SIM as Secure Key Storage in Communication Networks

György Kálmán, Josef Noll
UniK, University Graduate Center, Kjeller, Norway
{gyorgy, josef}@unik.no

***Abstract*— With the exponentially growing number of users, who are accessing online services, easy authentication became a key factor. A trusted and secure platform can enable seamless authentication in most of the applications. This paper extends the possible use of the Subscriber Identity Module (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.

Scenarios for different security or user needs are shown and appropriate key policies are suggested. Solutions are focused on ease of use, security and the needs of different usage areas.

***Index Terms*— seamless, SIM, encryption, secure storage, identification, identity**

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. Both mechanisms 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 networks, the SIM cards, provide a possibility to extend the GSM-like seamless authentication to enable access of wireless networks and online services.

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 [1].

We think, that a hardware device, like the ones already widely used for bank and VPN access, is a good solution to provide a higher level of security with eliminating most of the possible weak points in passwords and other user chosen credentials.

This could be a separate one, like a usual one-time password generator or maybe a more advanced device. We propose to extend the possiblities of the generator device with two-way communication towards the network and also, to act as a primary authentication and key management solution.

To achieve this functionality, the device have to have a network connection, storage - preferably tamper resistant -, some computing power and a user interface, which is pleasant for the users.

Such a device could be the mobile phone, where the standardized SIM and java techology enables manufacturer independent implementation of an authentication entity without compromising the security of keys nor the user experience.

This paper will first show, why the mobile phone has the potential to serve as an identity provider in the digital world, it will justify the possible use of the SIM card, and propose a secure key management with the SIM card and NFC reader of the mobile handset.

Service scenarios will be shown, where different security and convenience factors are considered. An example NFC based phone admittance service will be presented.

II. Mobile Security Infrastructure

Today, users of cellular networks, like GSM and UMTS, are authenticated in a seamless manner. This enables operators to provide personalised services and incerase security while keeping the users free from the hassle of remembering different credentials.

The user is (optionally) authenticated by the PIN towards the handset, and this basic authentication together with the provider, which connects the identity of the SIM to a subscriber can enable personalisation functions. With extending this functionality, like requesting an additional username and password, a higher security service access can be enforced compared to traditional username password pairs.

The SIM card, as the base of this paper's proposal, provides wide encryption capabilites: e.g. Public Key Infrastructure (PKI), One Time Password (OTP), Extensible Authentication Protocol - Authentication and Key Agreement (EAP-AKA) or the normal SIM authentication.

These methods are also recommended by the Open AuTHentication initiative (OATH) [2], and accepted by most European governments as required technologies for digital signatures.

As stated in [3], the current GSM network is able to provide secure enough encryption for the most demanding applications. With extending the current infrastructure, employing the Extensible Authentication Protocol for GSM Subscriber Identity (EAP-SIM), the SIM card can supply network authentication services.

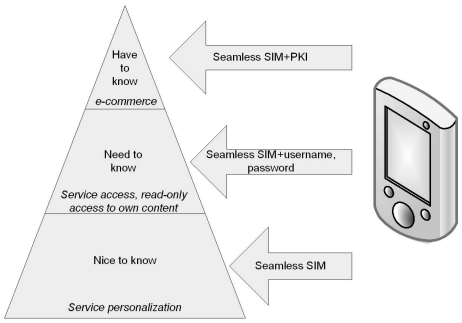

Fig. 1. The trust pyramid

This solution extends the possible use of the GSM networks authentication for wireless networks. We propose to use this authentication only for the initial network access, third party service access should use dedicated service keys. This can be either based on the EAP protocol family - EAP-TLS or EAP-IKE for example - or other PKI based solution.

In the service realm, different authentication levels are required in order to reach certain service levels, enable features. A possible categorisation of services is shown on Fig. 1. Based on this three categories, different key handling methods are needed.

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. Based on the user preferences, some services might be used with seamless authentication. Others will require SIM plus an additional knowledge based authentication.

The third level, *Have to know*, integrates the current One Time Password (OTP) systems and uses PKI in addition to the seamless SIM authentication to provide better security, for e. g. electronic banking.

SIM authentication is used for GSM/UMTS network access and in some specific segments for personalization of services [5]. In wireless networks EAP-SIM or Extensible Authentication Protocol - Authentication and Key Agreement (EAP-AKA) are examples of authentication using the SIM credentials for getting access. Introducing application specific access, we suggest implementing a set of access keys on the SIM card. This can lead to a more equalized access management while preserving the ease of use.

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

A. Handset as part of identity

In the physical world, the phone is becoming a permanent part of the user’s personal area. In many cases the handset is already part of the user’s identity.

In a convergence between the online and the physical world a part of the digital identity can be included into the phone preserving the convenience of the user.

Including indenification functions into the phone has considerable advantages:

- It is always available for the user,
- always connected to a network,
- has tamper resistant storage,
- widespread and
- trusted platform.

The key of the authentication functionality could be the SIM, since it already acts as authenticatior towards the mobile network.

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, as it enables

- 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.

III. Keyring in the SIM

This section shows a possible architecture, which is capable to provide the different security levels shown in Fig. 1. Admittance and payment services are enabled through introducing NFC into the phone.

According to [3] and ETSI standards [4], the SIM card provides a possibility of storing files in the internal storage.

The capacity of the SIM is currently at least 32 KBytes, which allows the storage of a considerable amount of keys, each of them typically beeing less then 1 Kb in size. The relatively low key sizes are justified with the possibility of downloading new keys over the air. Because of this function, the keys have to ensure security only for a limited time period (which is altough longer than a session key, typically months or a year).

Conditional file access features ensure, that access is enabled only for 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.

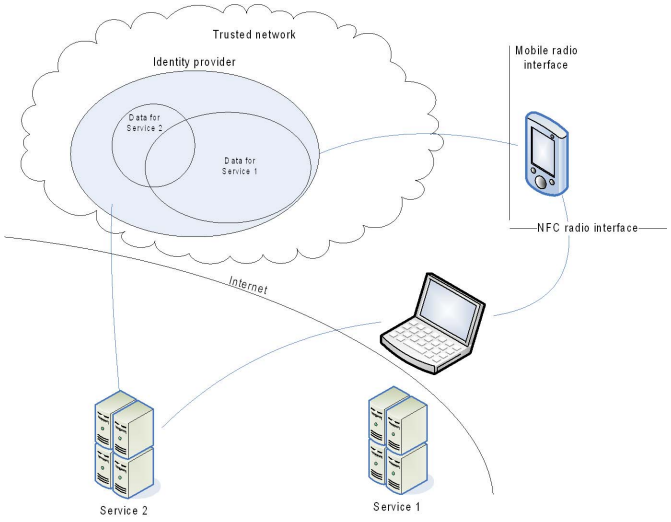

Fig. 2. Entities in secure service delivery

A. Architecture

With the SIM card, the system has an authenticator device, but mobile phones lack the capability of distributing the keys locally. The use of NFC as a primary transfer method of encryption keys is promising, because of it's limited range and standard-ensured atomicity.

In the proposed architecture (Fig. 2), the following actors are present:

a) User Terminal: NFC enabled terminal, from the service will be accessed.

b) Mobile Phone: NFC enabled mobile phone.

c) SIM: Subscriber Identity Module, with stored master key and the possiblity to store new encryption keys.

d) Identity Provider: A network service, which is able to provide identification and authentication services to end users and external services. Has direct connection to the mobile providers network or can access it through a secure channel. The identity provider maintains mutual trust relationships with external service providers and stores mobile phone master keys.

e) Service Provider: External service provider, which relies on the Identity Provider to authenticate users. Maintains trusted relationship with the Identity Provider, issues session keys for end users.

The sort range of NFC ensures secure key transfer. Also, the user's interaction is needed even for sending down session keys to an other terminal, since the handset must be placed very close.

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).

B. NFC in 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 to 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 identity provider and the user can get a new key without losing access to the services.

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.

Since authentication is needed just for several times a day, the power consumption of key exchanges doesn't affect the battery life of the phone considerably, especially when compared to other auxiliary hardware put into current models [9]. Standby power of the modules is approx. 25 mW and considered the short active periods, the transmit power of around 300 mW [8] is still acceptable.

The user may have the possiblity to identify itself via multilevel traditional username and password pairs, if the authentication device fails.

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.

IV. 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 challenge-response authentication, so the key won't be transmitted or even read out from the card.

With the use of the secure storage, the SIM can provide solid background for using authentication methods like EAP-TLS.

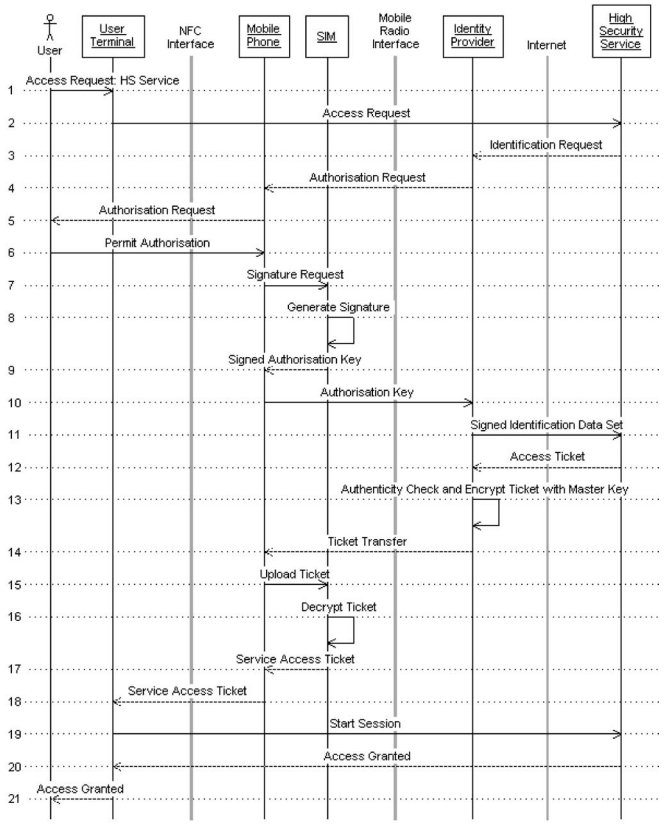

Fig. 3. Accessing a service with high security service

V. Service scenarios

Authentication with keys stored on the SIM can serve a wide range of possible services. Aside of the need of user identification, these services raise different needs towards the authentication process, key strength, validity period and user contact.

In the following, three different scenarios will be presented, which require different key processing and validation methods.

A. Short-term keys

In a high security environment, a *Have to know* authentication is required. A session key is negotiated with the help of the secret master key stored on the SIM by the operator.

The session key has a very limited validity period, after closing the session, it will be dropped. High security appliances will require to re-negotiate before every session.

As phishing is getting more widespread, mutual authentication has key importance. Since the Identity Provider maintains trusted relationship with the possible Service Providers, it can also check the authenticity of the incoming session key packages, before transmitting them to the phone. If the authenticity check succeeds, the Identity Provider encrypts it with the mobile phones master key, signs it with it's private key and transmits the package through the closed telecom network.

The signature can be checked inside the SIM and accepted only if the check succeeds.

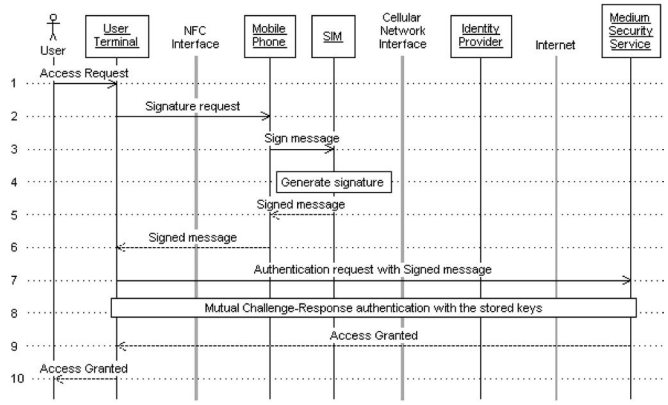

Fig. 4. Accessing a service with a stored temporary key

B. Medium-term keys

In services with lower security requirements, temporary storage of the encryption key may be allowed. This can enable seamless user authentication and lower authentication costs.

The first access to the service is done like in a high security environment, but instead of a session key, a long-term key is negotiated and stored on the SIM for a limited time period. This can be for example a week.

In this scenario, the first authentication is done as shown on Fig. 3, but the key is stored on the SIM. As such, the second access is done by a challenge-response authentication between the service provider and the mobile terminal (Fig. 4).

During the authentication process, the peers are identified mutually.

C. Long-term keys

Long term keys are stored on the SIM permanently. This keys can be e. g. DRM keys, personalisation keys, micro-payment IDs etc. These keys can be used for seamless user authentication, especially the personalisation keys, which are meant for such purpose.

Because of the long validity period of these keys, revocation is important. Enabled by the mobile network itself, the Identity Provider is capable to remove or invalidate stored keys. This ensures, that if the handset gets lost or somehow unauthorized access to SIM is becoming possible, the keys can be revoked without user interaction.

1) DRM keys: A right management key has usually a long lifespan. With a key stored in the secure storage of the SIM, the user can access the content without the need of being always connected [7].

With the appropriate home infrastructure, the user is able to generate and upload his own keys to the phone. This can enable e.g. granting access to own content for friends, family members or other users, with generating the appropriate key.

After that, the key can be uploaded to the user's phone with various methods, like sending down via NFC from the owner's phone or transmitted with a normal NFC device placed inside the owner's home network.

For example, if the user want's to access one of his documents stored on the User Terminal, which is encrypted

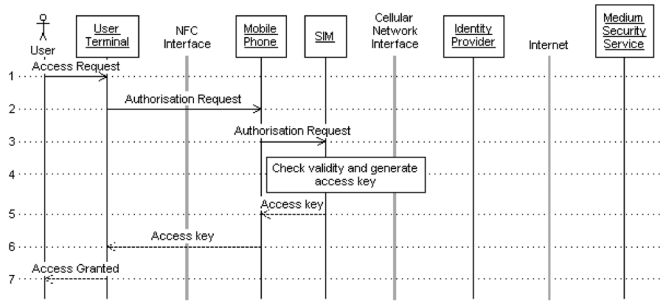

Fig. 5. Getting DRM keys from the phone

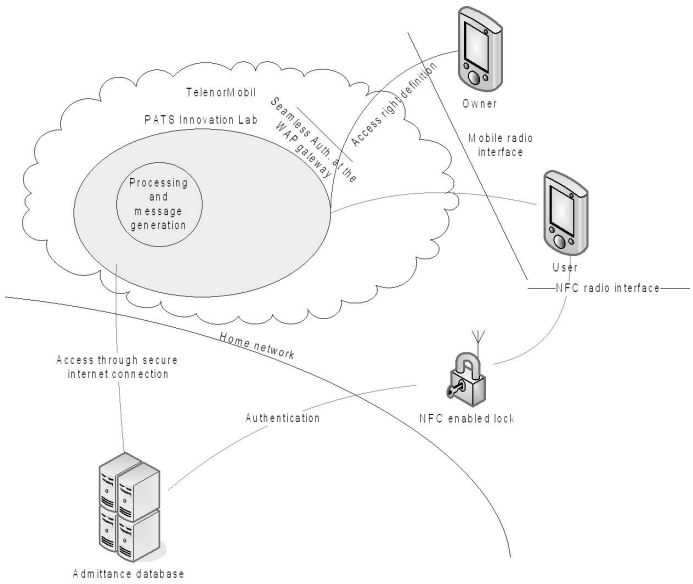

Fig. 6. Actual architecture based on fig. 2

using a DRM method, the mobile phone can provide the key without interacting with the DRM service on the remote server. An access to such content is shown on Fig. 5.

2) Personalisation: To provide personalised features, a service may want to authenticate the user (based on a minimal set of personal data, negotiated during the first key exchange).

The long-term keys can be used for example like cookies, to store preferred TV channels in the program guide or access package tracking at the user's favourite webshop (other account settings may be restricted to be accessed just with a fresh session key).

3) Micropayment: The SIM may store electronic money, which replaces the purse and allows offline purchases.

Electronical money is placed in the mobile phone and as such, the handset is the owner. As such, no further negotiation is needed with the bank or the identity provider. The user can show his will by placing the phone on the reader and for example pressing a random button, which will be requested on the screen of the mobile.

VI. A PRACTICAL EXAMPLE

In this section we show a working service based on the NFC integraton: SMS initiated admittance. The user can give a key to NFC enabled locks, by sending an SMS

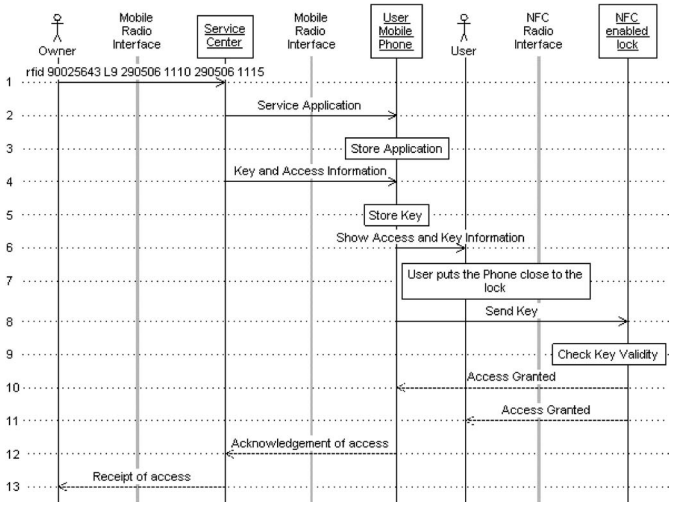

Fig. 7. Admittance Service with NFC

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 is done as follows:

Message: `rfid 00025643 L9 290506 1110`

1) John sends SMS to service number to allow Mary accessing his flat, through the door locked by lock 9.
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.

The actual system is working based on the services of Telenor's PATS Innovation lab and a set of Nokia 3220 phones with NFC shells attached. The seamless authentication of the owner is done by the PATS lab and also, composition of messages towards the user is done here [1].

It comprises elements of seamless authentication, interworking between mobile and near-field communication and provides new and advanced services to the end user.

VII. REQUIREMENTS AND FUTURE WORK

The proposed architecture has no special requirements towards the network, but requires an initial security setup. That consists of storing a master key on the SIM and also placing that key into the identity manager's database. It may be 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 use 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.

The Identity Providers must build trust relationships with Service Providers.

A drawback of the proposed architecture is, that the current phones already suffer because of the low battery capacities, altough based on [8], the transmitter won't cause a big drop. On the other hand, the required processing power highly depends on the actual implementation, say, the protocol set used and the transmitted data mass. As the proposal is based on a mobile device, energy awareness is of key importance.

Computing power raises also a user concern: if generation of a key needs several seconds, the users can get annoyed very fast, since the concept of NFC based key transfer is based on a *touch*. We think, that this can be solved with a properly optimised protocol stack or by changing the way keys are generated [10].

VIII. Conclusion

In this paper, we show a potential key management system. The current mobile phone system is able to provide these services with minor modifications.

The phone can provide a solid background for authentication solutions like EAP-TLS, because of it's hardware features and permanent connectivity towards the mobile network. With the keys in the SIM's secure storage, the phone can act as a highly advanced authentication device which can provide an all-in-one solution for user identification in various environments.

The SIM is a widespread, cheap and trusted platform for storing sensitive data, and with the proposed key management, it is able to provide security management for any service access. The user retains his full control during the whole identification process and can limit the data set, provided to new services. This ensures, that the service provider gets only the minimal amount of personal data, needed to grant access.

With these functionalities, a seamless authentication system based on SIM authentication is a cost effective and user-friendly way of rights and content management.

References

[1] J. Noll, J. Calvet, K. Myksvoll, *Admittance Services through Mobile Phone Short Messages*, ICWMC 2006

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

[3] Do van Thanh et al., *Offering SIM Strong Authentication to Internet Services*, Whitepaper, 3GSM World Congress, Feb 2006

[4] *ETSI Technical Specification 100 977 v8.13.0*, ETSI, Sophia Antipolis, France

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

[6] *AMUSE, A Mobility trial with Umts/wlan SEamlessly*, Technische Universität Eindhoven, 2004

[7] J. Noll, U. Carlsen, Gy. Kálmán, *License Transfer Mechanisms Through Seamless SIM Authentication*, Proceedings p. 333-338, Winsys 2006

[8] Philips Semiconductors, *Near Field Communication PN531 microprocessor based Transmission module*, v2.0, Philips, 2004

[9] Martin Peter Michael, *Energy Awareness for Mobile Devices*, Research Seminar on Energy Awareness, University of Helsinki, 2005

[10] Bogdan C. Popescu, Bruno Crispo, Frank L.A.J.Kamperman, Andrew S. Tanenbaum, *A DRM Security Architecture for Home Networks*, Proceedings of the 4th ACM workshop on Digital rights management, ACM Press New York, 2004

György Kálmán is a graduate 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.

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.