Semantically supported Authentication and Privacy in Social Networks

Josef Noll[1], Mohammad M.R. Chowdhury[1], György Kálmán[1], Juan Miguel Gomez[2]
[1]UniK, University Graduate Center, Kjeller, Norway
[2]Universidad Carlos III de Madrid, Spain
{josef,mohammad,gyorgy}@unik.no, juanmiguel.gomez@uc3m.es

***Abstract*—Service access in a ubiquitous computing and pervasive Internet environment has reached a new dimension. It is not longer a question of enabling services for customers, but to design a convenient and trusted service usage. While semantic services open for a description of user preferences, profiles and social groups, privacy handling is not addressed so far. Social communities based on friend of a friend (*foaf*) principles, LinkedIn, or Facebook are open for all registered users, thus data about yourself are spread all-around.**

This paper presents an architecture to enable social networks to enable privacy, based on the identity of the user. Focus is on the semantic description of user's role in social networks and on securing the access through appropriate authentication mechanisms. Depending on the security requirements of the user, Internet trust mechanisms or mobile-based key exchange mechanisms can be applied. The user-centric approach will enable the user to select an identity provider for the trusted management. A prototype using semantically defined social relationships demonstrates the capabilities of the suggested approach.

I. Introduction

Service access to proximity and Internet services is a commonality. The majority of customers use computers for these type of service access, appreciating the convenience of a good user interface. Computers have multiple disadvantages, they suffer from *(i)* the insecure computer environment and infrastructure and *(ii)* the limitations to certain environments. While insecure computer environment and infrastructure are subject to research in various projects, the limitations to a quasi-stationary environment, at work, at home or in the office is a hinder for active participation in social communities. According to a study from the Ball State University an average PC usage is just above 2 h/day[1] [1]. This limits the usage of PC-based social communities, and most of these communities currently work to establish a mobile portal to their communities.

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 [2]. Taking into account that mobile users are available 24 h/7 days a week shows the potential for mobile service access. The access is currently hampered by a non-convenient user interface and limited adaptation of services towards the mobile platform. To overcome the limited interface capabilities is one of the key challenges for mobile operators [3], and subject of current activities in the Wireless World Research Forum [4].

Threats to privacy in social networks comes through the "unlimited" availability of electronic content once it is published and the traceability of users in a 24/7-available mobile environment.

This paper presents an architecture to enable secured service access for members of a social community. Focus is on the semantic description of user identity and user roles (sect. II) and on securing the access through a role-based membership and access to electronic content. The paper discusses potential candidates for a security infrastructure covering both Internet technologies and mobile phone based key distribution. It introduces in sect. III an identity architecture, covering private, corporate and social identities. An I-centric approach will enable the user to select an identity provider for the authentication and trust management, ensuring the privacy requirements of a user in a certain context. The paper provides in sect. IV a concept and a prototypical implementation using a semantic identity with appropriate authentication mechanisms.

II. User, device and service environment

This section focusses on the challenges of a ubiquitous service environment, supporting the preferences and context of the user and his communication devices. Historically a service centric architecture was introduced to let services communicate with each other. The user- or 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 [5]. 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 [6].

The key challenge in a user-centric approach is the handling of user preferences, context, devices, and connectivity. The Eu-

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

ropean project ePerSpace introduced personal service delivery in the home segment, based on user profiles and preferences [7]. Experiences from this and similar projects showed that managing and updating preferences is a tedious work and that users often disagree with the selected services resulting from a rule-based decision engine. 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 personalisation is easy and intuitive. Several authors suggest 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 [3], [4], [9]. Such systems would become to complex to be handled through rules, thus reasoning is seen to be a more appropriate matter to handle what to present to the user.

A. Service environment scenario

Service access is coupled to an identity, or a way of *prove that I'm the person who is allowed to access/purchase the service*. Identity is verified through an authentication mechanism. The Web community has defined Laws of Identity, providing a unifying identity meta-system that can offer the Internet the identity layer it needs [10]. Claim two handles *Minimal Disclosure for a Constrained Use*, thus the claim to protect the privacy of the user.

Personalisation is based on handling the user's identity. Approaches for a mathematical description of identities have a long tradition. Khoshaflau claimed back in 1986 the need for a 'strong support of identity', and described identities

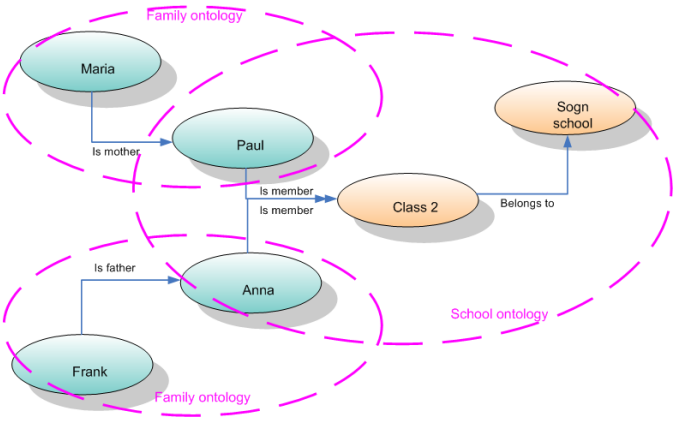

Fig. 1. Social relationship based on a school scenario

through a graphical representation [11]. 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 the family ontology as their respective parents. This paper suggests a distributed ontology of memberships where "Class 2" members are handled by the school, and family relations through family-based ontolotgies. It thereby 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

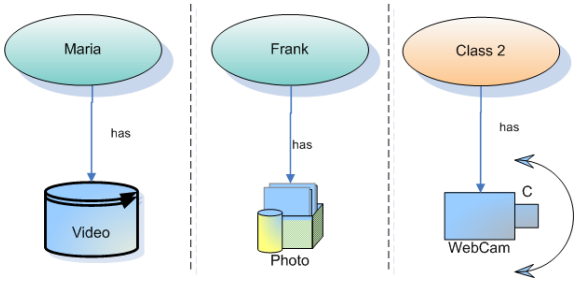

Fig. 2. Document and service repository in a social context

on the relation between the actors, and establishes access rights to services and documents. Further details on the selected approach are given in sect. IV.

B. Semantic service delivery

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. According to the OASIS framework SOA is an architectural paradigm (model) that does not necessarily mean usage of Web Services although Web Service is a popular implementation [12]. One prototypical implementation of a Semantic SOA platform was performed in the European Research project Adaptive Services Grid[2] (ASG) in order to dynamically create services for the end user. While a technical implementation of a semantic service platform 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 [13]. Kagal et. al. pointed out similar findings and claimed the necessity to extend Web Services with privacy and security [5]. They suggested an extending of Semantic Web Services with policies, representing security requirements for service discovery and privacy protection of user requests. This paper suggests to extend the usage of semantic descriptions to user preferences and context, thus allowing to dismiss only the required information for a specific service request.

C. Authentication mechanisms

The mobile service world has made the move to a Web service oriented architecture. In [14] 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.

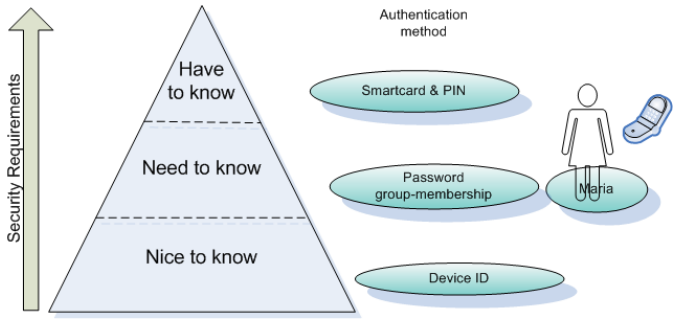

Fig. 3. Security requirements for service access

Extending the user preferences and context description in a semantic manner supports the disclosure of just the relevant user information for secure service access. In our scenario, access to content of *school class 2* should only be granted to relatives of the class members. Today such an access is often secured through directory access mechanisms which have limited functionality and are complex to manage.

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

Our approach is to define access rights through social relations, e.g. *all parents from pupils of class 2 have access* to photos or member information. Depending on the security requirements of the specific service (see fig. 3), identification can be of type *nice to know*, e.g. using the device identity; *need to know* through e.g. password or *have to know* through e.g. smartcard and pin code. Different identification mechanisms for the variety of services are defined and realise the mechanisms suggested by the Initiative for open authentication[3] *(i)* SIM authentication (SIM), *(ii)* Public Key Infrastructure (PKI), and *(iii)* One-Time-Password (OTP).

The difference to today's authentication is that a person does not identify himself to a specific service, but is asked to verify his role (e.g. social relationship) providing him with the service access. Information about the user will not be disclosed, the service provider will just receive a certificate ensuring that the user has sufficient rights to use the service.

D. Mobile supported service world

Service access includes more and more the mobile phone, examples of which are admittance and payment services through contactless cards. Near Field Communications (NFC) enables these services on the mobile phone; the technology is prototyped world-wide, e.g. from Mastercard in Dallas [15]. 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. IV uses short messages (SMS) and NFC to distribute group keys, and thus demonstrates an important aspect of access provisioning.

III. Identity based service access

A dynamic service request, taking into account the privacy requirements of a user, can be treated as identity administration. Roccas introduced the term of *social identity complexity* in 2002, defining a new theoretical construct that refers to an individual's subjective representation of the interrelationships among his or her multiple group identities [16].

A. 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 [17]. Fig. 4 shows example applications of PID, CID and SID.

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

[3]OATH, http://www.openauthentication.org/

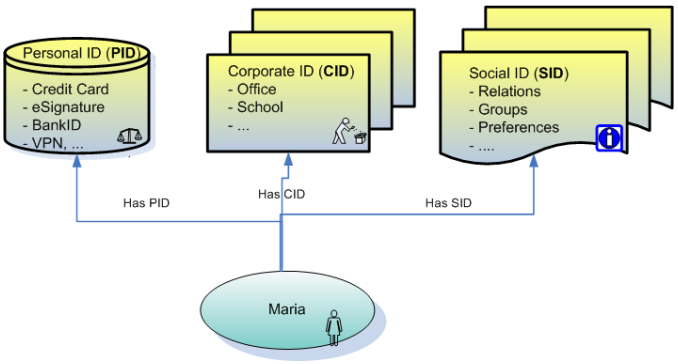

Fig. 4. Personal, Corporate and Social Identities

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. Personal identities (PID) require 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. IV-A.

B. 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. 5. Through the relation (here:

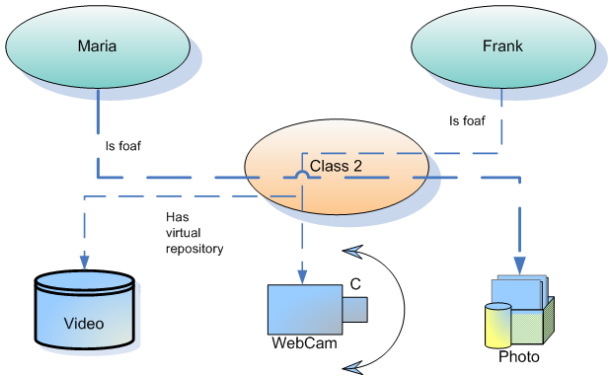

Fig. 5. Virtual data and service repository

mother of a child in class 2) Maria 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. 6. Maria sends 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. Authentication is key issue in this sequence. *How to ensure that Maria is the mother of a child in class 2*, and *that being allowed to access the photos Frank has taken*? We

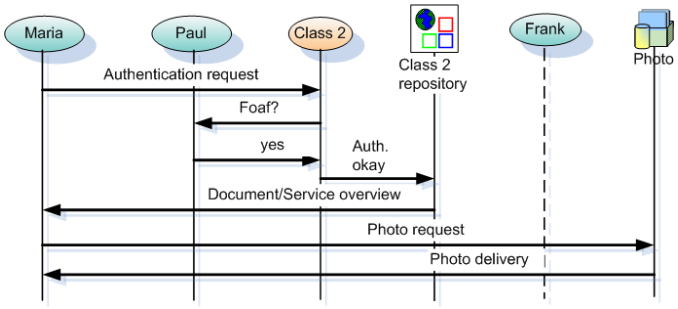

Fig. 6. Sequence diagram for data access in the 'class 2' repository

suggest that maria will use a "Web of Trust"[4] mechanisms or an ID provider (see sect. IV) to prove that she is mother of Paul, and that these credentials can then be added to the "parents lists" of class 2.

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.

IV. 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.

A. 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. 7 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 network. Keys and certificates of sensitive

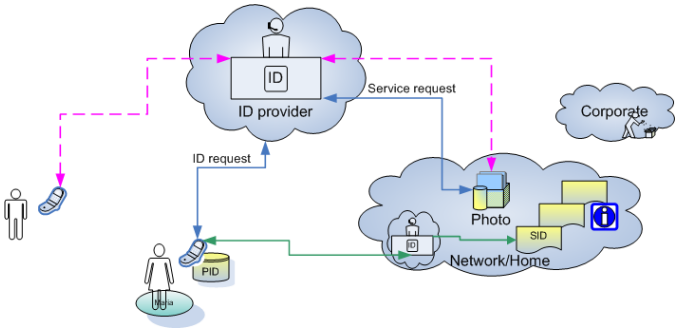

Fig. 7. Authentication and privacy handling in a distributed manner

[4]Web of Trust RDF Ontology: http://xmlns.com/wot/0.1/

TABLE I
ONTOLOGY FOR SEMANTIC IDENTITY (SEMID) BASED CONTENT ACCESS

Class2	
has roles	roles
teacher	administrator
members	pupils
parents	parents of pupils
guest	public info
has	access rights for
public info	guest, teacher, members, parents
memberlist	teacher, members, parents
photos	teacher, members, parents
Paul's personal map	teacher, Paul, Paul's parents

manner are stored in the personal device of the user.

Service preferences, user context and connectivity are stored in SIDs, allowing for adaptation of services. Privacy of those data should be ensured through Internet mechanisms as introduced in sect. III.

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

1) A definition of my social contacts based on *foaf* principles. Access to member information should be granted on a membership in a SID, e.g. the family, school or other interest communities. This will ensure that not all my memberships are public, but that e.g. family members have access to my family pictures.
2) The membership in these interest communities will also ensure an access to my preferences, which are of importance for just this community. Membership details will not be revealed to other SIDs.
3) Access to other preferences have to be granted on a case-by-case basis through mechanisms proposed by the Internet community (see sect. III).

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

B. Prototypical implementation

Our prototypical implementation covers the two main aspects, the ontology describing the relations between the members of the social community, their roles and access rights and the key exchange mechanisms for convenient and secure user authentication.

For demonstration purposes we use a combined ontology covering both the school ontology and the family ontology of fig. 1. The main purpose of this ontology is to prove that membership, roles and access rights, formulated in a semantic way, can be used for personalised access to community services. The ontology for our Semantic Identity (SemID.org) is implemented in OWL, and its key features are summarised in tab. I. It covers public information of the class like number of pupils, class restricted information as photos and member details and personal restricted information as teacher's comments.

The envisaged solution is based on any authentication provided either by Internet mechanisms or through mobile based key exchange. A generic solution demonstrating the key exchange in NFC and mobile networks was provided by the authors [19]. The service is an SMS initiated admittance, and generates access keys distributed through binary short messages (SMS) and NFC.

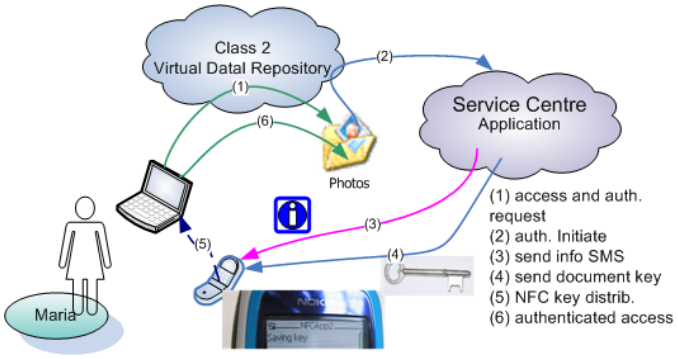

Fig. 8. Prototype of key handling for content access control

The realisation for content access control is as follows: Maria, the mother of Paul, wants to access photos of class 2 (step (1) in fig. 8). The authentication control in the class 2 repository send a "create authentication key" request (2) to the service centre, in our case using Telenor's mobile network through the PATS[5] Innovation lab. The 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) Maria's access to the photos.

C. Evaluation and future work

This prototype provides the basic mechanisms needed for content access management, here illustrated in a social context. The content is encrypted with a key containing the group identity, and only members of the group will have the rights to access the content. The mobile phone will be a central element in this architecture, as it can generate and distribute the keys.

The service scenario 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.

Our implementation uses a combined ontology for both the class membership and the family relations in order to easy demonstration. A real system would consist of a distributed ontology, where information about the class is covered in a school based identity system and information about family relations in a family ontology. Current ontologies like *foaf* are public available, which in itself does not respect the privacy requirements of the users. Future work in this area will establish distributed ontologies where policies decide on which parts of the ontology are available for which users.

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

The implementation of a NFC-based key distribution might be regarded as not necessary for community service access. Username/password is a good alternative though it requires authentication of the user. Our goal is to enable "role-based" seamless authentication and access, which includes the seamless distribution of access rights. NFC is seen as a promising technology to let user authentication be distributed between the user devices in a secure and seamless matter.

V. Conclusions

Ubiquitous computing and the pervasive Internet have enabled service access in every situation. However, adaptation to user needs is poorly handled, and service specific security implementations are only found for specific services. The paper introduces an integrated mechanism for identity provision facilitating role-based service access in social networks. A semantic description of user roles is used to describe the social identity of the user and the policies for access of group content.

Multiple factors of authentication mechanisms are employed to address different levels of security requirements. The paper also demonstrates key aspects of community-based service access using the proposed identity mechanisms. A combined ontology is established to prove that membership, roles and access rights, formulated in a semantic way, can be used for personalised access to community services. Authentication is either provided through Internet mechanisms or through SMS-based group key distribution. The SMS-based key distribution demonstrates how access or group keys can be distributed through the mobile network and used for contactless authentication.

References

[1] 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]

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

[3] W. Kellerer, M. Wagner, R. Hirschfeld, J. Noll, S. Svaet, J. Ferreira, O. Karasti, T. Hudginson, R. Giaffreda, S. Fallis, J.C. Francis, and C. Fischer, "Systems beyond 3G - Operators' vision", Eurescom Project P1203, December 2002

[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] L. Kagal, T. Finin, M. Paolucci, N. Srinivasan, K. Sycara, G. Denker, Authorization and Privacy for Semantic Web Services, IEEE Int. Systems, 2004, vol. 19, no. 4, pp. 50-56

[6] S.A. McIlraith, T. Cao Son, and H. Zeng, Semantic Web Services, IEEE Int. Systems, 2001, vol. 16, no. 2, pp. 46-53.

[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] K. Cameron, The Laws of Identity, http://www.identityblog.com/stories/2004/12/09/thelaws.html, [accessed 20.6.2006 14:10]]

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

[12] C.M MacKenzie, K. Laskey, F. McCabe, P.F. Brown, and B.A. Hamilton, OASIS, Reference Model for Service Oriented Architectures 1.0, 2 Aug 2006, http://www.oasis-open.org/committees/tc_home.php?wg_abbrev=soa-rm [accessed 10.1.2007, 22:10]

[13] 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.

[14] 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

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

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

[17] 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.

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

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