IADIS International Journal on Computer Science and Information Systems
Vol. 2, No. 2, pp. 51-64
ISSN: 1646-3692

INTEGRATED IDENTITY MECHANISM FOR UBIQUITOUS SERVICE ACCESS

Mohammad M. R. Chowdhury *UniK – University Graduate Center, P.O. Box 70, N-2007 Kjeller, Norway.*

mohammad@unik.no

Josef Noll *UniK – University Graduate Center, P.O. Box 70, N-2007 Kjeller, Norway.*

Josef@unik.no

ABSTRACT

Ubiquitous access and pervasive computing enable innovative services and provide the service access in every situation. People currently rely on numerous forms of identities to access remote or proximity services. The inconvenience of possessing and using these identities creates significant security vulnerability. This paper proposes an architecture that integrates the identities required to access various remote and proximity services. In the mechanism, identities are distributed into the user's personal device and a secure network space. Third party identity providers along with the mobile network provide the underlying secure infrastructure for identity information exchange. In this regard, the use of multi-factor authentication contexts meets different levels of service access security requirements. At the end, a prototypical implementation demonstrates a service access scenario based on the proposed mechanism.

KEYWORDS

Identity management, remote service, proximity service, security, SIM

1. INTRODUCTION

Now-a-days, fixed and wireless broadband networks are not the only means to access diverse web services. Ubiquitous access and pervasive computing enable the service access in every situation. The mobile network can provide sufficient capacity for real time data communication. The deployment of state-of-the-art technology in core networks is allowing fixed and mobile services to be seamlessly mixed. In addition to the remote (web) services, introduction of near field communication (NFC) at usage in mobile phones can enable many new proximity services [19]. All these significant developments in network and service capabilities can boost innovative service creations and interaction.

User identity handling will play a vital role for accessing diverse services. Now-a-days, service access in Internet is burdened with many user names and passwords. Reuse of these is frequent and unsafe. Service providers also use substantial efforts issuing and managing identities to the users. Gartner predicted in its annual IT security summit 2005, 80% of organizations will reach a password breaking point by 2007 [7]. Numerous physical identities are used to identify its owner to various services. Now-a-days, people increasingly use smart cards with electronic chip for service access and payment. It enhances the security and allows storage of user details on the card. To meet additional security requirements, the possession factor of physical/online identities is often enhanced by a knowledge factor, a PIN code. If there are several of these, the users tend to compromise security by writing down their PIN codes. It is evident that the current forms of identities are inconvenient to use and manage both for the users and service providers. Therefore, the service access scenarios demand a new form of identity management.

An integrated identity mechanism is suggested in this paper to overcome the deficiencies of current password identification. The proposed solution is expected to integrate the identities required to access both the remote and proximity services into a single mechanism. The identities are distributed into the user’s personal device and a secure network space. Third party identity providers along with the mobile networks provide the underlying security infrastructure for identity information exchange. The proposed mechanism has the potential to eliminate not only the numerous usernames and passwords but also the use of various physical identities. In addition to user’s convenience, such identity mechanism might also be useful for other stakeholders like, identity providers, service/application providers, and equipment vendors.

Section 2 presents the related work in this area. The following section illustrates the nature of ubiquitous services and the challenges in this area. The proposed identity mechanism and the service access demonstration based on the mechanism are discussed in section 4 and 5. Section 6 states the benefits of the stakeholders involved in the proposed identity mechanism and the paper concludes with section 7.

2. RELATED WORK

Managing identities is crucial for the development of the next generation of distributed applications and services. Ubiquitous access, sufficient bandwidth by mobile networks and capabilities of the future SIM card can bring many new services to the user. Identity handling should also consider the utilization of the strengths of the mobile environments. Numerous research works are going on in various institutes and industries to provide better identity management solutions. In one approach, Altman and Sampath propose a user-centric network identity management framework [1]. The paper suggests a unifying identity solution to integrate the multiple user credentials currently stored independently by the service providers. The authors only concentrate on the identity management issues over the Internet. In another solution, He and Zhang present a framework for identity management in a distributed environment [13]. It supports secure and convenient access to web-based applications and services. Most of the research concentrates on managing user identities over the Internet [2],

[3], [21], [22]. However, some of the initiatives also consider the capabilities and challenges of mobile environments in identity management [14], [15], [22]. It is to be noted that user identities include not only the username/password/PIN codes for accessing remote service but also many physical identities to access many proximity services. All these efforts lack solutions for handling the physical identities.

There are significant initiatives from the ICT industries to provide real life solutions in this area. In Liberty Alliance [16], members are working to build open standard-based specifications for federated identity and interoperability in multiple federations, thereby foster the usage of identity-based web services. Within this, they are focusing on end user privacy and confidentiality issues and solutions against identity theft. Some of these solutions incorporated mobile communication technology. Another solution, Sxip [24] has been designed to address the Internet-scalable and user-centric identity architecture. It provides user identifications, authentications and internet form fill solutions using web interfaces for storing user identity, attribute profiles and facilitating automatic exchange of identity data over the Internet. To access online services, Windows CardSpace [26] uses various virtual cards (mimic physical cards) issued by the identity providers for user identifications and authentications, each retrieving identity data from an identity provider in a secure manner.

Banking industry of Norway with a partnership of a mobile operator initiated BankID [5] for identification and signing agreement on the move. BankID for mobile phones will initially be used in four areas: logging on to Internet banks, mobile banking, electronic service for business and the public sector, and account-based payment service for internet and mobiles. Gemalto [11] provides online and offline identity management and security solutions based on smart cards with associated software, middleware and server-based solutions. NXP [20] is also offering identification products in areas like government, banking, and access control using secure innovative contactless smart cards and chips. MasterCard uses NFC-enabled mobile phone for a customer trial in Dallas, Texas for touch and go payment with the MasterCard PayPass [9]. The main focus of these initiative is towards the identity management in Internet domain (remote services), but some of the solutions also target services located in the proximity of users. For ubiquitous service access, the big challenge will be to integrate these scattered user’s identities into a single mechanism. The proposed integrated identity management mechanism is expected to address this challenge. The mechanism engages the SIM card as storage place for identities and uses the mobile network as secure underlying infrastructure for key distribution.

3. UBIQUITOUS SERVICE WORLD

Now-a-days people can access services from anywhere and any time, whenever it is necessary. Ubiquitous access and pervasive computing make these possible. The section will address the nature of the two types of services, remote services and proximity services.

3.1 Remote services

The introduction of state-of-the-art ubiquitous networks offers sufficient capacity, QoS and interoperability and allows the users to interact with numerous services remotely. Social communications (exchanging messages, voice, photos, videos), online shopping, reservation and banking, remote home or office network access are few examples of remote services. Fixed-mobile convergence [10] and thereby seamless user experience can boost such service creations and intake by users. These services are currently accessed through the Internet using different authentication mechanisms. This form of identification and authentication can be termed as *'something you know'* (knowledge based) and sometimes *'something you have'* (possession based) [25]. Users have to register prior to first usage and publish private information, often more than what is strictly necessary for service access. The access is often granted through username, password or PIN. Having usernames/passwords is an example of *some you know* and possessing a smart card to generate one-time-password (OTP) is an instance of *something you have*. Figure 1 gives a generic diagram for ubiquitous service access. It illustrates the notion of remote and proximity service access.

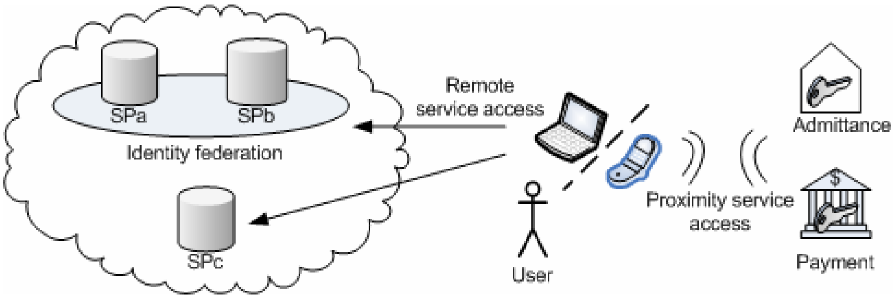

Figure 1. A generic diagram for ubiquitous service access.

3.2 Proximity services

The second group of services happens in close proximity of users. These services are accessed through physical interactions with physical cards or devices, e.g. payment cards and admittance cards. This form of identification can be said as *'something you have'*. Depending on the security requirements of the services, the possession based authentication might be enhanced by a knowledge factor (e.g. PIN code) add on. The devices/ cards and PIN codes are issued to the users when registered for relevant services. The introduction of NFC technology makes the transfer of user's information from one device to another possible. This will obviously boost the intake of proximity services.

In the ubiquitous service world, the border between remote services and proximity services is not strict. Proximity services like NFC may initiate remote services like ticket ordering for cinema tickets [19].

3.3 Challenges in wireless service oriented architecture (SOA)

Service Oriented Architecture (SOA) is an architectural style where functionalities and applications are packaged as services. Some of the requirements for efficient use of a SOA are seamless interoperability between different networks and systems, clear and unambiguous service description in a platform-independent fashion and high quality retrieval of services. Fixed and fixed wireless networks have capabilities to support requirements of SOA provisions. In this regard, wireless networks and devices have hardware and software limitations. Therefore, it is important to mention the challenges of wireless SOA provisions when wireless networks are considered as the driving force in ubiquitous service access. The following table points out some of these challenges compared to fixed SOA.

Table 1. Challenges in wireless SOA provision.

	fixed SOA	**Wireless**
SOAP protocol	- always online, - fixed internal delay < 50 ms	- bad radio, packet loss, retransmission round-trip-delay mobile up to 1.2 s - cost of air-time
Number of messages	- practically “no” limitations (not important in fixed networks)	- cost of air-time
Service repository	- UDDI[1], always available	- context and location dependent services - no reliable services due to bad radio, packet loss and service termination
Service support	- resources available	- limited CPU & battery power - specialised OS - device optimised for limited resource usage
Semantic support	- increased computing resources	- services optimised for device/OS, not for interoperability - limited support for semantic SOA

4. INTEGRATED IDENTITY MECHANISM

The ubiquitous service world and deficiencies of current forms of identities demand an integrated mechanism of managing user’s identities. The proposed integrated identity mechanism consists of certificates, keys and preferences. These identities are categorized broadly into personal identity (PID), corporate identity (CID) and social identity (SID) based on the roles exercised by a person in real life [6]. PID can be used to identify ourselves in our very personal and commercial interactions. CID and SID can be used in our professional and social interactions respectively.

4.1 The concepts and elements

The elements consist of identity providers (IDP), user’s personal devices and underlying mobile network infrastructure for identity service subscriptions, storage of identities and transmission of identity information with service providers and other IDPs.

[1] UDDI, Universal Description, Discovery, and Integration, is a platform-independent, XML-based registry for business worldwide to make them available on the Internet.

4.1.1 The role of identity providers

The role of an identity provider is very crucial in ID provisioning. Identity providers may come from user's social, corporate or personal domain. Figure 2 illustrates user's ID provisioning. Security requirements of ID provisioning from these domains depend on the relevant service access security demands. State/government is the traditional and most accepted identity provider in national and international level providing citizen ID. With strong regulations in place, banks and mobile operators can also act as an IDP. Having a state or citizen ID is obligatory to establish access to some of these services. These belong to high security environments and therefore the roles of these IDPs are strictly regulated.

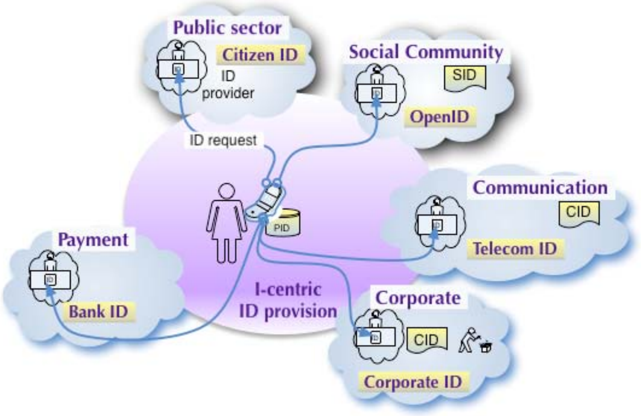

Figure 2. User's identity provisioning.

Similar to the subscription of voice and data services, access to identity services subjects to explicit agreement between users and identity providers. An IDP is maintaining strong trust relationships among the subscribers, service providers and the other IDPs. The proposed mechanism makes use of the mobile network along with phone and SIM card as the secure infrastructure for storing and exchanging identity information. There are reasons why we think the existing mobile network infrastructure is ideal for identity services like user authentication and consent such as,

- Mobile network's global acceptability, interoperability and reach.
- The security of 3G mobile systems has been strengthened by introducing longer cipher key, mutual (network, user) authentication, signaling and data traffic integrity and extension of ciphering back into the network [4].
- In addition to Bluetooth and Infrared, introduction of NFC makes the proximity service more accessible.

Introduction of mobile communication technology as a mean to provide identity service also brings new challenges, for example,

- Minimizing the consequences of mobile terminal's loss or theft.
- Restoration of user's ongoing session, dropped due to poor and erratic RF signal quality.
- Usability problems in terms of handling and user interface, especially referring to complex transactions.

- Requirements from emerging number-portability legislation are making interoperability even more complicated and more critical.

4.1.2 Distributed identities

With the identity services subscription, IDP issues a certificate to the user and allocates a secure identity space in the network. User identity data and attributes are distributed and stored into two places. A part of the user identities that contain very sensitive user information like, $\text{PID}_{\text{Bank/Creditcard}}$, $\text{PID}_{\text{Home admittance}}$ will be stored (permanently or temporarily) in the SIM card of mobile phone. Therefore, access to these requires strict authentication. Another part of user identities which need low authentication requirements, for example social identities and preferences (SID), will be stored into the secure identity space in the network. Table 1 gives several examples of PIDs, CIDs and SIDs, their possible realizations and where these identities will be located or stored. Considering the various levels of security, the corresponding security requirement of each identity is also mentioned.

Table 2. Identity types, realizations, storage, and security requirements.

Identity	Examples	Realization	Location	Security requirement
PID	PID (Bank/Creditcard)	Certificate + key (private + public)	SIM	High
	PID (Home admittance)	Home entry key		
CID	CID (Office admittance)	Office entry key	SIM	High
	CID (Other admittance)	Temp. entry keys	Network	Medium
	CID profiles	foaf/OWL		
SID	Preferences	foaf/OWL	Network	Low
	Attributes	foaf/OWL		Medium

During the subscription, an operator can load the SIM card with a private key for the user. Besides, $\text{PID}_{\text{Bank/Creditcard}}$ credentials are realized through certificates and keys provided from the Banks. These can also be stored in the SIM card. The trusted third party (whoever it is) can mediate the whole process. There are few possibilities of $\text{PID}_{\text{Home admittance}}$ realization. Admittance keys can directly be stored in binary format in the SIM card or a hash can be generated from the stored private key and hash algorithm. The keys or a hash can later be transferred to other devices using NFC technology. CID and SID profiles and preferences are realized using either FOAF[2] (friend of a friend) or OWL[3] (Web Ontology Language) and stored these foaf/owl files in the network. We think Semantic Web Technology (foaf/OWL) can provide solutions to access control and privacy in corporate and social environment by defining roles of user, access control and privacy policies and rules. We have already implemented several ontologies in OWL representing identity handling, access control and privacy support in corporate and social scenarios in a separate work [8]. Detail descriptions of these mechanisms are beyond the scope of this paper.

[2] FOAF, http://www.foaf-project.org/

[3] OWL, http://www.w3.org/TR/owl-features/

The SIM card is considered as storage place because it can be revoked, user now-a-days can rarely be found without a mobile phone and there are possibilities of further security enhancements in it. High capacity SIM cards are available in the industry with increased memory size, additional cryptographic and high speed communication (SIM-handset, SIM-network) capabilities [27]. Handling identities from the SIM gives the user control over the usage of his identities. Figure 2 depicts a user-centric (i-centric) vision of ID provisioning. The proposed mechanism is expecting that IDPs do not own or control SIM card rather act as facilitators to manage identities. To manage multiple credentials, IDPs can load additional IDs confidentially to either a SIM card (with over-the-air provisioning) or at network identity space with user's consent. In case of loosing the SIM card, a new one can be ordered and the identities previously stored in the card can be reloaded.

With the identity subscription certificate user can identify himself to access the network identity repository that contains identities for example SIDs. These identities will be used to access services that need medium or low level of security requirements. The SIM card holds only the most sensitive user identities. As an online network is vulnerable to many security threats, only information of less sensitive character are stored in the network.

4.1.3 Ubiquitous service access

To make the remote service access hassle-free, the concept of Circle of Trust (COT) developed by Liberty Alliance can be employed [7]. For remote service access, user can have single sign-on (SSO) functionality to move seamlessly between federated service/content/identity providers using a single SIM card credential (or identity subscription certificate) without entering numerous usernames and passwords. This is how a federated identity domain can be realized (figure 1). The identity subscription certificate issued by an IDP is not enough to access services that need additional security requirements. PIDs/CIDs stored in the SIM card have to be used to meet such requirements. Besides the mobile environment, services can also be accessed from PC when identity subscription certificate (issued by IDP) and user's PID/CID/SIDs are available from PC.

The introduction of NFC technology adds intelligence and networking capabilities to the phone and creates many new opportunities to add product and service capabilities to handset like digital transactions in very good proximities. It can make a mobile phone an ideal device for payments and gaining access [17], [18]. This is more promising when the mobile is considered as the preferred device in the proposed mechanism for certificate and key handling. Besides, less sensitive admittance keys can be stored at network identity space, and when required, can be downloaded temporarily to the SIM card memory. To access proximity services, the identity information stored in SIM card (permanently or temporarily) can be transmitted through the NFC interface. The channel between two NFC devices can be secured using available cryptographic protocols [12].

4.2 Authentication mechanisms

This section discusses about the authentication mechanisms for the proposed integrated identity architecture. The mechanism is supported by multiple levels of authentication, and SIM based certificate and key handling provisions.

4.2.1 Multi-factor authentication

Different levels of authentication mechanisms need to be maintained depending on service access security requirements. From user point of view, a securely maintained communication channel is required to exchange very sensitive user information with the service provider. There are services that require only little information about the user. Highly secured infrastructure is not a necessity for them. Besides, building or maintaining very secure channel requires good investment as well. Therefore, different levels of security should be employed for different types of services. Analyzing all these aspects, [17] introduced three levels of security: *Nice to know*, *need to know*, *have to know* (see figure 3).

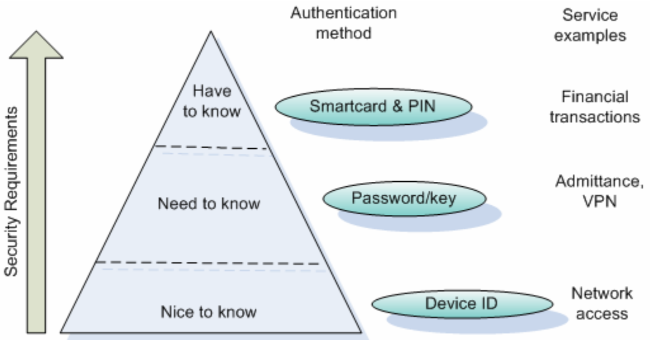

Figure 3. Security infrastructure based on security requirements.

Nice to know services are for example, network access, where knowledge about usage is only required in case of misuse of the network. *Need to know* services like Intranet or VPN access, admittance have higher security requirements. Highest security requirements have to be met for *have to know* services, such as credit card or bank transactions.

As the SIM card is proposed to contain most sensitive user identities and also allows the owner access to his/her network identity space, an extra protective measure should be employed for accessing SIM to make PIDs more secure. To address this, an extended SIM (ESIM) is proposed which is a customized variant of USIM (Universal Subscriber Identity Module). It has two modules: one is responsible for operator service access and access to network identity space. The other part contains the highly sensitive personal identities with protection through additional PIN code. Therefore, the solution has several layers of security provisions. *Something you have* which is a smart card (ESIM) gives low level of security, and *something you know*, a knowledge based ones (PIN codes) provide medium or high level of security.

4.2.2 SIM based certificate and key handling

SIM with PKI is proposed to solve the security problems. PKI enables the parties in a dialogue to establish confidentiality, message integrity and user authentications without having to exchange any secret information in advance. In cryptography, it is an arrangement that binds public keys with respective user identities by means of a certificate authority (CA). Users then can use public key information in their public key certificates to encrypt messages to each other. User can select the key provided by the Bank (and Credit card) to make online financial transactions. For other services, if necessary the users can utilize the key from the home operator. Banks and mobile operators can work as certificate authority respectively. The later is crucial when the user is under roaming. In this case, the visited operator can negotiate with the home operator for authenticating the users. BankID partnership [5] is an example in this regard where it provides user a public key infrastructure (PKI) built in SIM card for identification and signing the agreement.

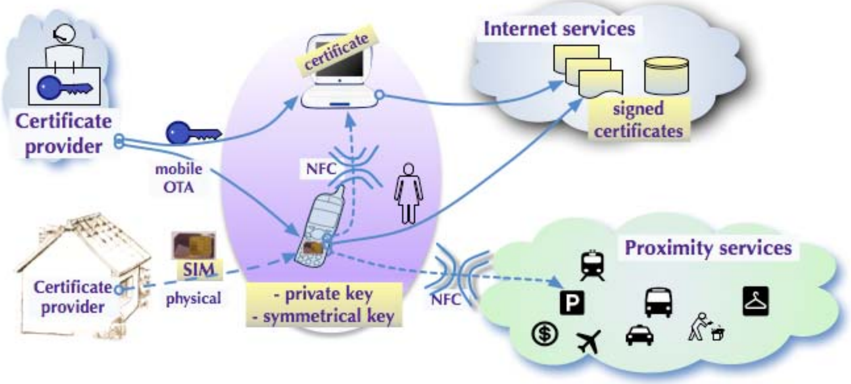

Figure 4. SIM based certificate and key handling.

Figure 4 illustrates SIM based certificate and key handling provisions. Certificates can be provided to the mobile phone either physically or through mobile over-the-air[4] (OTA) provisioning. It is possible to sign the certificate/transactions using stored private key from the mobile phone or PC. These signed certificate/transactions will provide authentication, integrity and non-repudiation services during service interactions.

5. SERVICE ACCESS DEMONSTRATION

A mobile based key exchange and thereby service access demonstrator was built based on an earlier implementation of NFC-based admittance keys [17]. The key generation and distribution was modified to support online access to contents of a service provider (SP). The authentication provider generates key upon request and transmit to the user through mobile phone system. The key is stored in integrated smartcard and transmitted on demand to the mobile terminal. The terminal can itself access services based on that key or, as demonstrated, can be used to perform user identification, where higher security is required. In our service example, the key is transmitted over the NFC interface towards SP.

User wants to access contents remotely from a service provider from the PC. Figure 5 illustrates the steps of service access demonstration. In step 1, the access request is sent to SP. Triggered by the request, in step 2, access control system of the provider sends a message to the authentication provider. This entity transmits access information and an access key to the mobile phone of user. We assume that Service and authentication provider belong to a common trust system and user’s mobile phone number is sent to SP during service access request.

[4] Over-the-air (OTA) is a standard for the transmission and reception of application-related information in wireless communication systems.

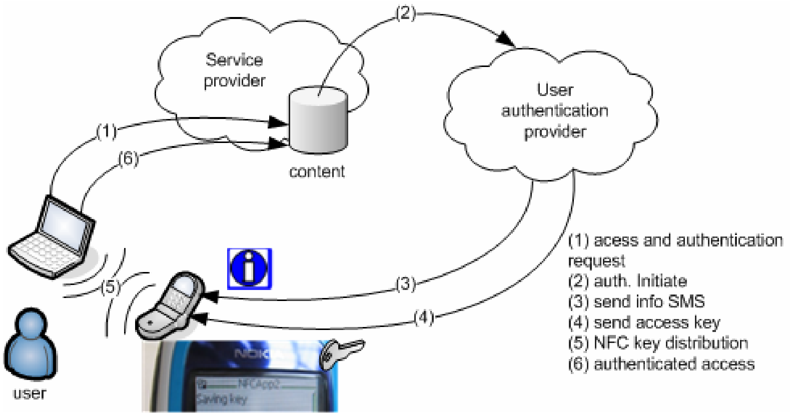

Figure 5. Prototype of key exchange for online content access.

The key is stored in the integrated SmartMX card of the phone and can be transmitted over the NFC interface. In step 5, the key is transmitted over NFC to the PC, which is used to access selected contents. Our implementation uses Telenor's mobile network through PATS[5] Innovation lab. The user authentication provider (service centre) creates an information message (3) and a binary key (4), which is transmitted to the user's phone (here Nokia 3320) and stored in the SmartMX card of the NFC unit. NFC-based connection to the PC transmits the admittance key and authenticates (6) access to contents.

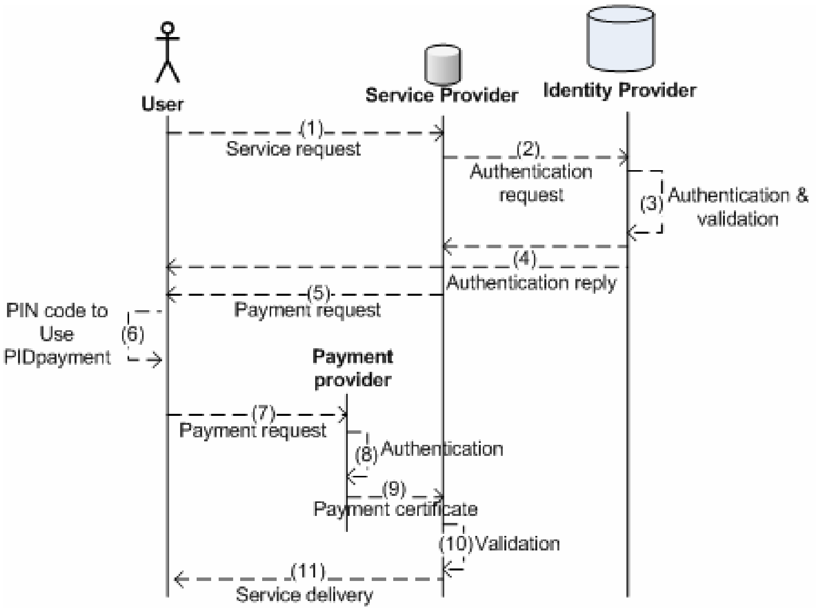

Figure 6. User requests a service that requires $\text{PID}_{\text{payment}}$.

[5] PATS Lab, http://www.pats.no/

The above prototypical implementation provides a *need to know* authentication using a key/password. Now we are going to describe a service access scenario which requires financial transactions. Figure 6 illustrates the corresponding sequence of messages. In step 1, uses requests for a service. The message contains the user certificate provided by the IDP during identity subscription. SP then forwards this certificate with its own one and asks the IDP for authenticating the user. In next step, IDP authenticates the user and SP (using their certificates) and returns reply to both so that user and SP can check each other's validity. SP then sends payment request to user (step 7). User then applies the PIN code to initiate a payment request using $PID_{payment}$ stored in the SIM. In step 9, a payment certificate is sent to SP when the request is authenticated (step 8). Upon validation, SP delivers the services. It is to be noted that the procedure avoids providing payment information directly to SP. Instead using $PID_{payment}$, a payment certificate is generated which confirms the payment to SP. It further enhances the security avoiding disclosure of payment information to SP. These service access demonstrations depict the use of proposed integrated identity mechanism for accessing various types of services in a secure manner.

6. STAKEHOLDER'S BENEFITS

Users, identity providers, service/application providers and equipment vendors every associated entity can be benefited through the proposed integrated identity mechanism.

User is benefited through easy-to-use and mobility in service interactions at a lower cost. With strong security mechanism in place by the underlying infrastructure, the proposed identity mechanism can ensure more secure service access. Single sign-on (SSO) through the use of COT allows users to move seamlessly without entering numerous user names and passwords [16]. Use of NFC makes this identity mechanism more accessible to new proximity services. Finally, hassle-free service access is a main feature of this mechanism.

Revenues can be generated through providing identity services including user authentication and consent, and infrastructure sharing, including SIM, with other identity providers (when operators choose not to be the identity providers because of trust). Mobile/wireless operators can extract value from their infrastructure investment with the increase in data traffic over their licensed airwaves and expansion of their brand's reach. The identity service provision positions the mobile network as a preferred channel for trusted services.

Service provider benefits generally derive from a lower cost-of-business and more service intake by users. User is motivated to use more services as integrated identity mechanism provides, hassle-free usage, security, ease of use and availability. Use of identity provider services for user's authentication lowers the cost of business (by not maintaining an individual authentication mechanism), integration efforts and accelerates time-to-market.

Mobile vendors, including network infrastructure, devices and platform, and smart card/chip vendors benefit from an increased demand for standardized, higher-end devices and interfaces. User demand for identity-enabled services accelerates device renewal. Higher demand leads to volume savings in production cost. Multi-functional and easy to use terminals increase user experience and brand loyalty.

7. CONCLUSION

The paper introduces an integrated mechanism for identity provision that facilitates both remote service and proximity service access. It addresses the concerns that user can no longer cope with the current identity usage scenarios. The proposed mechanism suggests the storage of user identities in a distributed manner. A customized SIM card is proposed that stores most sensitive user identities. Less sensitive ones are stored at a secure user identity space in the network. Multiple factors of authentication mechanisms are employed to address different levels of security requirements. The paper also demonstrates service access architectures using the proposed identity mechanism. The use of such an integrated identity concept can benefit the application/service industries, infrastructure vendors and above all, the users. Nevertheless, there are few challenges such as the role of home certificate authority internationally, certificate revocation and limitations of mobile environments. In our future work, we will focus on these challenges and will extend the work further to develop a complex use case on seamless user experience in heterogeneous wireless networks when the user is roaming.

ACKNOWLEDGEMENT

The contribution is a part of an ongoing research in WP2 of SWACOM project, funded by The Research Council of Norway. The authors would like to acknowledge the contributions and supports provided by their colleagues from UniK, Kjeller and Telenor R&I, Fornebu, Norway.

REFERENCES

[1] Altmann, J. and Sampath, R., 2006, UNIQuE: A User-Centric Framework for Network Identity Management, *Network Operations and Management Symposium, NOMS 2006,* Vancouver, Canada, pp. 495-506.

[2] Buell, D. and Samdhu, R., 2003, Identity Management, *IEEE Internet Computing,* Vol. 7, No. 6, pp. 26-28.

[3] Berthold, O. and Kӧhntopp, M., 2001, Identity Management Based on P3P, *Designing Privacy Enhancing Technologies: International Workshop on Design Issues in Anonymity and Unobservability,* Springer Berlin / Heidelberg, pp. 141-160.

[4] Boman, K. et al., 2002, UMTS security, *Electronics and Communication Engineering Journal,* Volume 14, Issue 5, pp. 191-204.

[5] BankID: Delivering Bank-common Trust for Web-based Transactions, https://www.cybertrust.com/intelligence/case_studies/ [Accessed on April 2, 2007]

[6] Chowdhury, M. M. R. and Noll, J., 2006, Service Interaction through Role based Identity, *Proceedings of Wireless World Research Forum Meeting 17*, Heidelberg, Germany.

[7] Chowdhury, M. M. R. and Noll, J., 2007, Distributed Identity for Secure Service Interaction, P*roceedings of the Third International Conference on Wireless and Mobile Communications, ICWMC07,* Gaudeloupe, French Caribbean.

[8] Chowdhury, M. M. R. et al., Enabling Access Control and Privacy through Ontology, to be published in proceeding of the 4th International Conference on Innovations in Information Technology, Innovations'07, Nov 18-20, Dubai.

[9] Cellular-news, “MasterCard Tests NFC Payments with Nokia Handsets”, http://www.cellular-news.com/story/20211.php [Accessed on April 2, 2007]

[10] Fixed-Mobile Convergence Alliance, http://www.thefmca.com/ [Accessed on November 5, 2007]

[11] Gemalto, a digital security company, http://www.gemalto.com/ [Accessed on November 5, 2007]

[12] Haselsteiner, E. and Breitfuss, K., 2006, Security in Near Field Communication (NFC) Strengths and Weaknesses, *Workshop on RFID Security - RFIDSec 06*, Graz, Austria.

[13] He, J. and Zhang, R., 2005, Towards Formal Framework for Distributed Identity Management, *Web Technologies Research and Development – APWeb 2005,* Springer Berlin / Heidelberg, pp. 913-924.

[14] Hoffmann, M., 2004, User-centric Identity Management in Open Mobile Environments, *Privacy, Security and Trust within the Context of Pervasive Computing,* Springer Netherlands, pp. 99-104.

[15] Jøsang, A. et al., 2007, Usability and Privacy in Identity Management Architectures, *Proceedings of the Australian Information Security Workshop (AISW’07),* Victoria, Australia.

[16] Liberty Alliance Project, http://www.projectliberty.org/ [Accessed on November 5, 2007]

[17] Noll, J. et al., 2006, Admittance services through mobile phone short messages, *Proceedings of the International Conference on Wireless and Mobile Communications ICWMC’06*, Bucharest, Romania.

[18] Noll, J. et al., 2006, License transfer mechanisms through seamless SIM authentication, *International Conference on Wireless Information Systems, Winsys 2006*, Setubal, Portugal.

[19] NFC forum, http://www.nfc-forum.org/ [Accessed on November 5, 2007]

[20] NXP Semiconductors, http://www.nxp.com/ [Accessed on November 5, 2007]

[21] Poursalidis, V. and Nikolaou, C., 2006, A New User-Centric Identity Management Infrastructure for Federated Systems, *Trust and Privacy in Digital Business*, Springer Berlin / Heidelberg, pp. 11-20.

[22] Siddiqi, J. et al., 2006, Secure ICT Services for Mobile and Wireless Communications: A Federated Global Identity Management Framework, *Proceedings of the Third International Conference on Information Technology: New Generations (ITNG’06)*, Nevada, USA, pp. 351-357.

[23] Shin, D. et al., 2004, Information Assurance in Federated Identity Management: Experimentations and Issues, *Web Information Systems – WISE 2004*, Springer Berlin / Heidelberg, pp. 78-89.

[24] Sxip Identity, http://www.sxip.org/ [Accessed on November 5, 2007]

[25] Two-factor authentication, http://en.wikipedia.org/wiki/Strong_authentication [Accessed on November 5, 2007]

[26] Windows CardSpace, http://cardspace.netfx3.com/ [Accessed on November 5, 2007]

[27] White paper: High Capacity SIMs, http://visionmobile.com/whitepapers.html [Accessed on November 1, 2007]