WIRELESS WORLD

RESEARCH FORUM

Abstracts for Contributions to the WWRF15 Meeting

Using this template will provide the reviewers with uniform information, which will simplify their work. Please delete the guidance given between < > when typing.

1 WG or SIG to which this Contribution is submitted[1]:

SIG2

2 State which of the categories a) – f) on the front page of the CfC this Contribution is addressing:

a) Contributing to the currently identified research areas of the WGs or SIGs

3 Title of research item

SIM-card enabled Seamless Access in Mobile and Broadband Access Networks

4 Contact details of author/submitter

Josef Noll, Josef@unik.no, ph: +47 9083 8066, UniK - University Graduate Centre, N-2027 Kjeller, Norway

Juan Carlos Lopez Calvet, juan.calvet@telenor.com, Telenor R&D, N-1331 Fornebu, Norway

5 Subject area (WG/SIG and subtopic (as of CfC) where appropriate)

- Identification of new features, mechanisms and protocols for identity management and AAA

- Identify new requirements, solutions and potential research areas in the field of security and trust in mobile communication systems.

6 Relevance of the topic to the above subject area

- Topic has been chosen to address potential of SIM card based authentication for seamless service access

- Addressing the user needs for “convenience” and “seamless security”

- Enabling personalised services in mobile and wireless networks

- Opening for new business in e.g. access to private content, home surveillance

7 Preferred presentation form: < speech or poster >

Speech

8 Abstract (on next pages)

[1] If you are submitting this contribution to several WGs/SIGs, please state to which and stress to which you would prefer have it presented.

SIM-card enabled Seamless Access in Mobile and Broadband Access Networks

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

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 becomes the identity provider in the virtual/electronic world.

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 to having her mobile phone around, and the SIM card opens for 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]. Usage of private WLAN networks is inexpensive, thus 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 conclude with an overview over current developments. Developments addressing RFID/NFC and Bluetooth based authentications, and functionality in the mobile network through WAP gateway and Traffic Analyser.

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, who define a unifying identity metasystem 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 based on unique access keys in the SIM card, and provided through wireless communications to the identifier.

Security infrastructure

From the many authentication initiatives, we propose to follow the mechanisms suggested

by the Initiative for open authentication (OATH)[2]:

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

These mechanisms fulfill 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).

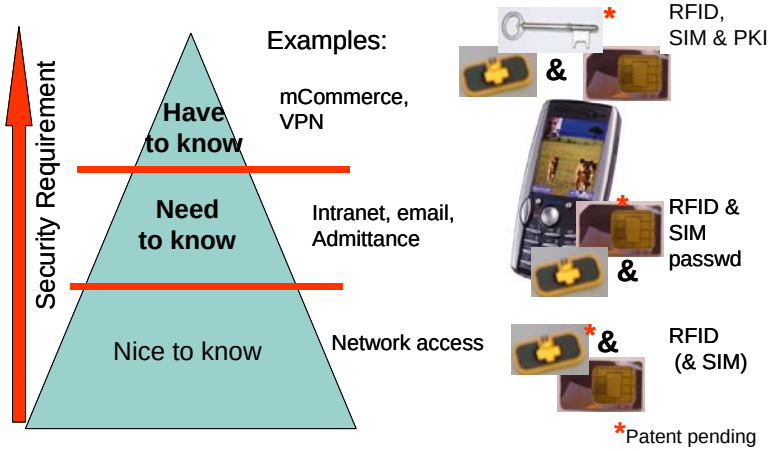

Figure 1: Security requirements

Current implementations as the EAP/SIM use the same credential for getting access. We suggest to introduce 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 the new car through the mobile phone.

Service scenario

In this chapter we provide a service example, which will be extended by the more complete set of potential services in the full paper.

Scenario: John is taking the subway to meet his friend Mary at the city centre, before entering the subway he places his mobile phone in front of the information kiosk at the station. The screen shows that he doesn't have a valid ticket, so he sends an SMS to the mCommerce service number 2500 "Oslo day" and after a couple of seconds he receives an SMS that configures the RFID tag in his phone with a day ticket for Oslo. He places his phone at the gate and enters the subway.

While on the subway he decides that it would be a good idea to go to the movies. He uses mCommerce to buy two tickets and shortly after he receives an SMS that configures the RFID tag in his phone with two movie tickets. When they show up at the cinema, he places his phone in front of the ticket machine and immediately receives to printed tickets.

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.

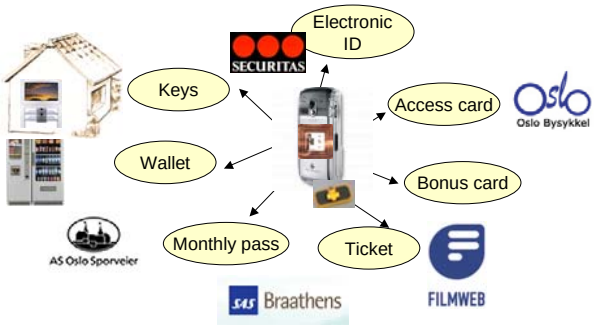

Figure 2: Potential services

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.

- Seamless access to an Open Broadband Access Network (OBAN). One of the first demonstrations of using seamless access to WLAN, authenticated through the SIM card in the mobile phone was given in

[2] OATH: http://www.openauthentication.org

June 2005 [4]. The demonstration was realized using EAP/SIM and Bluetooth SAP profile.

- The first European trial in using an NFC phone to purchase goods, demonstrated in January 2005. The demonstration was realized through a Nokia NFC phone making use of Telenor's eCommerce platform for mobile purchase [5,6].
- Automatic login to personalized home services, currently under development at Telenor & UniK. Authentication information is provided through the WAP gateway and UMTS traffic analyzer by adding the MD5 hash of the MSISDN. [7]

A more extended list will be provided in the paper, with details on the implementations.

Conclusions

This abstract 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.

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.

References

[1] Josef Noll, Vitor Ribeiro, Saemundur E. Thorsteinsson, "Telecom perspective on Scenarios and Business in Home Services", Eurescom Summit 2005, Heidelberg, Germany, 27.-29.4.2005,

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

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

[4] IST FP6 project OBAN – Open Broadband Access, http://www.telenor.no/fou/prosjekter/oban/

[5] Josef Noll, Juan Carlos Lopez Calvet, "Business through Mobile Phone initiated Near Field Communication", Norsk UMTS forum, Oslo, 11.5.2005

[6] Josef Noll, "Near field communication and RFID – opening for new business", tutorial at Eurescom Summit 2005, Heidelberg, Germany, 27.-29.4.2005, www.eurescom.de/summit2005/

[7] IST FP6 project ePerSpace – Towards personalised services at home and everywhere, http://www.ist-eperspace.org/