Security for Ambient Wireless Services

György Kálmán[1], Mohammad M. R. Chowdhury[1], Josef Noll[1,2]
[1]UniK, University Graduate Center, Kjeller, Norway
[2]Telenor R&I, Fornebu, Norway
{gyorgy, mohammad, josef}@unik.no

***Abstract*— Service delivery in the wireless world needs to provide a personalized and secure service access. This paper extends the security architecture of the mobile network into the service delivery. Personalized and secure service access is ensured through preferences and certificates, compiled in a *P*ersonal, *C*orporate and *S*ocial *ID*entity (*PID, CID, SID*). Specific service examples for doctors and patients in a hospital are used to prove the concept for admittance to areas and access to confidential information.**

***Index Terms*— nfc, identity, security, ambient, hospital, health-care, monitoring**

I. Introduction

When moving to service delivery in the wireless world, the user is confronted with lots of challenges, two of them being personalization and secure service delivery. Personalization of services includes adaptation to the user context and preferences. Secure service delivery needs to ensure an appropriate security mechanism, providing a convenient service access. Mobile customers are used to hassle-free access and services (GSM works everywhere), and will expect the same functionality in an ambient network environment. This paper extends the security architecture of the mobile network into the service delivery, taking into account preferences of the user and security requirements of the service.

The paper focuses on a hospital scenario, and takes the roles and preferences of doctors and patients as starting points for service delivery. The first part uses a scenario description (sect. II) to introduce the service requirements in terms of role based identity, privacy, and security. After a short state-of-the-art review, the paper will then introduce an identity concept (sect. V) allowing for personalized service provision. Our identity concepts covers *soft* issues like preferences, e.g. membership of social groups, as well as *hard* issues like certificates, used both in a corporate environment and as a personal identifier. We postulate that a role based identity can be composed of a subset of a personal, corporate and social identity. Personalized service access will happen through a *role based identity*, where a combination of certificates and preferences is used to identify the user towards the service provider.

The second part of the paper deals with specific service implementations for the hospital scenario (sect. VI), especially for services which *medium* and *high* security requirements like admittance and journal access. The service examples will show how standard infrastructure needs to be extended with an identity provisioning service to support personalized service interaction.

II. Service scenario

As an example for a secured ambient wireless service, we show a scenario in a hospital. We have two main actors, the doctor and the patient. In this environment, identities are handled through certificates and preferences, stored in a distributed environment including network and the mobile terminal. Based on roles, the hospital can offer intelligent call routing, forwarding incoming phone calls automatically to the doctor in charge. An indoor localization service enables a personalized information distribution to the screens in the operation room depending on the position of the roles of the doctors. It also opens for location-dependent alerts and messages. The doctor can access patient data by identifying himself through the mobile phone. Also, admittance is based on the phone equipped with near-field communication (NFC) capabilities.

When a patient is registered in the hospital, he gains access to new services and also faces some restrictions. This can be handled for example with an NFC enabled phone, where the credentials can be uploaded, thus opening for personalized service exchange between the patient and the hospital. This can enable hospitals to provide a more convenient service. The mobile phone acts as an identity provider and holds user credentials in the SIM's secure storage.

III. State of the art

NFC is prototyped as a solution for contactless payment or user authentication, like Deutsche Bahn's Handy Ticket [1] solution or the ticketing pilot project at Rhein-Main Verkehrsbund in Hanau [2].

Secure service provisioning is a.o. provided by the Trusted Computing Group (TCG) [3], supporting a trusted platform both for PCś and other mobile devices. This proposed architecture enables service providers to ensure the integrity of the system, but does not support user preferences and personalization of devices.

To enable wireless communication with health-care devices, such as heart monitors, these devices need to be extended by the appropriate wireless interface. These include ease of use and battery lifetime. A limited number of wireless sensors using Bluetooth are available in the health-care market, e.g. Memscap's wireless blood pressure sensor [4]. New radio interfaces as ZigBee [5] might overcome some shortcomings by providing higher battery lifetime, but ZigBee devices have not reached the medical market yet.

As suggested in [6], NFC technology could be a solution for low power data exchange for very short range transmissions. Also pairing of devices can be done with just one touch, which can replace the cumbersome pairing process of Bluetooth and lower the connection buildup time from some 10 seconds to a second or less. The major problem with using purely NFC is its very limited range.

In the following, we suggest to use NFC technology as a solution for proximity services and an identifier for service access, based on keys stored in the device.

IV. Identity and Security

People interact with many service providers to play numerous roles in life. As the service scenario described depending on the contexts and preferences, doctors and patients exercises relevant roles to receive their necessary services. Most of these interactions demands privacy and security. Identity is formed out these roles and ensures the services received by legitimate owner.

A. Role based identity

Analyzing every possible scenario in life, it can be said that every human being plays roles basically in three different areas, personal, professional and social areas. To carry out these roles, an individual needs to present identifications to others that represent his/her identity in this world. Instead of using numerous physical identities and usernames/passwords, a unique identity mechanism is expected to be developed in the digital realm where individuals would be able to control and manage their various digital identities, assigning the appropriate attributes to each according to their context. In our service scenario, the patient has a role as someone suffering from some kind of sickness. He/she requires specific identity based on severity of sickness, location of treatment (home or hospital), preferences etc. In case of admission into hospital, social security number of the patient may represent his/her identity. A role based identity mechanism can ideally represent individuals identity depending on contexts.

Role based identity can be divided into *my personal identity (PID)*, *my corporate identity (CID)* and *my social identity (SID)* [7]. My personal identity can be used to identify ourselves in our personal and commercial interactions. Similarly, My corporate identity and My social identity can be used in our professional and interpersonal interactions respectively. Each of these three identities will have several identifiers. Each identifier will be used to access several relevant services and a number of attributes will characterize an identifier.

B. Identity for doctors and patients

Here we will describe how we can relate PID, CID and SID to doctors and patients in proposed service scenario. For the patients, PID will possess the identifiers to deal with social services or government facilities (e.g. social security number) and to access financial services for payment. PID also contains and control patients admittance right to hospital areas and access to his/her medical information. SID will have my community information or contacts, calendar, address book etc. Patients interests, fondness, preferences or tastes are also dealt with by SID. For the doctors, CID will contain those identifiers to access hospital premises and databases. Doctors can access patients current medical records, past medical histories, patients previous visits, test results etc. from databases using CID. PID of a doctor may contain his/her social security number, professional registration number as a doctor etc. There might be some other identifiers useful for doctors to exercise roles as physicians.

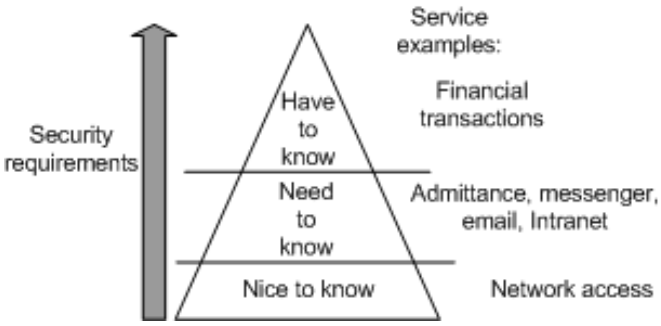


Fig. 1. Security infrastructure based on security requirements.

C. My digital identity

M. Choudhery proposed the concept of my digital identity, an identity repository [7]. Role based identity is a subset of my digital identity. Every roles based identity to interact with different services available in the digital world will be composed of components stored in the repository, my digital identity. It contains personal (PID), corporate (CID) and social (SID) identities to identify and authenticate the owner to various personal, corporate and social services. My digital identity will be placed party in the network environment and party in personal terminal. The personal terminal allows seamless identification to my digital identity. In addition to this, it will contain identity to interact those services that demand very stringent security requirements. For higher security assurance, we need a combination of knowledge and possession based authentication components [8]. The possession based component might be the SIM card in the personal terminal. Certificate handling in the SIM card is available through wireless interfaces. The knowledge based component might be a PIN code provided through the phone key pad. The mobile phone can be the proposed personal terminal. Three levels of security: *nice to know*, *need to know*, *have to know* have been introduced in [8] (see figure 1). As soon as the owner authenticates to the mobile phone, he/she can access the network as well as access my digital identity, own identity repository.

In addition to this, user can access community information or contacts, address book, calendar etc. in SID. These are *nice to know* services that require minimum security requirements. Another layer of security might be provided using extra PIN code to access *need to know* services, for example, admittance, access to messenger services, IP telephony and home/corporate VPN or databases etc. The highest security requirements

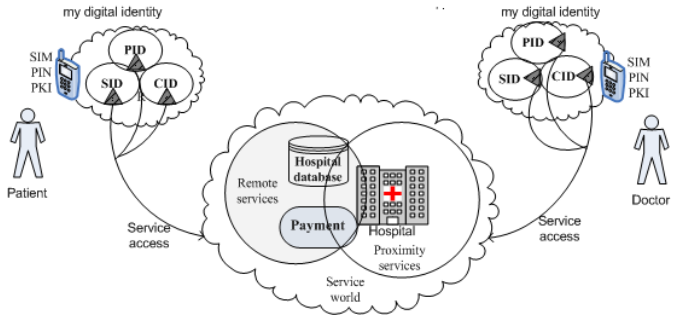
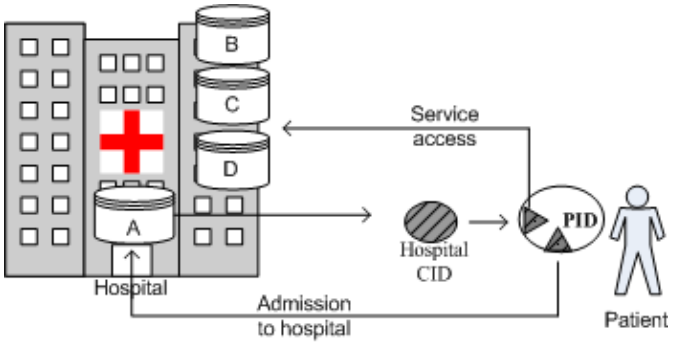


Fig. 2. Service world and service access



A: Admittance control
B: Access rooms
C: TV, newspaper, entertainment etc.
D: Food, special diet

Fig. 3. Service example: patient gets admitted into hospital

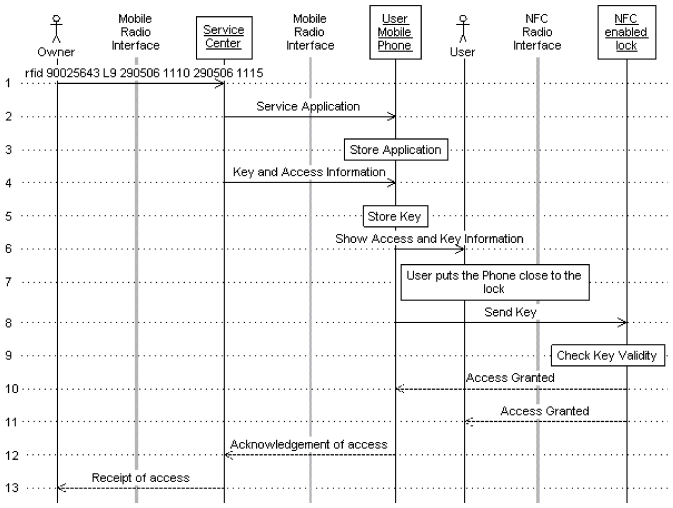


Fig. 4. NFC based admittance with the mobile phone

are required for *have to know* services. SIM card will hold those identifiers to access *have to know* payment services, for example, credit card, net bank etc. This might be realized by implementing for example, public key infrastructure (PKI) on the SIM cards, as introduced by Norwegian Banks in association with Telenor AS [9]. If necessary, SIM credentials can be transferred to PCs using Bluetooth, infrared or NFC to access my digital identity from computers.

V. Service Architecture for Secure Personalized Services

A. Hospital services using identity repository

Doctors and patients have such an identity repository supporting their roles. Fig 2 shows a generic diagram illustrating services and service access architecture in a hospital scenario. Depending on the context, a specific *role based identity* is composed from the components of my digital identity for services access to local (proximity) and remote (web) type of services. Examples of remote services are real-time telemonitoring of patient data; automatic uploading of real-time physiological data to databases in the hospital; access of medical histories, test results, up-to-date prescriptions, diet and exercise lists prescribed; automatic call to doctor; medical payment services etc. Examples of proximity services are admittance to hospital premises, payment services, and identification for journal access.

Depending on the location of patients and doctors, remote and proximity services are available to them. When patients and doctors are in the hospital, remote services and relevant identity and identifiers may no longer be required. Through remote services, monitoring and observation functionalities are available, regardless of the actual location of the the medical personnel. We suggest hospitals having their own CID, which is provided to the patient during the period of stay in hospital (fig. 3). It will be used together with the patients PID to access various hospital services.

The patient will use appropriate identifiers of his/her PID, CID and SID to access remote and proximity services. Doctor will use appropriate identifier of CID or PID to access both remote and proximity services. As described in [7], my digital identity has the capability to ensure secure identity handling and minimal disclosure of identity information. For a patient, secure and reliable medical data handling is extremely important, as it secures the data and enhances the privacy of the patients. It also brings convenience to doctors and patients allowing them to use different equipment (PDA, mobile phone, PC) to access/interact services using the specific identities required for that service. Figure 4 provides the details of admission for a patient as an example of a proximity service,

1) Patient gets admitted into hospital through PID (may be social security number) from his/her my digital identity.
2) Identity is verified by hospital. Hospital then allocates a hospital CID to patient for the period of stay.
3) Hospital CID will be stored in patients PID which includes
   a) the admittance key to access rooms
   b) access to personalized services like, TV, newspaper, entertainment.

B. SIM based identity management

This paper will concentrate on the secure access service access, mainly supported by the PID. We suggest using the mobile phone as an identity provider and the SIM card as secure storage for PID values. It provides wide encryption capabilities: e. g. Public Key Infrastructure (PKI), One Time

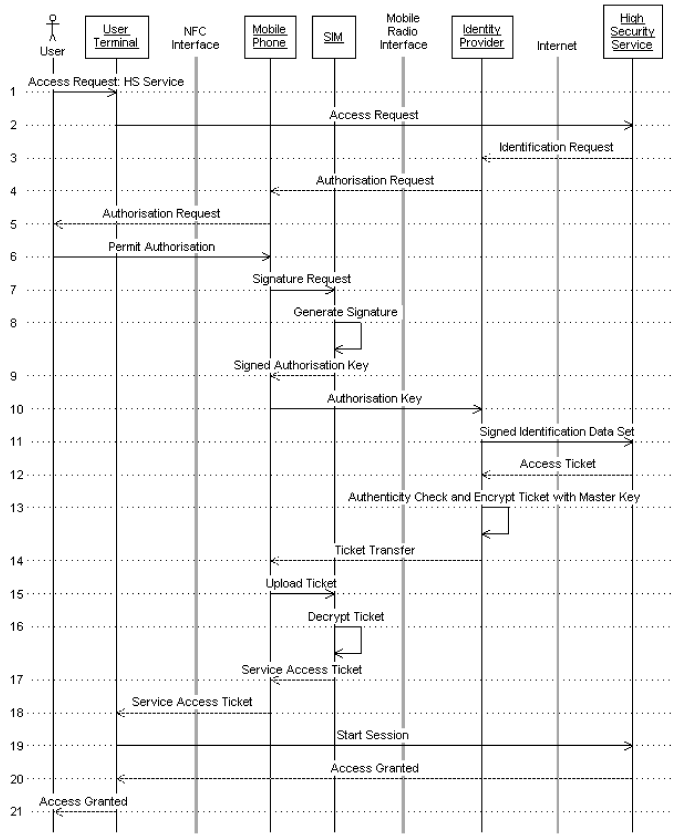


Fig. 5. Authentication for a service with high security requirements

Password (OTP) or the normal SIM authentication, recommended by the Open AuTHentication initiative (OATH) [10], and accepted by most European governments as required technologies for digital signatures. As stated in [11], the current GSM network is able to provide secure enough encryption for the most applications. By extending the current infrastructure, e.g. through usage of the Extensible Authentication Protocol for GSM Subscriber Identity (EAP-SIM), the SIM card can supply basic authentication services for mobile health-care. Preshared keys can be used for seamless user authentication. Using NFC it is possible to build an admittance system, enabling personalization services or instrument access.

In applications with higher security demands the basic authentication services should be extended by an additional identification through e.g. a challenge-response authentication procedure (see fig. 5).

C. SIM as identity provider

Moving the ID handling into the SIM card provides various advantages for authentication. Collection of security items (keys, admittance, identity) in one place make the solution convenient for the user, as it enables

- replacement of the user devices without losing credentials,
- advanced protection for misuse, as the SIM can be disabled remotely,
- strong encryption capabilities,
- secure storage.

When the mobile phone/SIM card [12] acts as an identifier for the user in the wireless service world, the secure distribution of keys is of vital importance. We suggest NFC for key transfer, where security requirements are taken into account through the short range of near-field communication and the capability of user interaction when key transfer is taking place.

The key actor in the system is the identity (ID) provider. This actor has to keep trusted relationships with all service providers (or the possibility to build trusted relationship through relaying identity providers).

D. NFC in the mobile phone

NFC adds intelligence and networking capabilities to the phone and creates many new opportunities to add product and service capabilities to the handset like digital transactions and sharing in very close proximity.

Through the mobile phone, the user has full control over the identification process either based on the location e.g. putting the phone close to the reader or on knowledge e.g. typing in a PIN when requested by the remote service, thus minimizing the possibility of eavesdropping and unwanted key exchanges.

A key problem is the correct selection of the identifier to be used in a transaction. This can be done by selecting correct identities. These identities are composed by one or more identifiers. If one of the identifiers gets compromised, it can be revoked by the identity provider and the user can get a new key without losing access to the services. The remote revocation and user control makes the SIM an ideal device for making payments and gaining access to services. The integrated NFC transmitter can be used for key exchange, mutual identification and limited data transfer.

After exchanging encryption keys via NFC, the system also needs a secure storage. The SIM has an integrated secure storage, which enables storing keys in a place which isnt accessible from outside. To ensure secure transfer of new service keys, the identity provider may install a secret master key to the SIM at its activation. New keys can be encoded with this master key inside the operators network and then transferred to the unit. The data will be protected against eavesdropping and man-in-the-middle attacks, since only the receiving SIM card will be able to decrypt it.

Decryption can be done by SIM internal routines, which can access the master key and store the new service key into the protected storage. As such, the key is encrypted until it reaches the secure storage.

For service access, the system can use a challenge-response authentication, so the key wont be transmitted or even read out from the card. To enable fast key access, we suggest to build a b-tree in the memory of the handset from hash values generated by SIM internal routines. This enables to give a hard limit of access delay maximum of $log_n k$ where n is the number of leaves per node and k is the number of keys currently installed.

VI. Proof-of-concept

A technological solution for the health-care service scenario includes:

Medical data gathering

The patient gets equipped with wireless sensors. These sensors are paired with the data collection unit or the patient's mobile phone through NFC by just bringing the sensor and the unit close together. Pairing the sensors with the mobile phone enables mobility of the patient and supports data transmission over longer ranges.

An example might be a permanent heart rate monitor, a blood pressure sensor or a blood sugar tester [4]. The sensor data are transmitted to the mobile phone, which forwards them to doctor or the hospital's data center.

Secure data transmission

During the pairing process, encryption keys are exchanged between the devices. When initiating data transmission, the sensors and the phone authenticates themselves with the shared keys. So, or example, the sensor initiates a Bluetooth connection with the phone, and secures the channel with the preshared key. The system uses the default encryption of the bearer technologies just in the initiation process, and secures all data with the additional key. The data transmission between the hospitals computer and the mobile phone is then secured with the additional key.

Admittance control

Admittance control can be performed through the mobile phone. Noll demonstrated admittance control through NFC equipped mobile phones, including distribution of admittance keys through mobile messages [8]. This concept can be applied for patients, allowing access to certain parts of the hospital and to doctors for almost unlimited access to all areas. It also supports visitors for one-time access to an area, being a visiting room or a waiting area for an examination. The access restrictions are built up on the CID of the user, thus enabling to define generic access rules for different groups.

Authenticated service access

Patient data require high protection, thus a person requiring the data needs to identify himself through an authentication based on *possession* and *knowledge*. Our solution uses the mobile phone as *possession* element, and a pin code for the additional knowledge-based authentication. Such a service has similar security requirements as a BankID, which is expected to be available in 2008 [9].

Authenticated service access of the patient depends on the CID provided to him by the hospital. He might be able to change time of appointments, request a meeting or cancel one. Fig. 6 provides the sequence diagram for authenticated service access.

When he is registered for a stay in the hospital, a set of new services will be enabled, including selection of food preferences, access to recreational facilities, and access to communication networks.

VII. Conclusions

This paper provided a concept for personalized and secured service access, and applied the concept to services in a hospital. The suggested service architecture extends the security of the mobile network into a security for personalized service delivery. Personalization is achieved using a subset

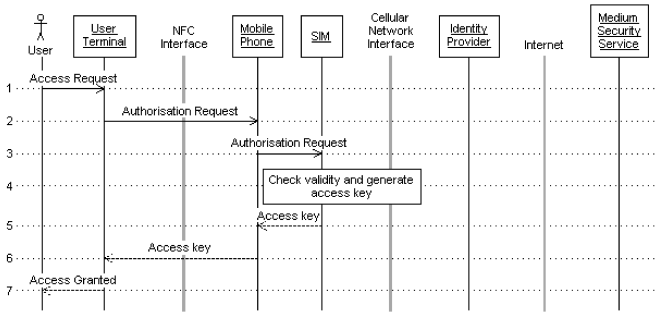


Fig. 6. Authentication with keys stored in the SIM's secure storage

of identities from a *P*ersonal, *C*orporate and *S*ocial *ID*entity (*PID, CID, SID*). The items in the identities are expressed through certificates and preferences, depending on the privacy and security demands. The paper suggests to use a distributed architecture, where items with high privacy demands like social identity number or payment card information are stored in the SIM card of the mobile phone, whereas items with lower privacy demands like food preferences are stored in the network.

Specific service examples for doctors and patients in a hospital are used to prove the concept for admittance to areas and access to confidential information. Secure information like access keys are stored in the SIM card of the mobile phone, and can be accessed either through near field communication (NFC), through Bluetooth and WLAN, or through the mobile network. An example of such a usage is the distribution of encryption keys through NFC, allowing for encrypted traffic in a WLAN network based on keys stored in the mobile phone. The service examples show how standard infrastructure (network based certificates) can be used together with an advanced mobile phone (NFC phone) to deliver health-care services cost-effective, while providing an appropriate security.

References

[1] Deutsche Bahn AG, "Handy ticket," 2006. [Online]. Available: http://www.bahn.de/handy-ticket

[2] Rhein-Main-Verkehrsbund, "get in." [Online]. Available: http://www.rmvplus.de/

[3] TCG Mobile Phone Working Group, "Use case scenarios v2.7," 2005.

[4] Memscap AS, "Wireless health and care." [Online]. Available: http://www.wshc.no/demo_ instrumentation.php

[5] Z. Alliance, "Zigbee specification." [Online]. Available: http://www.zigbee.org

[6] J. P. A. Y.-o. I. K. Esko Strmmer, Jouni Kaartinen, "Application of near field communication for health monitoring in daily life," in *IEEE EMBS*, 2006.

[7] J. N. Chowdhury M. M. Rahman, "Service interaction through role based identity," in *Proceedings of WWRF 17*, 2006.

[8] K. M. Josef Noll, Juan Carlos Lopez Calvet, "Admittance services through mobile phone short messages," in *Proceedings of the International Conference on Wireless and Mobile Communications ICWMC06*, 2006.

[9] "Telenor and the banking industry launch bankid for mobile phones." [Online]. Available: http://press.telenor.com/PR/200610/1078768_ 5.html

[10] "Open authentication initiative." [Online]. Available: http://www.openauthentication.org

[11] D. D. van Thanh et al, "Offering sim strong authentication to internet services," in *Whitepaper, 3GSM World Congress*, 2006.

[12] Gy. Kálmán and J. Noll, "SIM as a key of user identification: enabling seamless user identity management in communication networks," in *WWRF 17*, 2006.