LICENSE TRANSFER MECHANISMS THROUGH SEAMLESS SIM AUTHENTICATION

Rights Management based on SIM Keys

Josef Noll, György Kálmán
University Graduate Center, UniK
Instituttveien 25, 2027 Kjeller, Norway

Ulf Carlsen
Agder University College
Grooseveien 36, 4898 Grimstad, Norway

Keywords: Content, access, license, user, SIM, home, NFC, DRM, device, network, authentication.

Abstract: Critical issues in the acceptance of wireless services are the authentication and authorisation to these services. This paper presents the SIM as device for 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 has the potential becoming the identity provider in the virtual/electronic world, enabling wireless network access, VPN and Mobile Commerce application access. The paper extends the seamless service access into the digital rights management, suggesting methods on how the rights keys can be managed on the SIM card, while content remains distributed on the customer devices. Final focus is on the requirements for future SIM cards in order to support the suggested methods.

1 INTRODUCTION

Authentication is the key for a customer relation, and the entry for value-added services. The mobile 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.

This paper applies not only to mobile networks, but service access in mobile, wireless and near field networks. Broadband penetration is expected to reach 60 % in certain European regions in 2007, and 80 % of those households will built this home network wireless (Noll, Ribeiro, & Thorsteinsson, 2005). The same paper suggests that centralized network storage will be a focal point in private homes. Together with the anticipated upstream capacity expected from future broadband access, e.g. ADSL 2+, this will lead to content usage at home and elsewhere. Initiatives like the EU's FP6 project OBAN enable access to home content, based on seamless network access in visiting wireless networks (OBAN, 2006). As the user will have her mobile phone around, we suggest to base both network access, service access and rights management on the SIM card of the mobile phone.

This paper will first justify why the mobile phone has the potential to serve as an identifier in the digital world. Having addressed the potential home services and service scenarios, the paper will provide an overview over current developments for network and service access. Developments addressing RFID/NFC and Bluetooth based authentications, and functionality in the mobile network through WAP gateway and Traffic Analyser. The final part of the paper will address rights management, based on near field, touch-based authentication.

2 SIM BASED SEAMLESS AUTHENTICATION

Access to content is based on the *possession* of the material, typically a CD, DVD or a device carrying the content. With faster access networks, digital

Carlsen U., Noll J. and Kálmán G. (2006).
LICENSE TRANSFER MECHANISMS THROUGH SEAMLESS SIM AUTHENTICATION - Rights Management based on SIM Keys.
In *Proceedings of the International Conference on Wireless Information Networks and Systems*, pages 333-338

content does not longer need to be carried around, only the access rights have to follow the user.

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

2.1 Security Demands

Depending on the content, access might be public, limited to a group or limited to a single user. Examples of public content are picture galleries. Group limited content might be address databases, private pictures or DVDs owned by the family. Single user content is typically confidential, being it access codes or eCommerce services.

The identification of the user should follow the requirements of the application. We suggest following the mechanisms suggested by the Initiative for open authentication (OATH, 2006), i.e. SIM authentication (*SIM*), Public Key Infrastructure (*PKI*), and One-Time-Password (*OTP*).

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.

2.2 Service Access

SIM authentication is already used 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, providing admittance (keys, access cards, and tickets), payment (wallet) and content access (home). Examples of such services are presented in figure 1.

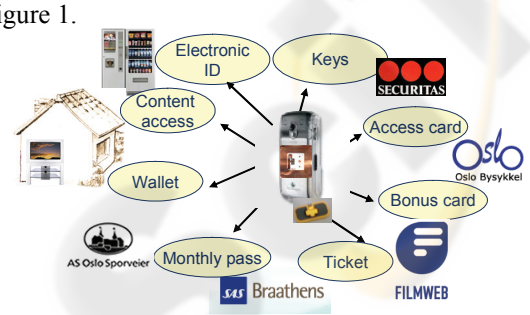

Figure 1: Examples of service access through SIM in near field, personal area, wireless and mobile networks.

2.3 Home Content Access

Somogyi (2006) extended the seamless authentication to personalisation of services. The WAP gateway (see figure 2) adds an information string to the http header, which is forwarded to the content server. The string contains both information

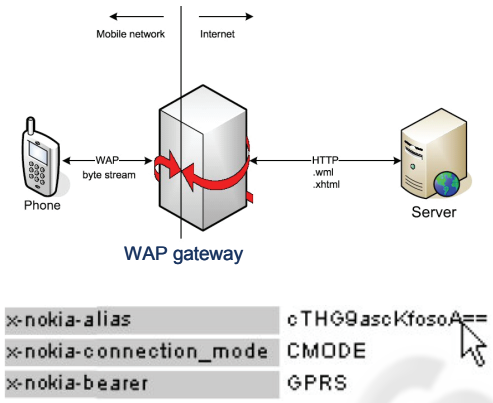

Figure 2: Mobile Network (WAP gateway) authentication with user and device identification.

on the user and the device requesting the service. The user (x-nokia-alias) is represented through a md5 hash of the mobile ID (MSISDN), and the device is represented through a device identifier (mobile phone type).

The seamless SIM based authentication was demonstrated for various types of home content: a photo gallery, music and community address book.

2.4 Touch Authentication Through NFC

Adding Near Field Communications (NFC, 2006) to the phone extends the capability of service access to proximity/vicinity based applications (see figure 1). Payment and admittance are two potential services enabled through NFC (Lopez Calvet, 2005). NFC is a specific RFID implementation, bringing the physical world and the electronic world together by help of radio frequency identification (RFID).

The established standard uses 13.56 MHz as an operating frequency, and incorporates the ISO/IEC standards 14443 for proximity card operations, ISO/IEC 15693 for vicinity card operations. This paper investigates in further details the split of radiofrequency (RF) and identification (ID). We suggest moving the ID into the SIM card, and leave the RF in the device (see figure 3).

Moving the ID handling into the SIM card provides various advantages for authentication and DRM management:

- Collection of security items (keys, admittance, identity) in one place makes the solution convenient for the user

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

The major challenge is the standardisation of the interface between the RF (= NFC communication unit) and the SIM card, indicated as NFC2SIM interface in figure 3. Standardisation of the interface is ongoing, but does not cover DRM handling yet.

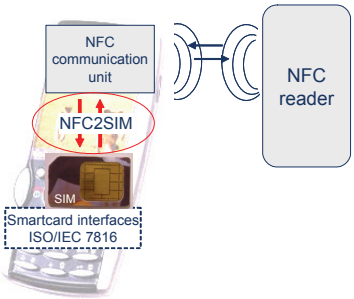

Figure 3: NFC communication with split functionality: RF in the device, and ID handling in the SIM card needs a new interface between NFC and SIM (NFC2SIM).

The following chapters suggest the functional architecture, and state requirements both for the interface and the SIM card.

3 NFC AND SIM BASED RIGHTS MANAGEMENT

This chapter describes rights management based on communication and security functionality of the NFC equipped mobile phone. It will first suggest a functional architecture for rights management, and will then postulate in detail the requirements for license transfer.

3.1 Functional Requirements

The functional requirements are based on the following assumptions:

- Content will be available in a digital form.
- A variety of devices will access content.
- A ubiquitous network allows content access wherever the user is.
- The SIM card is the secure place to store identities and access rights.
- The user owns the SIM, access/content providers will install access keys to the SIM.
- Rights Management is delegated to the SIM.

Figure 4 represents the steps for content access fulfilling the functional requirements stated earlier. We have selected access to home content as example, suggested by Noll, Ribeiro & Thorsteinsson (2005).

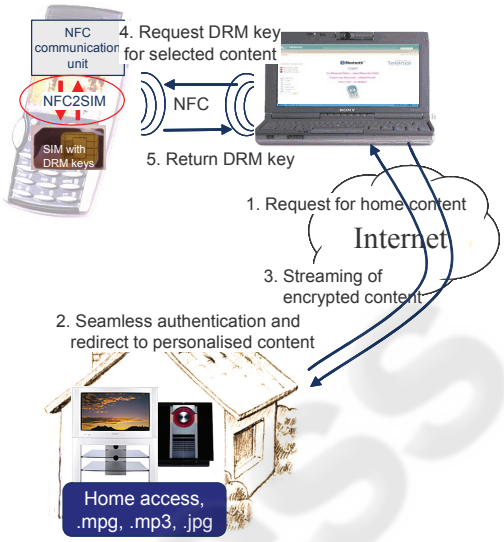

Figure 4: Functional scenario for SIM based DRM handling of home content.

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:

1. The user requests home content by addressing his home content storage.
2. The user device is authenticated in a seamless matter, and access to content is provided.
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 NFC.
5. The personal device provides authentication for decryption of content in the media player.

Steps 1-3 are realised in prototypical implementations (Somogyi, 2006). 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 following paragraph will address DRM specific issues in this solution.

3.2 DRM Specific Issues

This paper postulates the split of licensing keys and content in a DRM management system. Such a

solution will enable the user to carry his content rights wherever he goes, and allows content access both on all media players. It will be more convenient for the user, and enhance the acceptance for licensing. Typical application areas are:

- Usage of content on any media player able to handling the media format
- Purchase of licenses through mobile channels
- Distribution of gift licenses
- Permanent of time-limited transfer of licenses from one user to another
- Backup/update/restore of license keys

The following chapter will address license issues in DRM systems.

4 DIGITAL RIGHTS MANAGEMENT

The purpose of DRM (Digital Rights Management) systems is to ensure that digital objects and resources can only be accessed in an authorised manner. DRM enforces mandatory access control (Reid & Caelli, 2005) typically on a per-content basis, often extended with further limitations e.g. to allow access for a limited timeframe only or to a specific number of *views* or *runs*. RELs (Rights Expression Languages) such as OMA REL (OMA, 2006) and (XrML, 2001) are used to state these access conditions. The actual content is often cryptographically protected, with decryption keys and -attributes residing in the license. The license therefore also needs to be protected both during transfer and storage.

4.1 Mobile Licensing

Many DRM systems for mobile systems have been proposed over the years, including OMA DRM (OMA, 2006), Microsoft Windows Media DRM (WinDRM, 2006) and Apple's FairPlay system.

OMA DRM and Windows Media DRM keep REL-defined licenses separately from content. On the other hand, FairPlay incorporates licensing information into the music file itself. While self-protecting documents can be convenient and hassle-free from a distribution point-of-view (since the license is always present together with the document itself), maintaining licenses separately from the content ultimately provides a greater flexibility with regards to license updates, as licenses (if allowed by the policy) may be renewed or forwarded without also having to download the entire content once again.

4.2 License Backup

The ability to carry out data backup is a fundamental security requirement and principle. DRM systems limit the backup of licenses, as they prevent duplication of digital objects and/or their associated licenses/rights, thereby precluding individuals and organisations from implementing a proper backup policy. For example, if a license is locked to a specific device (i.e. node-locked) and this device becomes defect, obsolete or lost, then restoring/transferring the license to a new device may not be feasible. A backup restore operation to a different device (for a non node-locked license) could equally well constitute an illegal duplication of the license. Some licenses contain state information which changes as the licensed object is accessed. One such example is counter-based licenses which allow a certain number of views/executions of a licensed object. Since the backup copy of this license generally does not contain the most recent state information, a backup restore would cause this state information to be lost and therefore grant the user additional rights.

Ensuring compliancy between DRM solutions and ordinary data backup principles is an important but difficult challenge. If an object is split into a protected content part (the licensed object) and a license then the DRM system normally allows the licensed object to be freely copied, duplicated and backed up through any traditional techniques. There is no danger of misuse since the licensed object can only be accessed through its license. Such copying can also be viewed as proliferation of the content, and is supported by OMA DRM and Microsoft Media DRM. The challenge is in the license handling. OMA DRM allows licenses (which in their terminology are called Rights Objects) to be backed up and restored to the same device or to a device in a defined device domain, and also provided that the license does not contain dynamic state information. Windows Media DRM includes an option where licenses may be backed up and restored on a different computer (WinDRMF, 2006). Upon restore, a centralised fraud detection service hosted either by Microsoft or the content owner keeps track of the number of different computers/devices onto which the license has been restored. If a given threshold is reached the restore operation is aborted.

The FairPlay DRM model integrates the licensing information into the media itself. The system opens up for a fair amount of copying, allowing copying between any number of iPods and onto CDs. However, direct copying from iPods onto

other music players is prohibited. The DRM system proposed in (Messerges & Dabbish, 2003) allows copying of licenses within a defined family domain.

The backup/restore functionality of all these systems have several shortcomings. The threshold limit might through unfortunate circumstances be reached/exceeded, or it might for good reasons be set to zero (backup/restore is disabled) by a content owner who does not wish to open up for any possibility of potential illicit copying, e.g. because the content has a high commercial value. Forming and maintaining device domains will have an administrative cost and might be a hassle-factor for the user – and what will the rules be for allowing new devices into a domain? If a domain cannot be established and the device gets lost or becomes obsolete, restore can not take place. If the license contains stateful information, restore cannot take place either. In sum, there are still quite a few pitfalls which may hinder effective backup.

4.3 License Transfer

This section proposes a license transfer mechanism and protocol which meets some of the challenges pointed out above. It reconciles the apparent conflicting requirements for maintaining license backups while preventing license duplication.

Consider a single-user, unlimited license which we may label L. For simplicity we ignore the past, so the license will be valid from now and onwards, i.e. within the timeframe $[t_1, \text{unlimited}\rangle$, where t_1 denotes the current time.

The basic underlying idea is to consecutively subtract sub-licenses from L: Initially a new license L_1 is subtracted from L. L_1 is valid during an appropriately short time interval $\Delta t = t_2 - t_1$, i.e. during the timeframe $[t_1, t_2\rangle$. At the same time, the validity of L is reduced accordingly, and is now valid for the remaining timeframe $[t_2, \text{unlimited}\rangle$. License L is kept on an "online backup server". L_1 on the other hand is transferred securely via a piracy-proof channel (i.e. a channel which does not allow duplication or "double-spending" of the license L_1) to its destination device, for example the SIM card of a portable phone, where it is consumed. Once L_1 expires, or preferably a short time before, either the destination device requests a new license from the backup server (license pull), or the backup server automatically transmits a new license L_2 (license push). This license L_2 is, and subsequent licenses L_3, L_4, … are extracted from L in the same manner as L_1.

The same mechanism can be applied to other license types, e.g. to time-restricted licenses, where the license L now has a timeframe $[t_1, t_n]$ for two specific points in time (e.g. from 1.1. to 31.12.). A time-restricted license could also be a duration Δt (e.g. Δt = 30d) which is converted into a fixed timeframe $[t_1, t_n]$ upon first usage. For counter-based licenses, the counter (e.g. 100 views or runs) is split into multiple sub-counters (e.g. 10 x 10 views).

A cryptographic protocol which is suitable for secure and duplication-proof transfer of license from A to B is described in (Carlsen, Hammerstad & Gorancic, 2003). This protocol has the properties that the licensed is transferred no more than once to the rightful destination token, and may never be transferred to any other token.

The online backup server could be hosted by the vendor / content owner. It could also be a smart card which could then be located in the home domain indicated in figure 4. The sub-licenses are transferred to and stored on the mobile device SIM card. Now, if the mobile device SIM card is lost or corrupt the damage is reduced since only sub-licenses are stored here. Furthermore, the time interval Δt can be made small to minimise the consequences of a lost or corrupted SIM card.

4.4 Requirements for Future SIM Cards

The paper has demonstrated content rights management as a potential application for future SIM cards. SIM functionality is not limited to DRM, but can have a more general functionality, being the security infrastructure of the user in the digital world (Lopez Calvet, 2005). The basic requirement for such functionality is that the SIM can act on behalf of the user, supporting different roles and functionalities. This includes 3rd party security applications, e.g. keys for admittance to buildings, authorisation to banks and other legal entities.

We suggest using a hierarchical structure, where the SIM has a master identity module (see figure 5), which controls the secrets.

Such an identity module might be administrated by a legal entity, e.g. a network operator, a bank, or the state. It can then allow administrate secret keys for other applications, e.g. update, backup, restore. We see this functionality happen over a secure channel over the air, and indicated the functionality by over the air application (OAA).

Admittance and license management are two items which will require clock (CLK) functionality,

as admittance or licenses might only be given for certain time intervals.

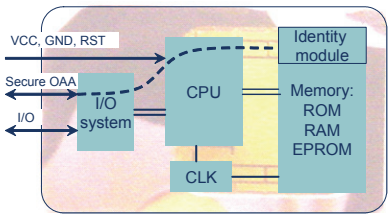

Figure 5: Requirements for future SIM cards: Secure over the air applications (OAA) and identity handling of SIM card, as well as clock (CLK) functionality for a.o. DRM handling.

5 CONCLUSIONS

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. The paper extends the seamless access into the digital rights management, suggestion methods on how the rights key can be managed the SIM card, while content is distributed on the customer devices.

This paper suggests basing both network access, service access and rights management on the SIM card of the mobile phone. With faster access networks, digital content does not longer need to be carried around, only the access rights have to follow the user. The scenario used in this paper is the access to home content, which contains the following elements: The home content storage, the media player, the personal device and the network elements interconnecting the devices.

NFC is introduced to exchange information including NFC as communication medium, and NFC2SIM as protocol for exchange of information between the NFC and the SIM card. Application keys like access or licensing keys are stored on the SIM, and are accessed through the NFC radio. While current DRM systems implement and enforce mandatory access control for a limited number of devices, our solution suggests letting license keys to be handled from a central user device, allowing every media player to play the content. This solution provides a greater flexibility with regards to license updates, as licenses (if allowed by the policy) may be renewed or forwarded without also having to download the entire content once again.

This paper argues that current DRM licensing techniques are less suitable especially for higher-value assets where the demand for proper backup technology and mechanisms will be required. A license transfer mechanism and protocol which meets the requirement for backup is proposed. The technique reconciles the apparent conflicting requirements for maintaining license backups while still preventing license duplication.

REFERENCES

Carlsen, U., Hammerstad, H. & Gorancic, E., Process for Compiling and Executing Software Applications in a Multi-Processor Environment, patent app. NO-20045687, May 2003, http://v3.espacenet.com/textdoc?DB=EPODOC&IDX=WO2004003861&F=0

Fairplay, Available at: http://en.wikipedia.org/wiki/FairPlay

Lopez Calvet, J.C., 2005. The role of RFID in the mobile phone, *Telektronikk 3/4.2005,* pp. 131-142

NFC – The Near Field Communication Forum, 2006, Available at: http://www.nfc-forum.org/

Messerges, T.S. & Dabbish, E.A., Digital Rights management in a 3G Mobile Phone and Beyond, DRM 2003, ACM Transactions.

Noll, J., Lopez Calvet, J.C., Myksvoll, K., Admittance Service through Mobile Phone Short Messages, *Proc. ICWMC 2006*, Bucharest, 28.7-3.8.2006

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

OATH – Initiative for open authentication, 2006, Available at: http://www.openauthentication.org/

OBAN – Open Broadband Access Networks, EU FP6 project, 2006, Available at: http://www.telenor.no/fou/prosjekter/oban/

OMA DRM Architecture, Version 2.0, March 2006. Available at: http://www.openmobilealliance.org/release_program/drm_v2_0.html

Reid, J.F. & Caelli, W.J., DRM, Trusted Computing and Operating System Architecture, Australasian Information Security Workshop, 2005

Somogyi, E, 2006. Seamless access to structured home content. *Masterthesis Budapest University of Technology,* Jan 2006

Windows Media DRM 10 for Devices, Sept. 2004, at: http://go.microsoft.com/fwlink/?linkid=40518

XrML – eXtensible rights Markup Language, 2001, Available at: http://www.xrml.org/