Admittance Services through Mobile Phone Short Messages

Josef Noll[1,2], Juan Carlos Lopez Calvet[2], Kjell Myksvoll[2]
[1]*UniK, N-2027 Kjeller, Norway,* [2]*Telenor R&D, N-1331 Fornebu, Norway*
josef@unik.no, juan.calvet@telenor.com, kjell.myksvoll@telenor.com

Abstract

A critical issue in the acceptance of wireless services is the authentication to these services. Wireless networks are available, including the home/office network, public hot-spots and the mobile networks. They will extend, including new access technologies such as 4G, and WiMax. Service take-up in these networks will be limited, unless seamless service access is guaranteed. The success of GSM, and especially of premium services (e.g. SMS, iMode) are based on seamless user authentication to the network and to the services, provided with adequate security.

This paper focuses on the current developments in Mobile phone/SIM card based authentication. The mobile phone can be used for physical access (admittance) and service access using near field communication (NFC). It may act as the security device in wireless network access, using EAP/SIM and Bluetooth, or using the SIM credentials for VPN and Mobile Commerce applications. In combining these authentication mechanisms, the Mobile phone has the potential being the identity provider in the virtual/electronic world.

1. Introduction

Authentication is the key for a customer relation, and the entry for value-added services. Telecom customers are used to hassle-free access (GSM works everywhere), and will expect the same functionality in all networks.

The customer is used having her mobile phone around, and the SIM card enables authentication and encryption in every wireless network (Bluetooth, WLAN, WiMAX) in addition to GSM and UMTS.

We focus not only on mobile networks, but service access in mobile and wireless networks. Broadband penetration is expected to reach 60 % in certain European regions, and 80 % of those households will built this home network wireless [1]. Because of widespread use in home environments, seamless and secured access to these networks is essential for providing broadband wireless services.

This paper will first postulate the need for identity in the virtual world. It will then justify why the mobile phone has the potential to serve as an identifier. Having addressed potential services and service scenarios, the paper will provide an example service demonstrating admittance control.

2. Identity in the Virtual World

In the real world, each of us has created his own spheres of identity. Identity is reputation: “what I say about me” and “what others say about me” [2]. My reputation is different, depending on whether I’m at work, doing sports, or enjoy membership awards in a club.

In the virtual world identity handling is more difficult, as it is mainly verified through an authentication mechanism. The Web community has defined Laws of Identity, providing a unifying identity meta-system that can offer the Internet the identity layer it needs [3]. One of the conclusions is to provide the user with the capabilities of providing exactly the information required to receive the service, and not his complete identity.

In this paper we focus on methods of using different identification mechanisms for the variety of services. Identification is based on unique service access keys in the SIM card, which are provided through wireless communications to the identifier.

3. Security infrastructure

From the many authentication initiatives, we propose to follow the mechanisms suggested by the Initiative for open authentication (OATH[1]):

- SIM authentication (SIM)
- Public Key Infrastructure (PKI)
- One-Time-Password (OTP)

[1] Initiative for Open Authentication, http://www.openauthentication.org/

These mechanisms fulfil the requirements of the Norwegian Government and other European countries for an eSignature. The mobile phone has the capabilities of providing all of them: SIM, PKI and OTP, and thus may provide the security requirements for various applications in the virtual world (figure 1).

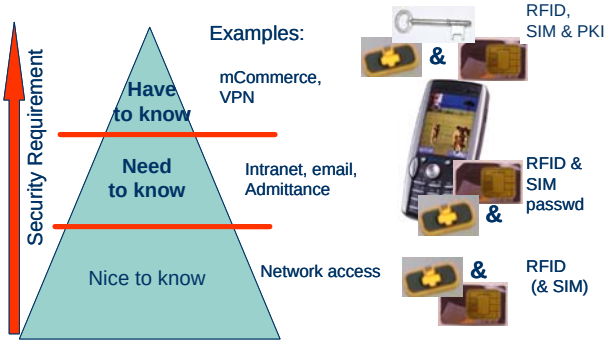

Figure 1 - Security infrastructure based on SIM, RFID and key management

We subdivide into three levels of security: *Nice to know*, *need to know* and *have to know*. *Nice to know* services are network access, where knowledge about usage is only required in case of misuse. A technical implementation might be based on the identification of the SIM card. *Need to know* services as Intranet access or Admittance have higher security requirements. These requirements might be satisfied through SIM authentication, and can be enhanced through a password/pin mechanism. Highest security requirements are required for *have to know* services, such as VPN or bank transactions. We recommend a PKI based authentication, which most European Operators have on their SIM cards.

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. The next chapters will provide a service scenario and provide details on the technical implementation.

4. Service scenario

In this chapter we provide a service example, indicating the potential of mobile phone based service access.

Scenario: John is the security responsible for a tenement house in a major European city. Major cost driver is the administration of admittance, especially when people loose their keys.

He replaced the lock system by Near Field Communication (NFC) enabled locks, providing control of admittance for everyone with a NFC phone. When John expects house cleaning or repairs, he just sends a short message (SMS), including the mobile phone number of the service people and the time interval for access to the flat. The service people will receive the admittance key to the flat, and can perform the requested service. On arrival and authentication, done through the NFC phone, John will receive a message that service people have entered.

This scenario covers only a subset of services indicated in figure 2, ranging from access to buildings and houses, ticketing services to VPN and eCommerce solutions. Further scenarios are addressed in the EU project ePerSpace [7]. What is common in all scenarios is the integration of service access, based on near field communication.

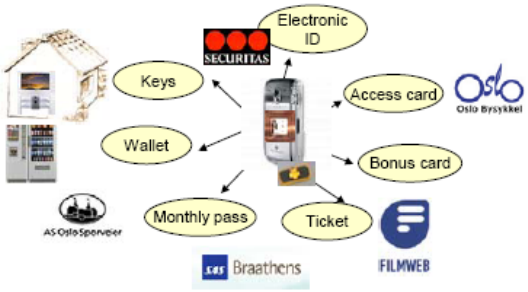

Figure 2 – Service scenario for mobile phone based access

5. NFC and GSM services

One of the main purposes of including the NFC technology into the SIM card was to be able to offer an alternative for the contactless card infrastructure. Contactless cards are common for admittance, and gain attraction as payment and ticketing cards in public transport systems.

Including NFC into the mobile phone gives contactless cards the advantage of being able to be installed, updated, backed-up and disabled over the air through the services offered by GSM. In case of loss of the phone all service access can be blocked by remotely disabling the SIM card. This feature provides enhanced security to the phone user, as a lost/stolen phone is of no further risk as soon as the loss is reported.

5.1. The NFC Forum

On April 2004 the NFC forum was establish with three founding members: Nokia, Philips and Sony with the vision of bringing the physical and the electronic world together. This was not a new vision, but was rather the Auto-ID labs "Internet of Things" vision, which was brought to the consumer market. By placing tags and readers into objects, users would be able to interact with them by touching them with other NFC devices (e.g. mobile phone).

The initial founders of the NFC forum saw the variety of opportunities that this technology would bring.

Philips provides two key elements into the NFC technology: The MIFARE standard, which is the most used contactless ticketing and payment standard in Europe with approximately 80 % of the market and the NFC chip itself.

Sony provides the Felica standard, which is the other biggest contactless ticketing and payment standard, mainly used in Asia.

Nokia brings this technology through the mobile phone to the mass-market. The main reason why Nokia was able to bring this vision to reality before other mobile phone manufacturers is because they were already active in integrating the RFID technology on their mobile phones focused towards industry usage such as mobile workforce management.

Since April until February 2006 more than 70 members have joined the forum from a wide variety of industries [8]. There are four levels of membership, but steering of the NFC forum is still performed by the founding members with the addition of VISA and Master Card who together dominate the payment market.

5.2. 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.

One of the main technological advantages of an integrated NFC module is that the phone can act both as a reader and a card, and is backward compatible with the contactless card standards. Therefore it makes a mobile phone an ideal device for making payments and gaining access. The user can through the mobile phone control the access to the NFC identity, the operator can update or cancel the card remotely and the phone is a device that users are already carrying.

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.*

5.3. The SIM in NFC

With the introduction of the NFC technology into the mobile phones, the SIM card takes a more important role for payment, ticketing and SIM card providers.

When NFC functions as a contactless card, it requires a place to store critical information such as ticket numbers, credit card accounts or ID information. This storage place could be basically anywhere in the mobile phone (RAM), but since the SIM card has storage capacity and already offers a high level of security; it is the obvious place for storage of critical and sensitive information (figure 3).

One problem is that communication between the NFC chip and the SIM card does not exist today and has therefore to be standardized. This is one of the main reasons why NFC mobile phones are still in the demonstration phase. The communication between the SIM card and the NFC chip requires a high-speed transaction in order to offer a real alternative for today's ticketing and payment system. Users would not accept a new ticketing solution that is not easier or faster than the already available solutions offered by contactless plastic cards.

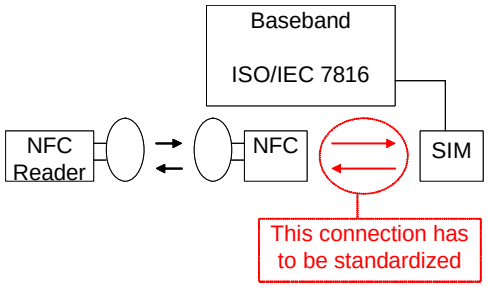

Figure 3 – Interface standardization for SIM key exchange

Standardization of the NFC/SIM interface is ongoing [8], incorporating mobile phone manufacturers, operators and SIM-card suppliers.

6. Implementations and demonstrations

Prototypes and demonstrations of the capabilities for SIM authentication are well under way. This chapter will provide examples of demonstrations, covering the capabilities and indicating where future research work is needed.

6.1. Prototype and early demonstrations

The first prototype in the transportation area was conducted by the Rhein-Main Verkehrsverbund (RMV), the public transport network operator for Frankfurt's greater area in Germany [8]. RMV launched a mobile ticketing project in early 2005 in the city of Hanau. It used NFC equipped mobile phones as a contactless ticket for the existing ticketing infrastructure. The solution was tested in Hanau allowing customers to buy, store and use tickets with a Nokia 3220 NFC mobile phone.

Since the pilot used the first version of the NFC Nokia phones, it wasn't able to store the electronic ticketing information on the SIM card, but instead it used an integrated smart card controller in the phone.

The first European trial combining NFC and PKI based electronic transactions was demonstrated in January 2005. The demonstration was realized through a Nokia NFC phone making use of Telenor's eCommerce platform for mobile purchase [4,5].

Telenor R&D and Nokia are currently joining efforts to test the NFC technology together with the most relevant transport systems in Norway, since there is a national effort to migrate ticketing systems all around the country towards a contactless card infrastructure where travellers can use the same card in any kind of transport (train, ferries, subway and busses).

6.2. 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 take up the service scenario of chapter 4 and explain the steps required to achieve an SMS initiated admittance. The admittance control is performed through the following steps (see figure 4):

1) *John* sends SMS to service number to allow *Mary* accessing his flat 15b.
   Example: SMS to 2034 "90838066 17.12.2006 1000-1400"
2) Service centre creates an service SMS installed on *Mary's* phone 90838066:
   "Admittance key transferred to NFC phone"
3) Service centre informs *Mary*:
   "Access granted to flat 15b, My Road, My City on 17.12.2006 from 1000-1400h. Use phone to get entrance."
4) *Mary* enters flat 15b with help of NFC phone. *John* might receive an acknowledge message when *Mary* enters the flat.

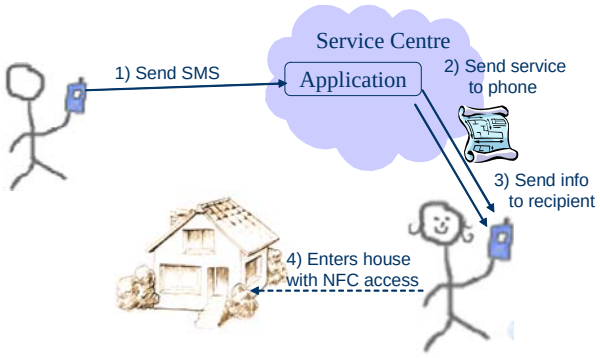

Figure 4 - Message structure for SMS supported Admittance Control

This example of an admittance control 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.

7. Privacy Concern & Security

Users are increasingly more concerned about the privacy of information, and when it comes to RFID cards or phones that hold sensitive information such as bank accounts or credit card numbers, they are afraid of theft and misuse. Such fears could be the biggest barrier for adoption of RFID based payments.

RFID payment devices offer a higher level of security than traditional payment cards. The ISO 14443, which is the standard adopted by credit card issuers (MasterCard, Visa and American Express) allows the account information on the card to be encrypted: Giving each company the possibility to use

a different encryption method and keys.

Unlike RFID for supply chain management, this standard is specified for very short-range communication (up to 4 cm) making it difficult to read from long distances. Even if someone is able to read the data with a specialized long-range interrogator, the attacker will still have to crack the encryption algorithms to be able to make some sense of the data acquired.

Security of information is maximized: When the cardholder waves the card by an RFID payment terminal, it turns the encrypted number into a digital signature, which is passed through the payment network and then decrypted to authorize the transaction. To further protect the account information, the digital signature changes each time a card is read. So even if a thief were to somehow access the digital signature, it could not be used to make another transaction.

The main challenge is therefore for card associations, banks and merchants to send a clear message to consumers that contactless payment systems are actually more secure than today's cards if they want consumers to comfortably adopt the technology.

8. Strategy for Operators

The SIM card has always been the most important asset of GSM mobile operators, but regardless of many efforts to increase its value towards the user, operators haven't been able to show this benefit to the customers.

The introduction of the NFC technology brings the unique opportunity to easily connect the SIM card with the physical world. All the visions of mobile payments can finally be realized without cumbersome WAP menus or slow SIM toolkit applications.

With the adoption of NFC, the SIM card will increase its value dramatically by storing the end users most valuable information: credit card numbers, bank account numbers, personal Ids, plane tickets, bus tickets, and bonus cards. This gives the operators the unique opportunity to offer a "real state" type of business to third parties like credit card issuers, banks, and transport companies. However, this will only happen if operators allow third parties to bring their applications to the phones and credentials to the SIM card.

NFC has the potential to change the operators' role from "access provision" to "service provision" (figure 4).

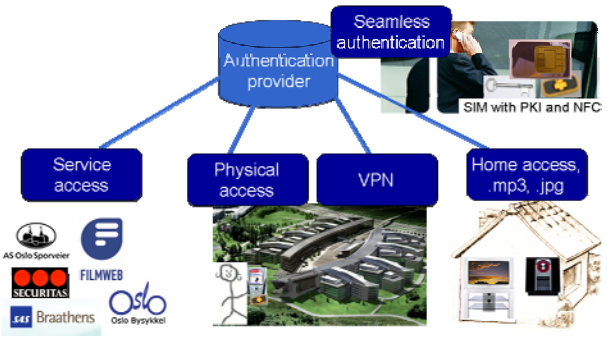

Figure 4 – Mobile operator as authentication provider

9. Conclusions

This paper indicated the challenges when addressing identification in the virtual world. It introduces the mobile phone, enhanced by PKI infrastructure and near field communication (NFC) capabilities to comply with governmental requirements for an eSignature. It provides examples for new services based on seamless mobile phone initiated authentication, fulfilling the security requirements and enabling seamless access to personalized services. The paper presented the prototype of an admittance control through the mobile phone messages (SMS), and addressed a potential strategy for Operators.

Acknowledgement

The work was partially funded by the European Union in the FP6 ePerSpace integrated project, the FP6 OBAN project and Eurescom P1401 OSIAN project.

10. References

[1] 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

[2] D. Hardt, "Identity 2.0", *OSCON 2005*, http://www.identity20.com/media/OSCON2005/

[3] K. Cameron, "The Laws of Identity", http://www.identityblog.com/stories/2005/07/25/thelaws.html

[4] J. Noll, J.C. Lopez Calvet, "Business through Mobile Phone initiated Near Field Communication", *Norwegian UMTS forum*, Oslo, 11.5.2005

[5] J. Noll, J.C. Lopez Calvet, "SIM-card enabled Seamless Access in Mobile and Broadband Access Networks",

Proceedings of the WWRF #15 meeting, Paris, 8.-9.12.2005
[6] E. Somogyi, "Mobile Access to Structured Home Content", *Master Thesis, UniK*, Kjeller, Norway, Jan 2006
[7] IST FP6 project *ePerSpace – Towards personalised services at home and everywhere*, http://www.ist-eperspace.org/
[8] *Near Field Communication Forum*, http://www.nfc-forum.org

Josef Noll is Prof. stip. at the University Graduate Centre at Kjeller, Norway (UniK) in the area of Mobile Systems. He is also Senior Researcher at Telenor R&D in the Products and Markets group. 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&D.

His working areas include Mobile Authentication, Wireless Broadband Access, Personalised Services, Mobile-Fixed Integration and the Evolution to 4G systems.

Juan Carlos Lopez Calvet is Research Manager at Telenor R&D, responsible for Mobile Terminal developments.

His working areas cover IP security and Mobile Technologies. Having received several awards for new mobile business, he is now leading the development and demonstrations of NFC-based applications in Telenor.

Kjell Myksvoll is engineer at Telenor R&D in the Mobile Terminal group.

His current areas of interest are NFC and NFC-based applications, operating systems for mobile phones and application development for mobile phones. He is the technical leader of NFC-based demonstration and prototype developments.