be expected that mobile systems will require fast and flexible deployment for all components, as these systems will evolve and expand steadily, even after first rollout. To accommodate this requirement for the SIM, we choose the new upcoming standards for smart card implemented web services[6], in order to enable an open architecture and to exploit the common HTTP communication as a basis for integration into the MOVE client described above.

VII. SMART CARD WEB SERVER

A Smart Card Web Server (SCWS) is a HTTP server that is implemented in a smart card that means in the mobile context in a SIM card. The SCWS can provide static content like HTML pages or media files that hence can easily be accessed, for instance from mobile phone, Internet browsers until departure. Another example is a one-time token for entering the gate shows in a “fig.”

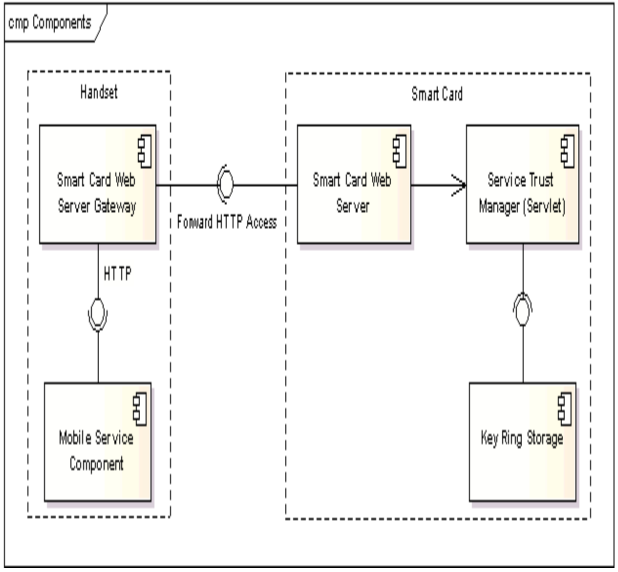

Figure.1 Smart Card Web Server Architecture

VIII. CONCLUSION

Users of future mobile services need assistance to deal with the manifold service offers and options without drawbacks for security, privacy, and trust. In order to cope with this requirement, the open architecture proposed by the ‘SMS project integrates the SIM as an enabler for security related services. During the remaining time of the project, this approach will be evaluated in demonstrators, user studies, and live trials with students at the University of Rome Tor Vergata . This evaluation will give indication to SIM manufacturers and mobile operators about the potential role of the SIM in future mobile services, in particular of user acceptance and business cases. The objective for this thesis had two parts. The first was to investigate how location-based services can be done; using information available in the cellular telephone. The second part was to implement a demonstration. . To retain these qualities it’s likely that the future solutions will consist of a mixture of network and handset based method.

REFERENCES

[1] Carsten Rust, Stefano SALSANO2, Lars SCHNAKE1Sagem Orga, Heinz-Nixdorf-Ring 1, Paderborn, 33106, Germany The SIM card as an Enabler for Security, Privacy, and Trust in Mobile Services Tel: +49 5251 8891519, Fax: +49 5251 8892951,

[2] University' di Roma "Tor Vergata", Via del Politecnico 1, Roma, 00133, Italy Tel: +39 320 4307310, Fax: +39 06 72597435,

[3] Stockholm , Oskar Mattsson Positioning of a cellular phone using the SIM , 2001

[4] SIMCLO]SIMcloning, http://en.wikipedia.org/wiki/SIM_cloning

[5] [GGSFMC] J. Eberspaecher / H.-J.Vorgel / C.Bettstetter, GSM Global System for Mobile Communication, 3. Edition, page 369

[6] [FGM03] Willassen, S., 2003, Forensics and the GSM Mobile Telephone System, International Journal of Digital Evidence, Volume 2, Issue 1.