COMMUNITY BASED SERVICE ACCESS

Josef Noll and Mohammad M. R. Chowdhury
University Graduate Center, UniK
Kjeller, Norway
josef.noll@unik.no, mohammad@unik.no

ABSTRACT
Ubiquitous computing and the pervasive Internet have enabled service access in every situation. However, adaptation to the user needs is purely handled, and service specific security implementations are only found for specific services. This paper presents an approach to combine the I-centric and service centric world based on a semantic description of user preferences and user relations connecting to proximity and remote services. Based on personal, corporate and social identities security requirements are defined for handling the service access. A prototype using over-the-air key distribution demonstrates the capabilities of the suggested approach.

KEYWORDS
i-centric, user-centric, SOA, profiles, personalisation, GSM

1 Introduction

Current developments in service delivery have the focus in two areas: *(i)* Mobile Service Delivery and *(ii)* Semantic Service Delivery. Current reporting from The World Factbook states 1.5 to two times as many mobile users as Internet users for developed countries like UK, France and Germany and roughly three times as many mobile users as Internet users in China [1]. Taking into account that mobile users are available 24 h/7 days a week as compared to an average PC usage of just above 2 h/day[1] shows the importance of mobile service access [2].

Mobile service provision is hampered from the limited interface capabilities of a mobile phone, thus needs to perform service personalisation, including adaptation to personal preferences, terminal and network capabilities. This is one of the key challenges for mobile operators [3], and subject of current activities in the Wireless World Research Forum. The forum has initiated an I-centric service architecture [4], which puts the communication behaviour of human being in the frequent interactions with objects in their environment.

Machine understandable Web and Web Services are the goals of developments in Semantic Web and Semantic Web Services [5]. Semantic Web is seen as the next generation of the Internet where information has machine-readable and machine-understandable semantics. Semantic Web Service implementations are seen as an extension of the Service Oriented Architecture (SOA), allowing a.o. for automatic service composition.

This paper presents an approach to combine the I-centric and service centric world based on a semantic description of user preferences and user relations connecting to

[1] 137.3 minutes/day for male users and 134.2 minutes/day for female users

proximity and remote services. It explains the principles of the I-centric and service centric world in sect. 2, with a focus on service delivery in mobile/wireless environments. It then introduces in sect. 3 an identity architecture, covering private, corporate and social identities. Based on the privacy requirements of a user in a certain context, it will then in sect. 4 provide a concept and a prototypical implementation, followed by the conclusions.

2 I-centric versus service centric approach

This section will focus on the commonalities and differences in a user-centric (or I-centric) and service centric approach. The difference between both approaches is historical, where a service centric architecture was introduced to let services communicate with each other. The I-centric approach, postulated by the Wireless World Research Forum (WWRF), is based on the transition of access delivery to service delivery [3]. Current rule-based algorithms become too complex when handling user context and preferences, thus asking for new mechanisms allowing dynamic adaptability of services. The service centric world was introduced based on service level agreements (SLA) between trusted partners. In a more dynamic service provisioning world, as envisaged in a Semantic Web Services environment, privacy and security become key issues [6]. Our approach is to take advantage of developments in both worlds, using the security and privacy mechanisms of the I-centric world and combine them with the semantic representation of data as known from the Semantic Web (Services) World.

2.1 I-centric vision

Access provision was the key issue in first and second generation mobile networks (1G, 2G-networks), while service provisioning is key in 3G and Beyond-3G networks. "Systems beyond 3G" will provide personalized wireless broadband access, and will incorporate mobile and wireless access methods including e.g. Wifi, WiMAX [3]. Offering personalized broadband wireless services across networks, both national and international, will require new ways of service interconnectivity.

The key challenge in personalized broadband wireless service access is the handling of user preferences, context, devices, and connectivity. The European project ePerSpace introduced personal service delivery in the home segment, based on user profiles and preferences [7]. While the home is a rather controlled environment, with trusted and known constellations of devices, service delivery in the mobile/wireless world is more complex. Louis V Gerstner, Jr of IBM said: *Picture a day when a billion people will interact with a million eBusinesses via a trillion interconnected, intelligent devices.* Pervasive systems *does not just mean computers everywhere; it means computers, networks, applications, and services everywhere.* The report from the UK Technology Strategy Board [8] pointed out that the high-added value comes from:

- **Always on** - availability of the right content at the right place and time.
- **User-centric** solutions - simple and practical person-oriented solutions.
- **Invisibility** - numerous, casually accessible, often invisible computing devices.
- **Intelligence** - removing the cognitive load through devices with embedded sensing and processing capabilities.
- **Increasing productivity** - market value propositions: saving time, saving money.
- **Life-enhancing** - penetration of technology into mainstream mass market applications.
- **Innovation** - using technology in ways that empower people to work, live, and play in radically new ways.
- **Omnipresent** - embedded into everyday devices and objects all around.
- **Ubiquity** - everyone and everything connected to an increasingly ubiquitous network structure.

To build these types of personalized 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. Noll suggested in [9] that 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.

Approaches for a mathematical description of identities have a longer tradition. Khoshaflau claimed back in 1986 the need for a 'strong support of identity', and described identities through a graphical representation [10]. The introduction of semantics and the representation in .rdf and .xml allows describing user preferences and relations to characterise the social context of the user as indicated in fig. 1 for a school scenario. Paul and Anna are members of class two of Sogn school, and their parents, here: Frank and Maria are defined through a friend-of-a-friend (foaf) based relationship. This paper connects social relations to document and service access as illustrated in fig. 2, here a Web camera connected to the classroom, and photos/videos taken by the parents. Our service scenario builds on the relation between the actors, and establishes access rights to services and documents. Further details on the selected approach are given in sect. 4.

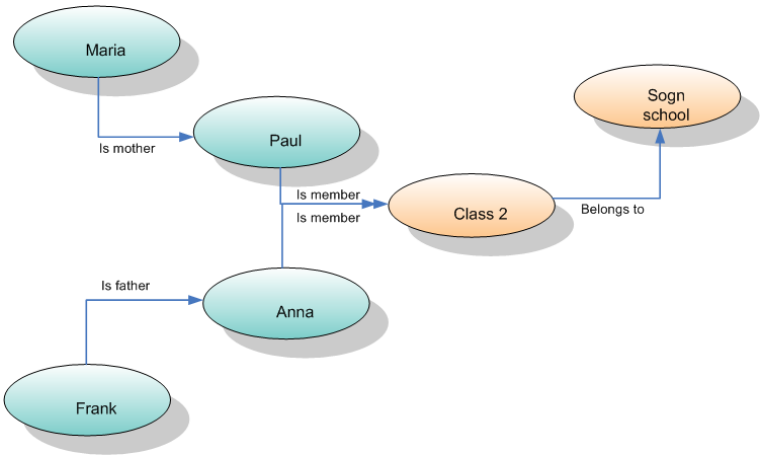

Figure 1: Social relationship based on a school scenario

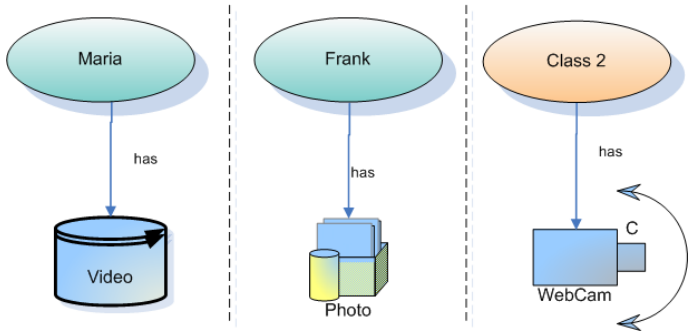

Figure 2: Document and service repository in a social context

2.2 Service centric approach

New methodologies, techniques and tools are necessary to develop and maintain services for the future that are both attractive, easy to use and cheap enough. Concepts and technologies like Service Oriented Architectures (SOA), Web Services (WS), Semantic Web (SW) and Semantic Web Services (SWS) have gradually grown up to show their viability, especially if they are used in combination. Semantic Web-based technologies are widely acknowledged to play an important role in solving the interoperability problem between applications; the usage of semantic description in the context of advanced services delivery is expected to support easy access to the services. Not only such formal and explicit descriptions enable easy service integration, but will also support exchange of preferences, profiles and context information of mobile users.

While SOA as a vision evolved well, different implementations hampered the applicability. To avoid those problems standardisation done by OASIS established a framework and drafted a reference model that a system has to adopt in order to claim compliance with the OASIS SOA specifications [11]. According to the OASIS frame-

work SOA is an architectural paradigm (model) that does not necessarily mean usage of Web Services although Web Service is a popular implementation. The SOA reference model should captures core principles and axioms of SOA and be used as a template for the SOA architecture [12]. One prototypical implementation of a Semantic SOA platform was performed in the European Research project Adaptive Services Grid (ASG[2]), which based the platform design on the following service specific requirements, using Web Service Modelling Ontology (WSMO) [13].

- **Reuse** of existing functionality, e.g. services and infrastructure, makes use cases cost-efficient to realise.
- **Standards and Reliability** are essential for industry to adopt solutions.
- **Openness** will allow integration of additional services with as little changes as possible.
- **Adaptivity** to current environmental constraints, e.g. user preferences and user connectivity is key for user acceptance of new services.
- **Dynamic** and transparent service composition is required to adapt to the specific service requests.
- **QoS awareness** handles specific user requests, e.g. budget or time constraints.
- **Semantic Awareness** is crucial for understanding the user request, service discovery and service composition.

ASG fulfils the requirements, and extends the specifications of the OASIS SOA reference model. In spite of the big conformity to the reference model it is a great chance that interoperability problems will occur between an ASG system and an OASIS compliant SOA system. The reason is the choice of different semantic standards for describing their respective data models [14]. While a technical solution might be expected in the time frame 2009/2010, issues like privacy and protection of user requests and dynamic service level agreements between service providers might hamper the time to market. Kagal et. al. pointed out similar findings and claimed the necessity to extend Web Services with privacy and security [6]. They suggested an extending of Semantic Web Services based on OWL-S with policies, representing security requirements for service discovery and privacy protection of user requests. However, this alone does not solve all issues when it comes to an I-centric mobile user scenario, as addressed in detail in the next section.

[2]http://asg-platform.org

2.3 Mobile service world

The mobile service world has made the move to a SOA oriented architecture. Most of the mobile services like location information are available through a Parlay X Web service interface [15]. In [16] a semantic annotations of advanced Telecom services was used to achieve exchange of roaming information on a dynamic basis. The main findings of the approach were the cost reductions in service delivery, due to reduced effort for testing and updating of Web services in a semantic service world.

Two issues remain unsolved when it comes to the usage of SOA in a mobile environment, *(i)* the variation of the radio quality and *(ii)* specific mobile services in the proximity of the user [9]. 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. A service oriented platform builds on reliable, minimum delay and high-bandwidth connectivity, which is not achievable in mobile/wireless environments.

The service world of a mobile/wireless user consists of proximity and remote services. Examples of **proximity services** are admittance services or payment through contact-less cards. These services are moved to the mobile phone through Near Field Communications (NFC) and prototyped world-wide, e.g. from Mastercard in Dallas [17]. One goal of these field trials is to demonstrate interworking between wireless technologies and NFC, another goal is to address security issues like potential threats, identity, privacy and simplicity. Adding NFC capabilities to the mobile phone opens for key exchange through near field and through the mobile network, thus providing a principle way of delivering authentication information. The prototypical implementation in sect. 4 will use short messages (SMS) to distribute admittance keys, which are used for admittance to a building.

3 Identity based service access

In the real world, each of us has created his own spheres of identity. Identity is reputation: *what I say about me* and *what others say about me* [19]. My reputation is different, depending on whether I am at work, doing sports, or enjoy membership awards in a club. In the virtual world identity handling is more difficult, taking into account the dynamic service requests and privacy requirements of a user. Roccas introduced this in 2002 through the term of *social identity complexity*, defining a new theoretical construct that refers to an individual's subjective representation of the interrelationships among his or her multiple group identities [18].

Identity is mainly verified through an authentication mechanism. The Internet was built without such an identity layer. In the current Web2.0 discussion Identity2.0 is introduced to interconnect people, information and software. Various institutes and industries are working to provide better identity management solutions. In Liberty

Alliance[3], 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. Another solution, Sxip[4] has been designed to address the Internet-scalable and user-centric identity architecture. It provides user identification, authentication 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[5] 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.

Most of these identity mechanisms are tailored towards remote services. In this paper we focus on methods of using different identification mechanisms for the variety of remote and proximity services, thus providing an Identity management for the I-centric and service centric world..

3.1 Representing the Identity

The proposed integrated identity mechanism consists of certificates, keys and preferences stored in a personal device and in the network. These identities are categorized in three groups of identity, personal identity (PID), corporate identity (CID) and social identity (SID) based on the roles exercised by a person in real life [20]. The PID can be used to identify ourselves in our very personal and commercial interactions. CID is used in our professional interactions, and SID in the social interactions. Fig. 3 shows the example applications of PID, CID and SID.

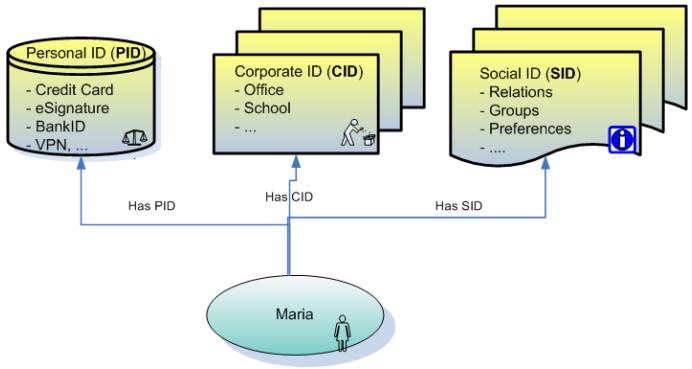

Figure 3: Personal, Corporate and Social Identities

Our approach suggest a de-centralized identity architecture, consisting of network components and the personal device of the user. Such an approach brings the user

[3]Liberty Alliance Project, http://www.projectliberty.org/
[4]Sxip Identity, http://www.sxip.org/
[5]Windows CardSpace, http://cardspace.netfx3.com/

Table 1: Identity types, storage and security requirements for role based service access

Identity	Example	Realisation	Location	Security Req.
PID	bank	certificate + key	SIM	high
PID	home admittance	home entry key	SIM	high
CID	visit admittance	temp. entry key	Network	medium
SID	preferences	*foaf*	Network	low
SID	attributes	*foaf*	Network	medium

in the control of his services, allowing him to accept or deny access to privacy information. The mechanism builds on a personal user device, typically a mobile phone, providing the underlying infrastructure. A trusted and well-accepted third party will provide authentication and identity, thus become an identity provider (IDP). The identity provider will issue certificate to the user and allocates a secure identity space in the network, in addition to the sensitive PID space on the user device. An example of such an approach is the BankID partnership which provides a PKI supported identity for bank transactions on the SIM card of the mobile phone [21]. The parts of the user identities which need lower authentication requirements, for example social identities and preferences (SID) will be stored into the allocated secure identity space. To manage multiple credentials, a trusted third party/service provider can load additional identities to either the SIM card or a network identity space. Control of the sensitive data is given through the mobile network: In case of loosing the SIM card, the card operator can disable the lost card and issue a new one, where identities can be reloaded through secure and signed SIM transactions.

With the identity subscription certificate users can access the network identity repository, e.g. service preferences located in the SID. Identities stored in this repository can give access to services (remote or proximity) that need medium or low level of security requirements. The main reason to store service and user preferences in the network is the availability of the network repository and the short response time, avoiding the costly and varying mobile/wireless link. Tab. 1 provides a summary of the identity types and their location. Personal identities (PID) are regarded as having high security, and thus will be stored in the personal device of the user, allowing him to control when and what PID information is released to service providers. Further guidelines supporting privacy handling are given in sect. 4.1.

The state or governmental organisations are traditionally the most accepted identity providers. With strong regulations in place, banks and mobile operators can also act as an identity provider (IDP). User should be able to make separate agreements with the selected IDP for the identity services. An IDP should maintain a strong trust relationship among its subscribers and with other IDPs. Such a strong trust relationship might be provided through the mobile network along with phone and SIM

card as the secure infrastructure for storing and exchanging identity information in the proposed solutions.

3.2 Data and service repository

This section will use the concept of role based identity presented in the previous section to enable service and document access for the scenario of fig. 1 and 2. We use the semantic description of social relationships to define service/document access rights as presented in fig. 4. Through the relation (here: mother of a child in class 2) Maria

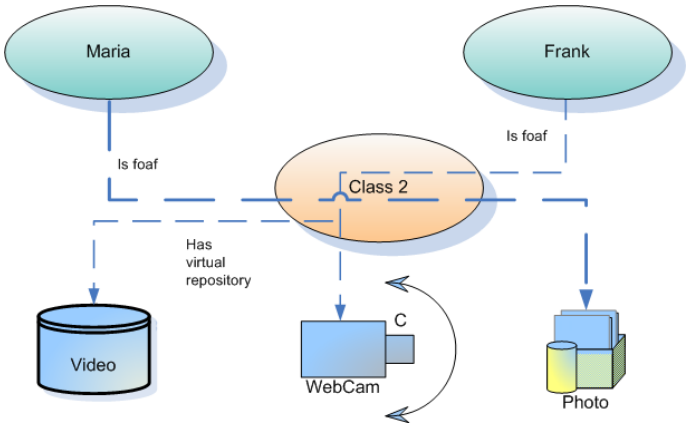

Figure 4: Virtual data and service repository

gets access to the photos taken by Frank, who is father of a child in class 2. The corresponding sequence diagram for this service access is given in fig. 5. Maria sends

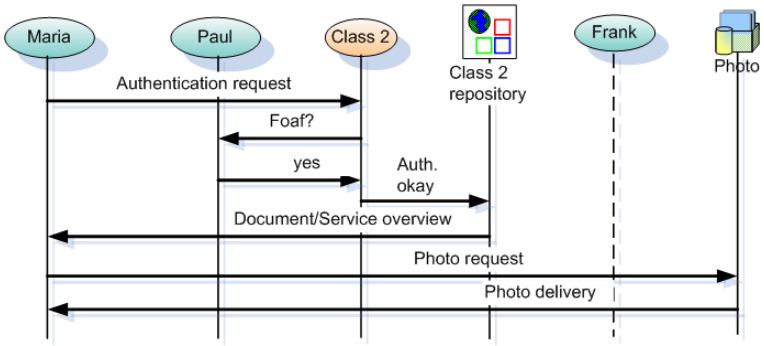

Figure 5: Sequence diagram for data access in the 'class 2' repository

an authentication request to the service repository of class 2. The authentication request checks that she is related to Paul (*foaf*), and thus provides access to the class 2 repository and finally access to the photos taken by Frank.

Our service access example uses social relations (SID) of Maria, and corporate (here: school) relations (CID) of Paul. Service realisations based on social identities will use

the semantic description of relationships, preferences and context information. Service access requiring PID information is subject to user involvement, as outlined in the next section.

4 Privacy and Authentication

This section will provide guidelines for privacy handling of user information in a semantically supported service environment. It will then show the prototypical implementation of personal identities, based on an admittance scenario.

4.1 Privacy protection in a distributed architecture

A service related security infrastructure should just provide the information which is necessary to access the service, and should not compromise the privacy of the user. Our approach is based on two factors, *(i)* the authentication provisioning by an accepted identity provider and *(ii)* the distributed storage of personal, corporate and social identity information. Fig. 6 provides a sketch of the distributed approach, where an identity request is either answered from a formal ID provider or an ID-provisioning engine located in the service domain, in our example the home or corporate network. Keys and certificates of sensitive manner are stored in the personal device of the user.

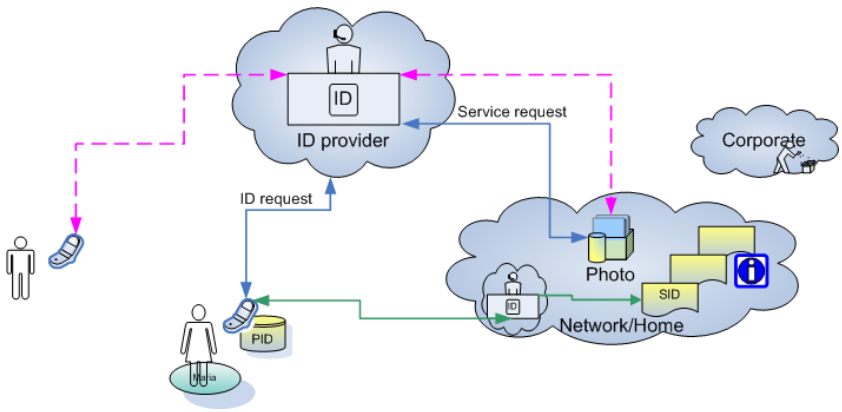

Figure 6: Authentication and privacy handling in a distributed manner

This will allow a strong authentication based on both a *possession* and a *knowledge* factor for e.g. bank applications. The reason to store the PID information in the mobile is to inform the user about transactions or access to other confidential data, and let him decide whether access should be granted.

Service preferences, user context and connectivity are stored in SIDs, allowing for adaptation of services. Privacy of those data should be ensured through mechanisms suggested by Sxip or Windows CardSpace, as introduced in sect. 3.

Following the distributed identity architecture of this paper, privacy is ensured through:

1. A definition of my social contacts based on *foaf* principles. Access should be granted on a membership in a SID, e.g. the family, cycling friends or other interest communities.

2. The membership in these interest communities will also ensure an access to my preferences, which are of importance for just this community.

3. Access to other preferences have to be granted on a case-by-case basis through mechanisms proposed by the Internet community (see sect. 3).

4. Sensitive information like payment will only be handled if accepted from the personal device of the user, either through profiles or specific user interaction.

The following section will show a prototypical implementation of handling of sensitive information.

4.2 Prototypical implementation

In this section we take up an admittance scenario following the home admittance PID case of tab. 1. The prototypical implementation covers two aspects, *(i)* the use of a home entry key and *(ii)* the secure distribution of such a key through the mobile network. Steps in the prototypical realisation are illustrated in fig. 7, and are based on the following steps [22]:

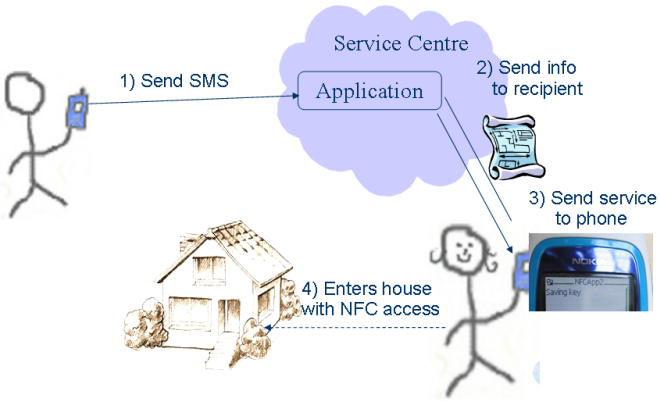

Figure 7: Prototype of key handling for admittance services

1. Frank sends SMS to service number to allow Maria accessing his flat 15b. Example: SMS to 2034 "90838066 17.12.2006 1000-1400"

2. Service centre creates an service SMS installed on Maria's phone 90838066: *Admittance key transferred to NFC phone*

3. Service centre informs Maria:*Access granted to flat 15b, My Road, My City on 17.12.2006 from 1000-1400h. Use phone to get entrance.*

4. Maria enters flat 15b with help of the NFC phone. Frank might receive an acknowledge message when Maria enters the flat.

This example of an admittance control is prototyped using the functionality of Telenor's PATS[6] Innovation lab, Nokia's 3320 phones with NFC shells and a simulated lock system. It comprises elements of seamless authentication, interworking between mobile and near-field communication and provides new and advanced services to the end user. Frank is authenticated in a seamless matter when sending the SMS, interworking is provided through PATS' lab based install messages. The users, Maria and Frank, experience admittance based on SMS exchange as an advanced new service.

The service scenario implemented above uses the mobile operator as identity provider. SMS is treated as a secure matter for distribution of admittance certificates. While this role of a mobile operator is accepted in some regions, it can't be generalised. This paper suggests that an identity provider should take the role of providing certificates, and that the SIM card is managed by the identity provider.

The current implementation demonstrates the distribution of PIDs, thus ensuring the privacy of the most sensitive parts of the user identity. Implementations of SID and CID are subject to further work, and will require a more detailed analysis of potential security threats.

5 Conclusions

Ubiquitous computing and the pervasive Internet have enabled service access in every situation. However, adaptation to the user needs is purely handled, and service specific security implementations are only found for specific services. The paper introduces an integrated mechanism for identity provision facilitating both remote and proximity service access. A semantic description of user preferences, context and connectivity is used to describe the social identity of the user to be stored in a secure user identity space in the network. Sensitive information, defined as personal identity, is suggested to be stored in the SIM card of the user's personal device, providing him with full control over the usage of such service.

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 mechanisms, both for proximity and remote services. As such it combines the I-centric and service centric service world. The prototypical implementation of SMS-based admittance key distribution covers two aspects, *(i)* the

[6] http://www.pats.no

use of a contactless home entry key and *(ii)* the secure distribution of such a key through the mobile network.

References

[1] The World factbook 2006, https://www.cia.gov/cia/publications/factbook/geos/gm.html, [accessed 17.12.2006, 20:23h]

[2] Ball State study finds computer usage trails only television viewing, News center from Ball State University, http://www.bsu.edu/news/article/0,1370,-1019-45461,00.html, [accessed 17.12.2006, 20:41h]

[3] W. Kellerer, R. Hirschfeld, M. Wagner, and J. Noll, "Systems beyond 3G - Operators' vision", WWRF #7, 3.-4.12.2002, Eindhoven (NL)

[4] S. Arbanowski, P. Ballon, K. David, O. Droegehorn, H. Eertink, W. Kellerer, H. van Kranenburg, K. Raatikainen, and R. Popescu-Zeletin, "I-centric Communications: Personalization, Ambient Awareness, and Adaptability for Future Mobile Services", IEEE Comm. Magazine, Sep 2004, pp 63-69

[5] S.A. McIlraith, T. Cao Son, and H. Zeng, "Semantic Web Services", IEEE Int. Systems, vol. 16, no. 2, pp. 46-53.

[6] L. Kagal, T. Finin, M. Paolucci, N. Srinivasan, K. Sycara, G. Denker, "Authorization and Privacy for Semantic Web Services", IEEE Int. Systems, vol. 19, no. 4, pp. 50-56

[7] P.Y. Danet, "ePerSpace: A European Project for the Seamless and Personalised Digital Communicating Home of the Future", European VPN Services Forum conference, 15-17.6.2006 London.

[8] UK Technology Strategy Board, "Information and Communication Technologies", April 2006, http://www.dti.gov.uk/files/file27990.pdf, [accessed 17.12.2006, 23:20]

[9] J. Noll, "Services and applications in future wireless networks", Telektronikk 3/4.2006, pp. 61-71

[10] S.N. Khoshaflau and G.P. Copeland, "Object Identity", Proceedings OOPSLA'86, Sept. 1986, pp 406-416

[11] OASIS, "Reference Model for Service Oriented Architectures", Working Draft 09, 20 September 2005

[12] IBM , "Transforming your business to on demand", http://whitepapers.zdnet.com/ whitepaper.aspx?cname=Regulatory+Compliance&docid=139018, [accessed 10.11.2005]

[13] D. Roman, U. Keller, H. Lausen, J. de Bruijn, R. Lara, M. Stollberg, A. Polleres, C. Feier, C. Bussler, and D. Fensel: Web Service Modeling Ontology, Applied Ontology, 1(1): 77 - 106, 2005.

[14] J. Noll, E. Lillevold, "Roadmap to ASG based Semantic Web Services" , in Proc. of The International Conference on Internet & Web Applications and Services 2006 ICIW 23-25.Feb 2006.

[15] 3rd Generation Partnership Project, "Stage 2 functional specification of User Equipment (UE) positioning in UTRAN", 3GPP TS 25.305, Release 5, Sept 2003

[16] J. Noll, F. Kileng, R. Hinz, D. Roman, M. Pilarski, "Estimating business profitability of Semantic Web Services for Mobile Users", in *S. Schaffert, Y. Sure, Semantic Systems, From Visions to Applications*, Proc. of the Semantics 2006, Österreichische Computer Gesellschaft, pp 195-204

[17] Cellular-news, "MasterCard Tests NFC Payments with Nokia Handsets", http://www.cellular-news.com/story/20211.php, [accessed 10.12.2006]

[18] S. Roccas, M. B. Brewer, "Social Identity Complexity", Personality and Social Psychology Review, 2002, Vol. 6, No. 2, 88-106

[19] D. Hardt, Identity 2.0, *OSCON 2005*, http://www.identity20.com/media/OSCON2005/

[20] M. M. R. Chowdhury, J. Noll, "Distributed Identity for Secure Service Interaction", in press, The Third International Conference on Wireless and Mobile Communications, ICWMC07, March 4-9, 2007-Gaudeloupe, French Caribbean.

[21] BankID: Delivering Bank-common Trust for Web-based Transactions, https://www.cybertrust.com/intelligence/case_studies/, [accessed 10.11.2006]

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