WIRELESS WORLD
RESEARCH FORUM

I-Centric Service Provision supported through Semantic Annotations

Josef Noll, György Kálmán, and Mohammad M. R. Chowdhury
University Graduate Center - UniK, Kjeller, Norway,
[josef,gyorgy,mohammad]@unik.no

Abstract—**The pervasive Internet haw enabled service access in every situation. However, adaptation to the user needs is purely handled, and user privacy is not handled properly. 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. 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.**

I. 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 bring user centric aspects into the service world. It explains the principles of the I-centric and service centric world in sect. II, with a focus on service delivery in mobile/wireless environments. It then introduces in sect. III 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. IV provide a concept and a prototypical implementation, followed by the conclusions.

II. 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.

A. I-centric vision

Access provision was the key issue in first and second generation mobile networks (1G, 2G-networks), while ser-

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

vice 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. 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 [7] 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 [8] 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.

Semantic techniques and their 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, and relates them to the social community *class two*. Our service scenario builds on the relation between the actors, and establishes access

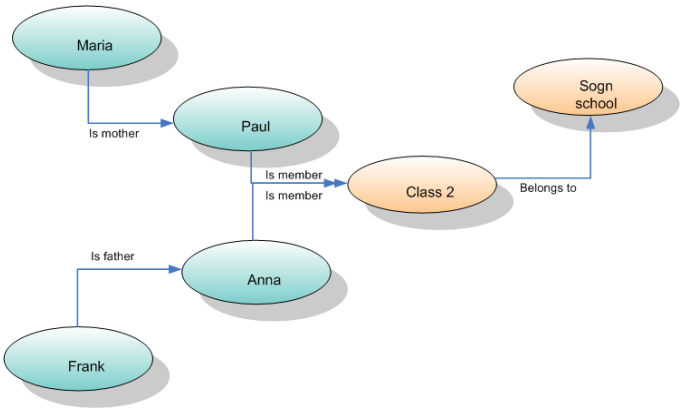

Fig. 1. Social relationship based on a school scenario

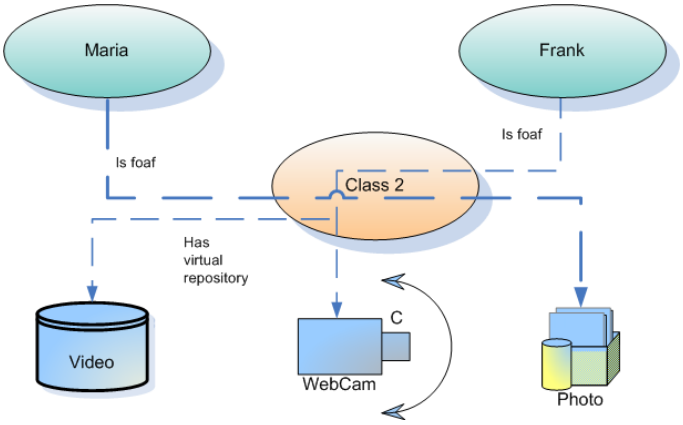

Fig. 2. Virtual data and service repository

rights to services and documents. Further details on the selected approach are given in sect. IV.

B. Mobile service world

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.

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 [9]. In [Noll et al. 2006b] 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.

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 [Mastercard 2006]. 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 will use short messages (SMS) to distribute admittance keys, which are used for admittance to a building.

III. Identity based service access

Most of the identity mechanisms described in literature, e.g. Liberty Alliance[2], Sxip[3] , Windows CardSpace[4], 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..

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 [11]. 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.

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 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).

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. I 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.

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

TABLE I
Identity types, storage and security requirements for role based service access

Identity	Example	Real.	Location	Security Req.
PID	bank	cert./key	SIM	high
PID	home adm.	entry key	SIM	high
CID	visit adm.	entry key	Netw.	med.
SID	preferences	*foaf*	Netw.	low
SID	attributes	*foaf*	Netw.	med.

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. 3 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. 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.

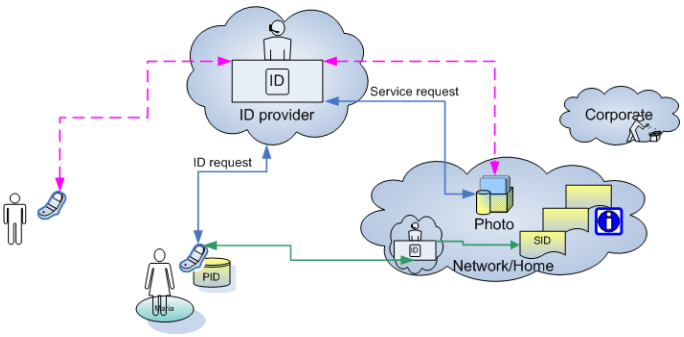

Fig. 3. Authentication and privacy handling in a distributed manner

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. 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 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. III).
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.

B. Prototypical implementation

In this section we take up an admittance scenario following the home admittance PID case of tab. I. 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. A generic solution demonstrating the key exchange in NFC and mobile networks was provided by the authors [Noll et al. 2006c]. The service is an SMS initiated admittance, and generates access keys distributed through binary short messages (SMS) and NFC. The provider of access (user) initiates an SMS to the service center, which generates a binary SMS providing the access key to the mobile phone of the person requesting access (guest). The guest's mobile phone can then use NFC to achieve access to a property.

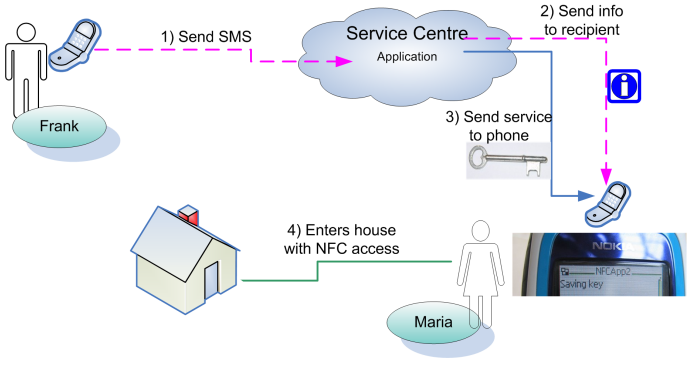

Fig. 4. Prototype of key handling for admittance services

The current implementation demonstrates the distribution of PIDs, thus ensuring the privacy of the most sensitive parts of the user identity. The keys will allow a seamless user authentication to the community, and together with a session authentication protect the privacy of the social group. Implementations of SID and CID are subject to further work, and will require a more detailed analysis of potential security threats.

V. Conclusions

The pervasive Internet has enabled service access in every situation. However, adaptation to the user needs is purely handled. The paper introduces a semantic description of user preferences, context and connectivity to describe the social identity of the user. 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. The prototypical implementation of key distribution is shown for an SMS-based admittance key distribution and covers two aspects, *(i)* the 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] UK Technology Strategy Board, "Information and Communication Technologies", April 2006, `http://www.dti.gov.uk/files/file27990.pdf`, [accessed 17.12.2006, 23:20]
[8] J. Noll, "Services and applications in future wireless networks", Telektronikk 3/4.2006, pp 61-71
[9] 3rd Generation Partnership Project, "Stage 2 functional specification of User Equipment (UE) positioning in UTRAN," 3GPP TS 25.305, Release 5, Sept 2003
[10] 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
[11] Cellular-news, "MasterCard Tests NFC Payments with Nokia Handsets", `http://www.cellular-news.com/story/20211.php`, [accessed 10.12.2006]
[12] 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.
[13] 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 ICWMC06*, July 29-31, 2006, Bucharest

Josef Noll (UniK) holds a professor stipend from the University of Oslo in the area of Mobile Services. Working areas include Mobile Authentication, Wireless Broadband Access, Personalised Services, Mobile-Fixed Integration and the Evolution to 4G systems.

He is also Senior Advisor in Movation, Norway's leading innovation company for mobile services. He received his Ph. D. from the University of Bochum (D), worked for the

European Space Agency at ESTEC from 1991-1997, and from 1997-2005 at Telenor R&I.

Gyorgy Kalman is a Ph.D. student at UniK, University Graduate Center in Kjeller, Norway. His research area covers personal and device authentication, security and privacy in wireless systems.

He got his M.Sc. degree in the area of communication networks from the Budapest University of Technology and Economics. He was Research Fellow at Telenor R&I at the Media Platforms group.

Mohammad M. R. Chowdhury is a Ph.D. student at UniK, University Graduate Center in Kjeller, Norway. His research area covers role based identity management in broadband wireless systems.