Services and Applications in Future Wireless Networks

JOSEF NOLL

Josef Noll is Prof.stip. at the University Graduate Centre at Kjeller (UniK), Norway

This *Telektronikk* contribution will provide a view on the future wireless service landscape, with a special focus on seamless service access to wireless services. Authentication for mobile network access is performed through the SIM card. In wireless networks such as the IEEE802.11 family authentication might be provided through SIM related protocols being the Extensible Authentication Protocol for Subscriber Identity (EAP-SIM) and the EAP for UMTS Authentication and Key Agreement (EAP-AKA). With the help of the Bluetooth SIM access profile (SAP), the SIM credentials can be transferred from one device (typically the mobile phone) to a second device (a laptop) for seamless WLAN network access for the user. Near field communication (NFC) has the potential of providing contactless authentication services, including identification to home devices. A critical issue is NFC2SIM, the interface from NFC to the SIM card. The contribution concludes with an overview over upcoming personalised broadband wireless services, including home data access and community services.

1 Introduction

Third generation (3G) mobile systems have entered the market, providing enhanced functionality to deliver multimedia communication to the mobile user. Network costs and limited cell capacity [1] have opened discussions on how to extend the public cellular network using other access networks, e.g. WLAN access or using UMTS as a return channel for a personalised DVB system. Such integration also requires additional network functionality for interworking and interoperation. The resulting system clearly represents an advanced stage of 3G, or even beyond 3G (B3G) depending on the definition. Work is ongoing in standardisation, specifically within ITU in the special study group on IMT-2000 and beyond IMT-2000 [2]. The Wireless World Research Forum and 3G.IP are other organisations heavily involved in B3G [3][4].

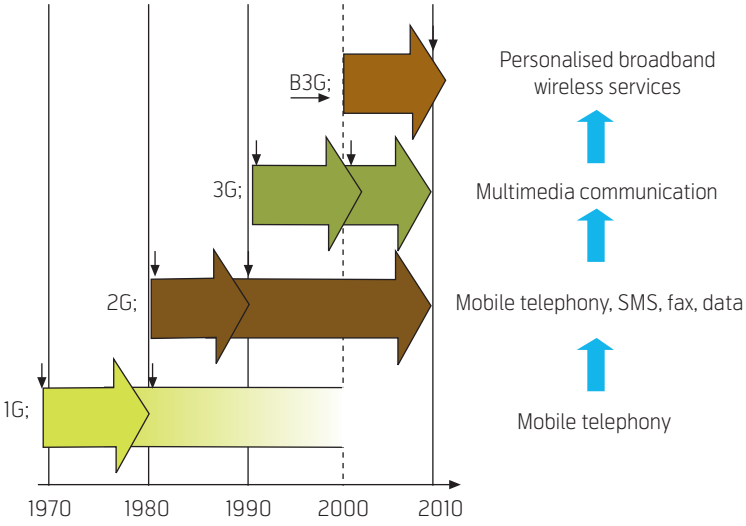

Figure 1 Service evolution from mobile telephony to personalized broadband wireless services

The major conclusions from the ongoing work state the need for addressing the relationship between User preferences, Services, and Technologies [5]. Access is expected to be provided through all kinds of wireless access networks, ranging from broadcast to wireless/mobile access systems. The main focus will be on providing personalised wireless services to the user.

This paper will in Section 2 provide an introduction to systems beyond 3G, address the communication challenges in Section 3, and introduce identity management in Section 4. It provides an overview over future community services in Section 5. The paper finally provides examples of services in the digital world in Section 6, and conclusions in Section 7.

2 "Beyond 3G"

Mobile telecommunication systems were previously defined in *generations* (see Figure 1). In the analogue system, mobile telephony was the first telecom communication service. One of the main reasons for introducing GSM was mobile telephony service provision in European countries, including SMS and data services. 3G was introduced to provide roaming on a world-wide base, and compatible standards such as UMTS currently provide multimedia communication in the whole world. "Systems beyond 3G" will provide personalized wireless broadband access and will incorporate mobile and wireless access methods including e.g. Wi-Fi, WiMAX [5].

Standardization of the system B3G started in 2000, and consists of the three major elements:

- *Wireless services:* Users prefer to receive their services wireless, either through the mobile network or a wireless (Wi-Fi) connection. This statement is

underlined by the sales numbers of mobile phones and laptops: There are 1.5 billion cell phones in the world today, more than three times the number of PCs [6]. In June 2005 the number of laptops sold bypassed the number of fixed PCs [7].

- *Broadband services:* Market expectations for fixed broadband services estimate that 60 % of households will have broadband in 2007 [8]. Mobile broadband services like TV and video telephony are available in most 3G markets.

- *Personalised Services:* The wide distribution of mobile phones has increased the need for adapting the content to both user preferences, terminal and network capabilities.

2.1 Wireless services

The major challenge of wireless service provision is the variation in radio quality. Radio is a shared resource, and the quality of the radio link is affected by:

- User mobility,
- Radio environment (user speed and coverage radius),
- Application topology, and
- User terminal requirements.

Service delivery to a wireless terminal should take into account the Quality of Service (QoS) measures on the radio interface, e.g. propagation delay, variation of delay, bit error rate, error free seconds, distortion, signal to noise ratio, duration of interruption, interruption probability, time between interruption, bit rate, and throughput. These parameters will depend on the user and terminal environment, and underline that an optimum access will have to use all available wireless and mobile connections.

2.2 Broadband services

Gordon Moore's prediction, popularly known as Moore's Law, states that the number of transistors on a chip doubles about every two years (Figure 2) [9]. Since the start of the digital age the amount of information created is tripled approximately every 12 months. Comparing these growth rates with the increase of modem speed and air interface capacity shows that modem speed has a similar growth rate to the number of transistors, while air interface capacity has not increased substantially from GSM to 3G/Wi-Fi. The experienced increase in air capacity is due to increased bandwidth B of the communication channel, from B_{GSM} = 200 kHz in GSM to B_{UMTS} = 3.8 MHz in UMTS, and $B_{802.11}$ = 25 MHz for 802.11b.

Claude E. Shannon defined the capacity C of a system as being proportional to the bandwidth B

$$C = B \log_2 (1 + P / N_0 B), \quad (1)$$

with B the bandwidth of the carrier, P the signal power and N_0 the noise level of the system. For a given bandwidth B, the maximum range R_{max} is a log-function of the signal to noise ratio

$$R_{max} = \log_2 (1 + P / N_0) \quad (2)$$

Propagation attenuation (free space loss) is proportional to the carrier frequency, thus carriers such as Wi-Fi have shorter ranges than GSM, but provide higher throughput. These indications support the usage of specific access networks for applications, e.g. broadcast for video, Wi-Fi for email and ftp services, and GSM/UMTS for mobile services. It can be assumed that services are available through all access networks, but will have their preferred network for operations.

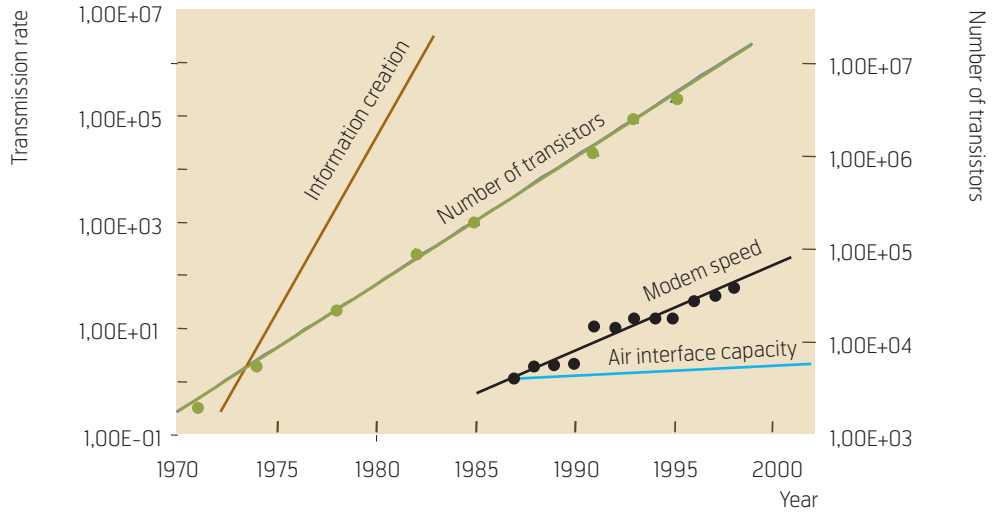

Figure 2 Moore's Law in transmission capacity and information creation

2.3 Personalised services

In order to design and develop innovative and successful services one has to understand the user and be able to "guess" his needs. This is the area of market researchers and service designers who have to sense and test the usability and social impacts of new service concepts, while looking for the added value that could make a service offer a success. To that end a phased methodology is recommended addressing the following topics [5]:

1 Understanding the users by understanding their culture and lifestyle;

2 Creating potential service concepts that satisfy particular user needs described by technical details and likely usage;

3 Validating the service concept against potential users by means of prototypes and models.

To build these types of personalised services is a challenge to the system design as well as the user interface. The system should be flexible and allow the definition of personal preferences, and these should be carried seamlessly with the user as he moves geographically or between access networks. The user interface should be such that personalisation is easy and intuitive. Personalisation might be supported by "learning" profiles handling the preferences of the user, the "presence" (where is the user, what is he doing), and the social/community characteristic of a user.

The next section will provide an overview of existing developments in order to overcome the borders between wireless and mobile networks.

3 Communication challenges

This section addresses the communication challenges of a mobile user, analysing trends in radio communication development, the position of the mobile phone and authentication as key issue for user acceptance.

3.1 Radio communications

Section 2 has concluded that optimum access networks will have to be used for the specific applications. This section will look into existing standardisation and market trends for wireless network access, e.g. UMA, IMS, and Bluephone.

3.1.1 Unlicensed Mobile Access (UMA)

The UMA Technology specification will allow the usage of mobile phones in unlicensed bands, typically using Wi-Fi or Bluetooth as radio interface. Typical applications cover the home and office environment, where WLAN subnets exist, but usage of mobile phones in those networks is not yet supported. Submitted in February 2005 to the 3rd generation partnership project (3GPP), UMA specifications are adopted as Generic Access Network (GAN) within the GERAN (GSM/EDGE Radio Access Network) TSG (Technical Specifications Group).

UMA has thus become the standard for fixed-mobile convergence (FMC). UMA technology enables access to mobile voice, data and IMS services over IP broadband access and unlicensed spectrum technologies. By deploying UMA technology, service providers can enable subscribers to roam and handover between cellular networks and public and private unlicensed wireless networks using dual-mode mobile handsets. With UMA, subscribers receive a consistent user experience for their mobile voice, data and IMS services as they transition between networks [10].

3.1.2 British Telecom – Bluephone/Fusion

While Eurescom launched a study called "Public Bluetooth Access" in 2001 [11], parallel developments started at British Telecom (BT) to enable Bluetooth based mobile services. Technical problems such as interference, especially in the voice channel, and missing standardisation delayed the launch of the *Bluephone* product until mid June 2005 [12]. After successful customer testing in 2005, BT runs the service as a conventional FMC package called *Fusion*, offering a Wi-Fi/Bluetooth combined router, which users can plug into BT's Broadband ADSL at home. Currently two mobile phones are supported, Motorola's RAZR V3 and V560.

The main difference between *Fusion* and UMA is the focus of the network operator. *Fusion* is based on SIP and IMS standards, thus promoting the developments in the direction of next generation networks, while UMA brings the home area into the mobile network, using mobile network core technologies.

3.2 My future terminal

While the access network development will follow the main position of the operator, i.e. mobile operators will tend to promote UMA, while fixed network operators will promote *Fusion*-like approaches, the developments on the terminal side are more widespread.

We see two major trends, on the one hand following the PC and making applications available for the mobile user, and on the other hand the development of specific mobile services, promoting lifestyle and community services. The mobile phone has the major advantage as it is available 24 hours / 7 days a week, as compared to about 4 h average usage of a PC.

Figure 3 Functionality of mobile terminals, e.g. communication portal (left), public transport information (middle, from [13]), video/surveillance (right)

Thus, the mobile phone provides the *always online* functionality with availability, email and Internet access (see Figure 3). While this trend is visible in the enterprise market, the consumer market is dominated by lifestyle trends. Decisions to buy a certain phone are rather based on attitude, e.g. the tough phone for the outdoor person, and the city phone for the urban person.

What is common in both trends is that service availability has reached all phones. Communication and interaction is provided, connectivity to my community (Figure 3, left), local services such as public transport information (Figure 3, middle) and video/TV (Figure 3, right) show some of the potential services.

The mobile phone has several service enablers inbuilt, i.e. positioning information, potential for seamless and personalised service access, mobile commerce, and adaptation of content to personal preferences. However, these advantages are not yet properly addressed by the operators. The following section will provide examples of personalised service access, indicating the potential of mobile services, but also addressing the current deficits.

3.3 Device, network and service authentication

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 for access to other networks and services. The customer is used to having the 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.

Service authentication has to satisfy the security requirements of the application, e.g. *nice to know* security for network access, *need to know* security for email and intranet access and *have to know* security for VPN and *m*Commerce services. We suggest the following the mechanisms from the Initiative for open authentication (OATH[1)]):

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

These mechanisms fulfil the requirements of the Norwegian Government and other European countries for an *e*Signature. 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.

The security requirements might be satisfied through SIM authentication and can be enhanced through a password/pin mechanism. The highest security requirements are required for *have to know* services, such as admin access to home content or electronic transactions. We recommend a PKI based authentication, which most European Operators have on their SIM cards [14].

1) *http://www. www.openauthentication.org/*

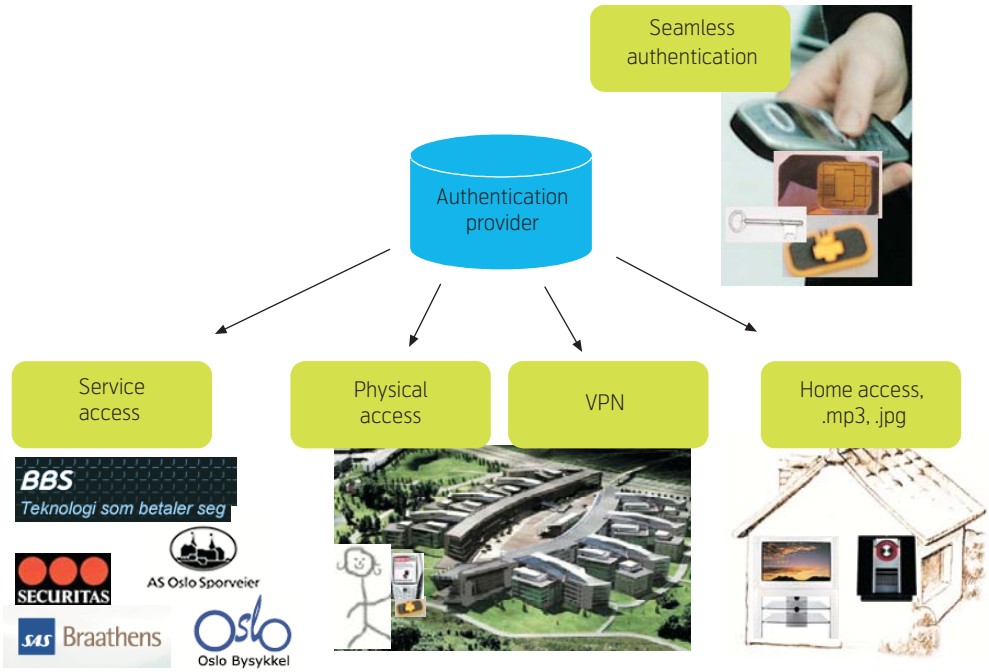

Figure 4 The mobile phone as authentication device for admittance, network and service access

4 My identity in the digital world

This section postulates the need for identity in the virtual world. It will identify the threats of using biometric identification, and suggests the mobile phone as an identifier. In the virtual world identity is 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 [15]. 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.

4.1 Biometrics versus SIM card

Biometrics, especially the fingerprint is used nowadays for identification to systems and services. Fingerprint authentication is used by Lufthansa to speed up check-in procedures and the hand's palm vein pattern by the Tokyo-Mitsubishi banks to increase security in ATM money withdrawal. Avivah Litan, an analyst with Gartner, argues that biometrics is the most secure form of authentication because it is the hardest to imitate and duplicate [16].

Current discussion is ongoing on how a safe storage of biometric information can be performed. Once biometrical information is stolen, it cannot be revealed. The fear of permanently losing your ability to use a biometric trait has caused European Legislators to deny usage of biometrical information. Measures are taken as e.g. a two-factor protection of the biometric information to protect the information, but the missing revocation is the most critical issue when it comes to biometrics.

Section 3.3 introduced the security mechanisms needed for different kinds of applications and has a two-factor authentication for the *has to know* security level. The SIM card in the mobile phone has the capability of providing all levels of authentication and supports mechanisms for revocation of credentials stored in the SIM card. A SIM card is only active if authenticated by the network operator. If the SIM card gets stolen, the operator can disable the card. The main challenge is on how SIM information can be securely distributed to other devices and services.

4.2 Supporting technologies

SIM authentication is used for GSM/UMTS network access and also as transaction receipts for content download, e.g. ring tones. Including authentication methods through Bluetooth and Near Field Communications (NFC), SIM-based authentication opens for all types of service access (see Figure 4). The NFC forum has introduced RFID technologies in mobile phones, and thus allows the mobile phone to replace contactless credit cards and admittance cards [17].

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 basically be 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 5).

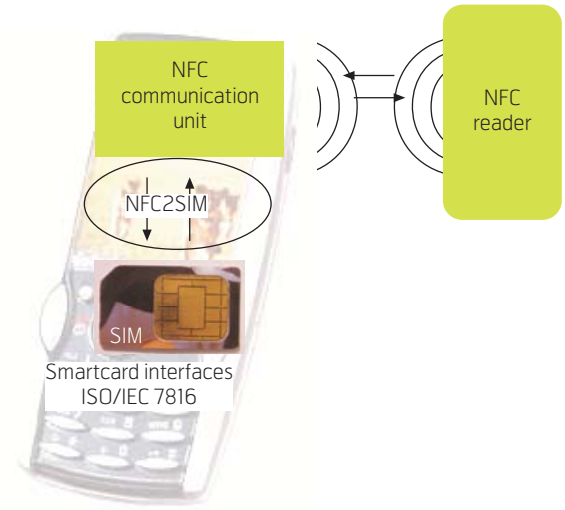

Figure 5 Mobile authentication based on near field communications (NFC)

Communication between the NFC chip and the SIM card, called NFC2SIM, has to be developed and 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 to today's ticketing and payment systems. Users would not accept a new ticketing solution that is not easier or faster than the already available solutions offered by contactless plastic cards.

Authentication for network access is performed in the mobile network through the SIM card. In wireless networks such as the IEEE802.11 family authentication might be provided through various protocols, with the two SIM related protocols being the Extensible Authentication Protocol for Subscriber Identity (EAP-SIM) and the EAP for UMTS Authentication and Key Agreement (EAP-AKA). If a mobile phone supports EAP-SIM, it can seamlessly connect to WLAN networks using the SIM card. With the help of the Bluetooth SIM access profile (SAP), the SIM credentials can be transferred from one device (typically the mobile phone) to a second device (a laptop) for seamless WLAN network access of the user. The EAP-SIM and Bluetooth SAP profile interworking has been demonstrated on several occasions, but is currently only available for a limited number of mobile phones [18].

SIM-based service authentication in mobile networks is known from premium SMS services, e.g. ring tone and logo download. Operators have introduced the SIM authentication also for WAP services, allowing e.g. a seamless access to the personal email account through the WAP portal. The WAP gateway adds an information string to the http header, which is forwarded to the content server. The string contains both information on the user and the device requesting the service. The user (x-nokia-alias) is represented through an md5 hash of the mobile ID (MSISDN), and the device is represented through a device identifier (mobile phone type) [19].

The following section will provide examples of services based on seamless authentication.

5 Community services

Having addressed security requirements and mobile phone/SIM-based authentication as a major service enabler, this section will address upcoming services. It will first address community services and then position the mobile phone as integrator for mobile and broadband services.

5.1 Communities, groups and roles

The digital services trend has reached everyday life. Information is spread by Internet, email and SMS, rather than by plain paper. Youngsters use micro coordination, using the mobile phone to communicate with their community at every minute of the day [20]. Depending on the context, these communities are changing, ranging from working colleagues to friends, to members of classes, school, or sporting clubs. Figure 6 indicates a location based service for a friend community, indicating at all times where your friends are, and even introducing an alert when a friend comes nearby. The mobile phone is the preferred device to keep control of your communities, providing availability, location and communication.

Community services will become more dominant in the future, addressing contact, location and availability as well as exchange of pictures, music and other digital content.

5.2 Digital content: picture, video, music

The digital home has turned into reality. As predicted by the Eurescom study P1401, flat screen and high-definition TV (HD-TV), broadband recording either on DVD or on hard-disk recorders, and the transformation from analogue to digital video and photography are the dominant events in 2006 [8]. The home broadband connection (e.g. ADSL) supports always online and enables on-demand services. Residential gateways are getting more mature, cheap, and offer innovative services in addition to communication. The social drives of a broadband, always-on connection are on-demand video and multimedia social connectivity. The home portal becomes the centre for communication, making people's content available in and outside the home and allowing for the control of the home infrastructure.

Even though video and TV recording are the current drivers, photo and music exchange are mature market services. Current upload/download network access rates support file exchanges (typical 1–3 Mb) and audio streaming (typically 128 kbit/s), while video exchange is still cumbersome. More advanced personal data recorders will support the streaming of video content in a mobile format, providing reasonable mobile video quality at data rates up to 384 kbit/s.

P1401 suggests to subdivide broadband home services into four categories; Entertainment, Home automation, Personal Enrichment and Social Inclusion [8]. This paper will concentrate on entertainment, providing electronic content like music, video and data while being on the move.

5.3 Mobile and broadband – a synergy

Section 3 has provided evidence for the fixed mobile integration, based on IMS or SIP standards. This paper goes beyond network access, and suggests the mobile phone becoming the identifier for home broadband services (see Figure 7).

Digital content in broadcasting is usually secured through a conditional access module (CAM), which requires a Smartcard to decrypt the incoming video streams. These systems, even though registered to a person, are used anonymously, as they stay in the set-top box. The mobile phone has the potential to allow a personalised access to broadband content by providing user information and preferences to the set-top box. This user information can either be provided

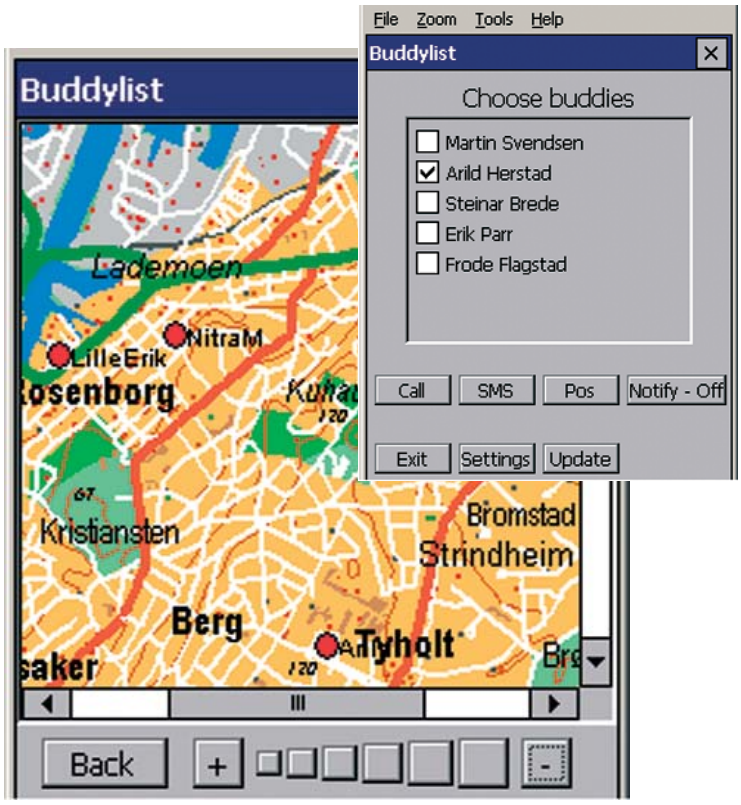

Figure 6 Community service, location of friends

through Near Field Communication (NFC), see Section 4, or through personal area network access based on e.g. Bluetooth or WLAN. Having established con-

Figure 7 Using the mobile to control and receive broadband services

nectivity and authentication, the user would be able to receive a personalised electronic programme guide (EPG), additional services through a locally forwarded channel or might even watch another channel or camera viewpoint on his personal device.

To provide a detailed overview of ongoing developments would exceed the scope of this paper. Lohse et al. provide a state-of-the-art discussion and suggest a network middleware solution, allowing mobile phones to control the digital video recorder, playing music stored in the home device, or chatting with visitors over the home located web cam [21]. The main challenge is to combine the broadcast and IP-world by introducing standards for interworking of authentication and DRM mechanisms in the virtual world.

6 Entering the digital world

Section 4 introduced seamless network and service access based on NFC, Bluetooth/WLAN, GSM/UMTS and WAP gateway authentication. Somogyi extended the seamless authentication to personalization of services for a picture gallery, using both user identity and device identity information [19]. Further work at UniK included access to various types of home content, including music download, web cam based surveillance and community address book.

6.1 Service examples

Internet services provide access to personal information through username/password authentication. On a mobile phone or a personal data assistant such a login procedure is not accepted by the customers, as input of text strings and passwords is too cumbersome. This section provides two examples of service access: Internet banking and access to a community data base (Figure 8). Both examples are based on WAP gateway authentication addressed in Section 5. The user is identified through his mobile number, and a provider specific md5 hash of the user id (MSISDN) is delivered to the service provider, here the bank. With this information the *nice to have* service account status and last transactions are provided to the user. For mobile transactions, a *need to have* service has to be provided in the form of a level 2 security, either through one time password or through PKI based authentication.

The second example provides access to a community database, where contact info is stored in specific databases, here a *Company* address list for companies the user has contact with a UniK list for all members at UniK. As compared to a public available database, such a community oriented database allows adding personal information which is only shared by members of the group.

6.2 Challenges/ongoing research

This paper concludes with access to encrypted home content from outside of the home, a typical OBAN case. The functional requirements are based on the following assumptions:

- Content will be available in a digital form, and content storage devices will be networked.
- The user will have a variety of devices which he can use for content access.
- A ubiquitous network allows content access wherever the user is.

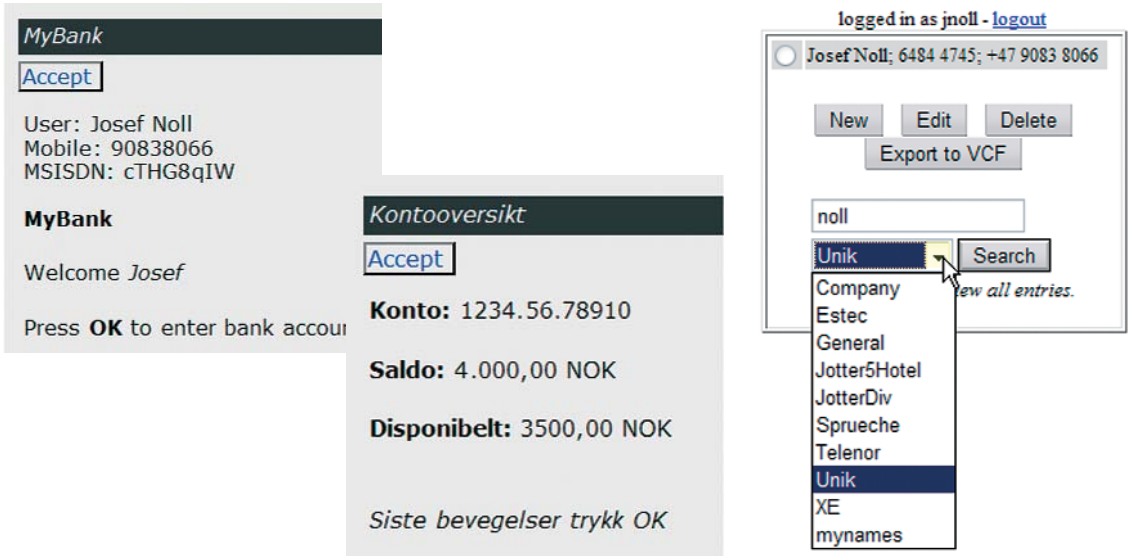

Figure 8 Seamless authentication, used for bank access (left) and community address book (right)

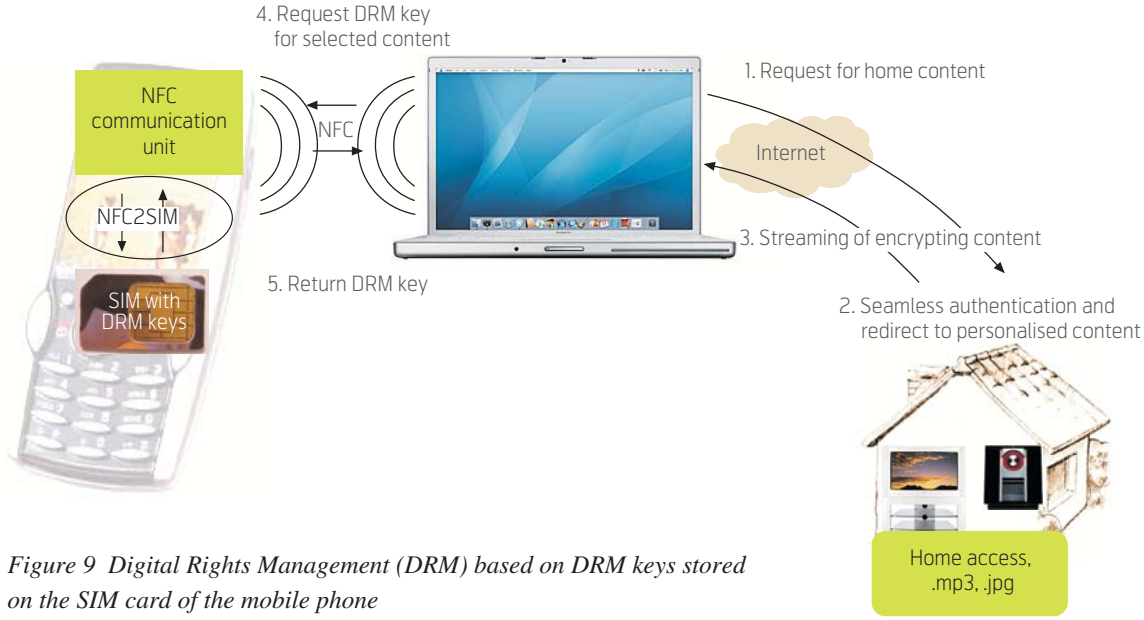

Figure 9 Digital Rights Management (DRM) based on DRM keys stored on the SIM card of the mobile phone

- The SIM card is the secure place to store identities and access rights.
- The user owns the SIM, and allows access/content providers to install access keys to the SIM. The SIM might be administered centrally, allowing for backup/update/restore functionality.
- Rights Management is delegated to the SIM. Content will be streamed to the device, and rights management checked against the access rights on the SIM.

Figure 9 represents the steps for content access fulfilling the functional requirements stated earlier. We have selected access to home content as example, following the argumentation provided by Noll et al. [8]. They claim that users will have a preference of having their content (music, video, pictures) at home, rather than storing them in the network.

The access to home content contains the following elements: The home content storage, the media player, the personal device and the network elements interconnecting the devices. The access is performed in the following steps [14]:

1 The user requests home content by addressing his home content storage.

2 The user device is authenticated in a seamless manner, and access to content is provided. Terminal capabilities are also transferred to the home content storage.

3 The content is adapted to the capabilities of the media player and network capacity, and streamed to the media player.

4 The media player asks for an authentication from the personal device, here indicated through an NFC interface.

5 The personal device returns an authentication, allowing for decryption of content in the media player.

Steps 1–3 are realised in prototypical implementations. Steps 4 and 5 are challenging, as they include NFC as communication medium, NFC2SIM as protocol for exchange of information between the NFC and the SIM card, and handling of DRM keys on the device in general.

The suggested NFC2SIM protocol has to secure the communication between the NFC module and the smartcard. Application keys like access or licensing keys are stored on the SIM, and are accessed through the NFC radio.

7 Conclusions

Service authentication has to satisfy the security requirements of the application, e.g. *nice to know* security for network access, *need to know* security for *e*mail and intranet access and *have to know* security for VPN and *m*Commerce services. Including authentication methods through Bluetooth and Near Field Communications (NFC), SIM-based authentication opens for all types of service access, providing admittance (keys, access cards, and tickets), payment (wal-

let) and content access (home). Examples of such services are mobile service access for banking, or ticket ordering, physical access based on proximity card functionality, VPN access based on *have to know* authentication, and *need to know* access to private home content. The SIM card in the mobile phone has the capability to provide a two-factor authentication, and supports mechanisms for revocation of credentials stored on the SIM card.

Authentication for network access is performed in the mobile network through the SIM card. In wireless networks such as the IEEE802.11 family authentication might be provided through various protocols, with the two SIM related protocols being the Extensible Authentication Protocol for Subscriber Identity (EAP-SIM) and the EAP for UMTS Authentication and Key Agreement (EAP-AKA). If a mobile phone supports EAP-SIM, it can seamlessly connect to WLAN networks using the SIM card. With the help of the Bluetooth SIM access profile (SAP), the SIM credentials can be transferred from one device (typically the mobile phone) to a second device (a laptop) for seamless WLAN network access of the user.

References

1 Annunziato, A, Jankovic, M, Odadzic, B, Noll, J, Buracchini, E, Melis, B, Harris, J. Guidelines for the Design of the UMTS Radio Access. *Proc. EURESCOM Summit 2001*, Heidelberg, Germany, 13–15 Nov 2001.

2 ITU-T Special Study Group: *IMT-2000 and beyond*. 10 August 2006 [online] – URL: http://www.itu.int/ITU-T/studygroups/ssg/

3 *The Wireless World Research Forum*. 10 August 2006 [online] – URL: http://www.wireless-world-research.org/

4 ITU-R Working Party 8F: *IMT-2000 and systems beyond IMT-2000*. http://www.itu.int/ITU-R/index.asp?category=study-groups&link=rwp8f&lang=en

5 Noll, J, Svaet, S (eds) et al. *4G – the next frontier: Perspectives for Research on Next Generation Mobile Systems*. Heidelberg, Eurescom, Sep 2001. (Project Report Eurescom P1145 study)

6 Stone, B. Your next computer. *Newsweek*, 7 June 2006. URL: http://www.msnbc.msn.com/id/5092826/site/newsweek/

7 Associated Press. *Era of mobile computing arrives – Notebooks have outsold desktops for first time*. 10 August 2006 [online] – URL: http://www.msnbc.msn.com/id/8090448

8 Noll, J, Ribeiro, V, Thorsteinsson, S E. Telecom perspective on Scenarios and Business in Home Services. *Proc. Eurescom Summit 2005*, Heidelberg, Germany, 27–29 April 2005, 249–257.

9 *A Prediction Made Real Improves Billions of Lives*. 10 August 2006 [online] – URL: http://www.intel.com/technology/silicon/mooreslaw/

10 *Nokia and Kineto Announce Collaboration in UMA technology*. 10 August 2006 [online] – URL: http://www.kinetowireless.com/news/press_releases/nokia.html

11 *Public Bluetooth Access – an opportunity for operators*. Eurescom P1118, Project deliverable D1, Nov 2001. (www.eurescom.de)

12 Kewney, G. BT 'BluePhone' is better than Skype because ...? *The Register*, 15 June 2005. (http://www.theregister.co.uk/2005/06/15/btfusion_launch/)

13 Valmot, O R. Finn veien med mobilen. *Teknisk Ukeblad*, 2 May 2006. (http://www.tu.no/nyheter/ikt/article52133.ece)

14 Noll, J, Carlsen, U, Kálmán, G. License transfer mechanisms through seamless SIM authentication. *Intern. Conf on Wireless Information Systems, Winsys 2006*, Setubal, Portugal, 7–10 August 2006.

15 Cameron, K. *The Laws of Identity*. http://www.identityblog.com/stories/2005/07/25/thelaws.txt

16 Kerstein, P L. *Biometrics ID devices are gaining popularity*. 10 August 2006 [online] – URL: http://www.csoonline.com/talkback/102505.html

17 Noll, J, Lopez Calvet, J C, Myksvoll, K. Admittance Services through Mobile Phone Short Messages. *Proceedings of the International Conference on Wireless and Mobile Communications ICWMC'06*, Bucharest, 29–31 July 2006.

18 Derenale, C, Martini, S. EAP-SIM based authentication mechanisms to open access networks. *Telektronikk*, 102 (3/4), 135–144, 2006. (This issue)

19 Somogyi, E. *Seamless access to structured home content*. Budapest University of Technology, January 2006. (Master thesis)

20 Ling, R, Yttri, B. Hyper-coordination via mobile phones in Norway. In: Katz, J, Aakhus, M. (eds.) *Perpetual contact: Mobile communication, private talk, public performance*. Cambridge, Cambridge University Press, 1999.

21 Lohse, M, Repplinger, M, Slusallek, P. Dynamic Media Routing in Multi-User Home Entertainment Systems. In: *Proceedings of The Eleventh International Conference on Distributed Multimedia Systems DMS'2005*, Banff, Canada, 5–7 September 2005.

Dr. Josef Noll is Prof.stip. at the University Graduate Centre at Kjeller (UniK), Norway, in the area of Mobile Systems. He is also Senior Advisor at Movation and at Telenor R&I. He received his PhD from the University of Bochum, Germany. He worked for the European Space Agency at ESTEC from 1991 to 1997, and from 1997 to 2005 at Telenor R&I. His working areas include mobile authentication, wireless broadband access, personalised services, mobile-fixed integration, and the evolution to 4G systems. Further information at http://jnoll.net.

email: Josef.Noll@unik.no