SIM as a key of user identification: enabling seamless user identity management in communication networks

György Kálmán[1], Josef Noll[1,2]
[1]*UniK, N-2027 Kjeller, Norway,* [2]*Telenor R&D, N-1331 Fornebu, Norway*
gyorgy@unik.no,josef@unik.no

Abstract— **Easy and secure access is of key importance in acceptance of new mobile services. This paper extends the possible use of the SIM as authenticator in the online world. The paper proposes Near Field Communication (NFC) technology as a transfer technology between the mobile handset and other devices. A possible architecture is shown, future SIM requirements and secure key transfer are addressed. Final focus is on handset-internal communication, with emphasis on requirements and constraints raised towards the internal architecture.**

***Index Terms*—identity, seamless, authentication, NFC**

I. Introduction

Easy and secure user authentication is the key to introduce value-added services. Today's methods are usually providing either security or easiness. In the traditional username and password pairs, the users tend to use weak passwords, while if the system has a strong password policy, the passwords will be written down, and so can be easily compromised.

Telecom customers are used to services, where they are seamlessly authenticated by the network. These customers represent a significant group (in some European countries, the mobile penetration is near or over 100%) of the online services market, who are used to this kind of authentication.

The existing infrastructure in the GSM/UMTS network's SIM cards provide a possibility to extend the GSM-like seamless authentication to enable access of wireless networks, online services etc.

Recent surveys reveal, that the home high-speed internet connection penetration is reaching 60%. With extending the authentication capabilites, the SIM can be a future identity provider also for the home terminals.

This paper will first show, why the mobile phone has the potential to serve as an identity provider in the digital world. Then it will evaluate the current security infrastructure. It will justify the possible use of the SIM card, and propose a secure interface between the SIM card and the NFC reader of the mobile handset. An example NFC based phone admittance service will be presented.

II. State of the Art

Current research in trusted mobile platforms mainly focus on extending the mobile phone with an additional hardware to provide encryption services.

In the Trusted Computing Group (TCG)[1], a complete set of security features are under development. The planned architecture now covers also the mobile devices. The proposal is provider centric and needs special hardware to implement a secure platfrom.

The implementation of an extendable root trust structure is optional, potentially, the platform on the phone will be locked to content providers based on the network operator's preference. Also, based on the specification, altough it covers PC's and other computing devices, defines no interaction between these. So, no key transfer or authentication is possible through a relay device.

Altough, this solution enables defines a more extensive platform, which also covers other devices, it needs considerable investment and hardware changes in the whole mobile system, including handsets. Currently, no cost estimation exists for implementing such a system.

An open DRM architecture is defined in the Open Mobile Alliance (OMA)[2], which supports a function called *super-distribution* which enables users to share content with others, but mainly focuses on industrial content management. Providing personal management of own conent is not addressed. Transfer of access keys in case of super-distribution is done by the mobile network, generating potential expense on the subscriber side.

III. Personalisation and Security

Personalisation is the key for enabling feature rich services and preserving the ease of use. With personalisation services, the subscribers will be able to adjust the complexity of the features to their needs.

To identify the subscriber, the system needs a secure and unique ID. The use of mobile phone as an authenticator is natural choice, since the SIM card provides a trusted and secure platform for transmission and storage of IDs.

Current SIM cards used in GSM/UMTS networks are smartcards, which can provide secure key storage with strong encryption support, like PKI.

Our proposal differs from TCG's one mainly in the role of the end user. TCG focuses on the enterprise and a trusted hardware platform, which was first announced for PC's and then extended to other mobile devices. This solution disables modifications in the mobile phone's software and also can filter the downloadable software based on TCG's or the network provider's preferences.

Also, prime assumptions differ, since TCG defines a trusted hardware platform, but our proposal operates only with PKI, storage and ecryption capabilities of the SIM.

A. *Security Infrastructure*

The SIM card, as the base of this papers proposal, provides wide encryption capabilites: PKI, OTP and the normal SIM authentication. These methods are also recommended by the Open AuTHentication initiative (OATH)[9], and accepted by most European governments as required technologies for digital signatures.

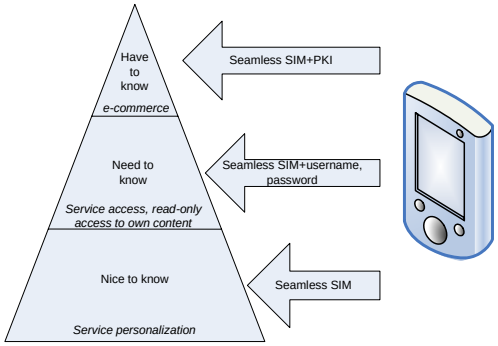

Figure 1 The trust pyramid

In the service realm, different authentication levels are required in order to provide service levels, enable features.

Our proposal divides these requirements into three levels.

The basic level, what we call *Nice to know* is designed to provide enough information for personalisation services, and with the help of the SIM card, the user can choose seamless authentication.

The middle level, *Need to know* provides a higher level of knowledge about the users identity thus enabling access to extra features, read-only access to personal content. To ensure security, SIM authentication and an additional username, password pair is needed.

The third, *Have to know* level the current One Time Password (OTP) systems can be integrated, but the use of PKI in addition to the seamless SIM authentication and provides better security, what e. g. banks require.

SIM authentication is used for GSM/UMTS network access and in some specific segments for personalisation of services [6]. In wireless networks EAP/SIM is an example of authentication using the SIM credentials for getting access. We suggest introducing application specific access, by implementing a set of access keys on the SIM card.

This will allow e.g. an "anonymous" purchase of a coffee, and a fully verified purchase of expensive goods through the mobile phone.

Admittance and payment services are enabled through introducing Near Field Communications (NFC) into the phone.

B. *Personalisation*

Seamless authentication through the SIM card enables transparent service personalisation. For the *Nice to know* security level, no user input is needed exept of that the mobile handset needs to be put close to the terminal.

This ensures, that the user is authenticated only, when he willingly wants to be.

To protect privacy, only the minimal amount of data has to be transmitted, e.g. there is no need for transmitting the user's name, if the parameter decides only about, that the webpage will show advertisements for ladies or gentleman.

IV. Architecture

With the SIM card, the system has an authenticator device, but the key needs to be transmitted from the mobile phone. The use of NFC as a primary transfer method of encryption keys is promising.

The sort range of NFC ensures secure key transfer. Also, the user's interaction is needed even for seamless key download, since the handset must be very close to the terminal.

The key actor in the system is the ID provider. This entity has to keep trusted relationships with all service providers (or the possibility to build trusted relationship through relaying identiy providers).

The suggested architecture is based on the following assumptions:

- there is trust between the service providers and the ID provider
- The ID provider has stored a secret key on the SIM
- The encryption keys are stored in the SIM's secure storage

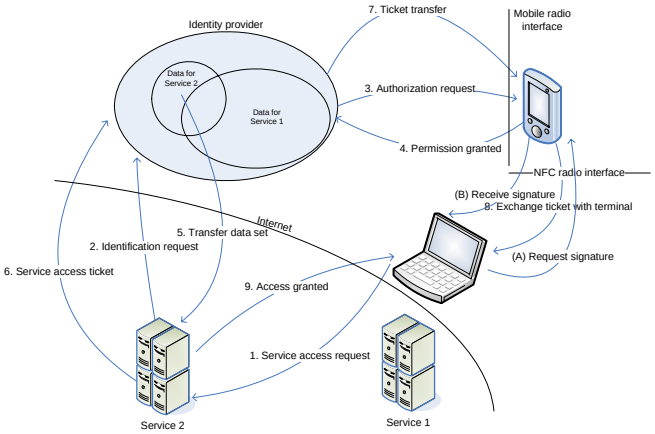

Figure 2 Identification and key exchange

The following authentication scenario shows a possible exchange of a session key. If the service allows it, with the same mechanism, it is possible to store a permanent key in the SIM and thus, skip requests towards the identity provider.

In the initial phase, the user's mobile terminal asks for a sign key from the handset (A). This key is transferred through the NFC interface and used as a terminal authentication (B).

Then the identification is done as follows:

1. The user's mobile terminal sends out a service

request signed with the terminal authenticator key
2. The service provider of Service 1 requests identification from the ID provider, the provider checks the authenticity of the request
3. The ID provider asks for authorization from the user through the mobile handset telling the name of the service and the requested data set
4. The user grants permission to authenticate towards Service 1
5. The ID provider transfers the required data set to Service 1 and an encryption key generated from the handsets secret key and the service's public key
6. Service 1 grants an access ticket encrypted with the generated combined key and signs with the Service 1 public key
7. The ID provider checks the signature and sends the ticket to the handset. The handset passes the key to the SIM and it decodes the data internally
8. Through NFC, the key is downloaded to the mobile terminal
9. Access granted

A. *NFC and the mobile phone*

NFC adds intelligence and networking capabilities to the phone and creates many new opportunities to add product and service capabilities to the handset like digital transactions and sharing in very close proximities.

Through the mobile phone, the user has full control over the identification process either based on the location e.g putting the phone close to the reader or on knowledge e.g typing in a PIN when requested by the remote service.

A key problem is the correct selection of the identifier shall be used in a transaction. This can be done either by profiles or by asking the user to allow acces to the data, requested by the service.

If it gets compromised, the identifier can be revoked by the operator and the user can get a new key without losing access to the services.

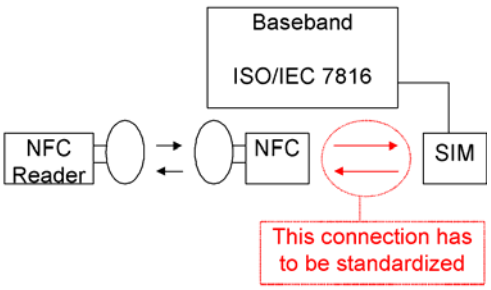

Figure 3 Internal structure

The remote revocation and user control makes the SIM an ideal device for making payments and gaining access to services.

When acting as a reader, an NFC mobile phone has the possibility to exchange data with other NFC devices, but most importantly it can trigger the download of content related to a specific object like a movie poster. For example: if a user walks by a movie poster, by just touching the poster it will trigger the browser, then the phone will automatically download information related to that movie, in what theatres is being played and it will give the user the possibility to purchase tickets if desired.

The possibility of remote application download through the provider network keeps the system open for new services. With a standard message format, any kind of application, which may use NFC can be deployed remotely.

B. *SIM as and identity provider*

Moving the ID handling into the SIM card provides various advantages for authetication. Collection of security items (keys, admittance, identity) in one place makes the solution convenient for the user

- Replacement of the user devices without losing credentials
- Device independent DRM management
- Advanced protection for misuse, as the SIM can be disabled remotely
- Potential for backup/restore functionality

C. *SIM as secure key storage*

According to ETSI standards [5], the SIM card provides a possibility of storing files.

The capacity of the module makes possible to store a considerable amount of keys, which are usually less than 1 Kb in size.

Conditional file access features provide the possiblity to store files, which can be accessed only by designated applications.

The provider is able to store a master encryption key on the SIM card and limit access to keys to SIM internal routines, protecting sensitive data against trojans or man-in-the-middle attacks coming from the user space of the mobile's operating system.

internal routines can provide data for example to challenge-response authentication either with the original GSM A8 or other external algorithms.

The internal communication between the NFC reader and the SIM needs to be standardized in order to ensure usability in handsets made by various handset manufacturers.

D. *NFC reader*

As an I/O device, the reader can be connected to the handsets internal bus and acts as a receiver/transmitter, there aren't specific security requirements.

With the SIM internal processing, the NFC reader just sends the encrypted package received, and is just in charge for transmitting the whole data sent to the unit. Atomic writes are ensured by the NFC standard itself, so the internal routines can focus on encryption functions, since the transport of data can be an internal task of the NFC part.

E. *Key management*

The SIM has an integrated secure storage. In this area, it is possible to store keys, which aren't accessible from outside.

To ensure secure transfer of new service keys, the provider may install a secret master key to the module at it's activation.

The new keys can be encoded with this master key inside the operator's network and then transferred to the unit. The data will be protected against eavesdropping and man-in-

the-middle attacks, since only the receiving SIM card will be able to decrypt it.

Decryption can be done by SIM internal routines, which can access the master key and store the new service key into the protected storage.

As such, the key is encrypted until it reaches the secure storage.

For service access, the system can use a challege-response authentication, so the key won't be transmitted or even read out from the card.

F. NFC2SIM interface

The communication between the SIM and NFC readere must follow the GSM standard to ensure easy and transparent deployment in the existing networks.

Security problems doesn't raise on this interface, since the data transmitted is already encoded in the SIM, so the secrecy of the key only depends on the strength of the algorithm used in the module.

V. EXAMPLE SERVICE UTILIZING NFC

Prototypes and demonstrations of the capabilities for SIM authentication are well under way. This chapter will provide an example admittance service based on an NFC enabled handset.

A. Prototype and early demonstrations

Current developments are focusing on mobile ticketing, like the mobile ticketing pilot at RMV in Hanau[10], Germay and the recently announce service or the Deutsche Bahn, HandyTicket [11].

The prototype developed at UniK uses the first version of the NFC Nokia phones, which aren't able to store the electronic ticketing information on the SIM card, but instead on an integrated smart card controller in the phone.

B. Admittance services

While NFC services are demonstrated world-wide, e.g. at the 3GSM World Congress 2006 [8], research focuses on two areas: Interworking with other wireless technologies and security issues. Goal of the interworking is to initiate and enable communications in Bluetooth, WLAN, or mobile (GSM/UMTS) networks. The security area addresses potential threats, identity, privacy and simplicity.

In this section we show a potential service based on the NFC integraton, SMS initiated admittance. The user can give a key to NFC enabled locks, by sendint an SMS message from a registered handset or using the web interface of the service. On the web, he has to fill out a form with the data needed, via SMS, a certain format has to be used:

rfid (number) (lock) (start date) (start time) (end date) (end time)

The admittance control is as follows:

1) *John* sends SMS to service number to allow *Mary* accessing his flat, through the door locked by lock 9. Example: SMS to 2034 "rfid 90025643 L9 290506 1110 290506 1115"
2) The service center sends a message to Mary, that she will get a key in the next SMS, and she should accept it in order to be able to use it.
3) The service center is sending down the application which is holding the key to open L9. Mary accepts the application, which saves the key on the phone.
4) *Mary* enters the flat with help of NFC phone. *John* might receive an acknowledge message when *Mary* enters the flat.

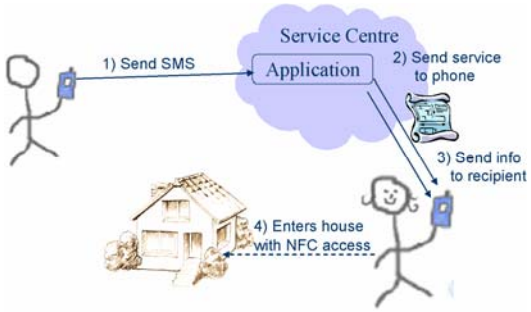

Figure 4 Admittance through SMS

An admittance control system is prototyped using the functionality of Telenor's PATS Innovation lab, Nokia's 3320 phones with NFC shells and a simulated lock system.

It comprises elements of seamless authentication, interworking between mobile and near-field communication and provides new and advanced services to the end user. *John* is authenticated in a seamless matter when sending the SMS, interworking is provided through PATS' lab based install messages. The users, *Mary* and *John*, experience admittance based on SMS exchange as an advanced new service.

VI. REQUIREMENTS

The proposed architecture has no special requirements towards the operator's network, beside the initial master key upload at activation of the card and the possible extension of the user register with the master SIM key. It is also possible to use the original user identification key, which is used by the network itself.

Current SIMs provide adequate storage for limited set of services, but the upcoming high capacity modules will solve this limitation. The cards already have the A8 encryption algorythm integrated, and it is also possible to install new ones, for example an implementation of Diffie-Hellmann key exchange protocol or Advanced Encryption Standard (AES).

The mobile handsets need to be extended with an NFC interface. The NFC2SIM interface has to ensure packet integrity. The NFC readers has to follow the specification regarding atomic reads and writes and to be able to insert incoming data into frames and add integrity protection.

VII. CONCLUSION

The introduction of NFC enabled identity management is possible with a few enhancements in the providers network and adding NFC reader modules to the mobile phones.

It can provide a safe, trusted platform with user controlled key management and possible remote revocation of compromised keys.

With the possiblity of NFC communication, the SIM can offer an identification service for other terminals without compromising the system's security.

REFERENCES

[1] Trusted Computing Group – Mobile Phone Working Group, *Use Case Scenarios v. 2.7*, TCG-MPWG, 2005

[2] Open Mobile Alliance, Digital Rights Management Short Paper, OMA, 2003

[3] J. Noll, V. Ribeiro, S.E. Thorsteinsson, "Telecom perspective on Scenarios and Business in Home Services", *Proc. Eurescom Summit 2005*, Heidelberg, Germany, 27.-29.4.2005, pp. 249-257

[4] J. Noll, Gy. Kálmán, U. Carlsen, *License Transfer Mechanisms Through Seamless Authentication*, Proceedings Winsys 2006, Setúbal, Portugal

[5] ETSI Technical Specification 100 977 v8.13.0

[6] E. Somogyi, *Mobile Access to Structured Home Content*, Master Thesis, UniK, Kjeller, Norway, Jan 2006

[7] NFC Record Type Definition (RTD) Technical Specification, 14.08.2006, first release

[8] *Near Field Communication Forum*, http://www.nfc-forum.org

[9] *Open AuTHentication initiative* *http://www.openauthentication.org/*

[10] *Deutsche Bahn AG, Handy Ticket* http://www.bahn.de/handy-ticket

[11] Rhein-Main-Verkehrsbund, get>>in, http://www.rmvplus.de/

György Kálmán is a Ph.D student at UniK, University Graduate Center in Kjeller, Norway. His research area covers personal and device authentication, security and privacy in wireless systems.

He got his M.Sc. degree in the area of communication networks from the Budapest University of Technology and Economics. He was Research Fellow at Telenor R&I at the Media Platforms group.

Dr. Josef Noll holds a professor stipend from the University of Oslo in the area of Mobile Services. Working areas include Mobile Authentication, Wireless Broadband Access, Personalised Services, Mobile-Fixed Integration and the Evolution to 4G systems.

He is also Senior Advisor at Telenor R&I in the Products and Markets group, and Senior Advisor in Movation. He received his Ph. D. from the University of Bochum (D), worked for the European Space Agency at ESTEC from 1991-1997, and from 1997-2005 at Telenor R&I.