Enabling Privacy in Social Communities

Josef Noll, Mohammad M. R. Chowdhury, György Kálmán
University Graduate Center - UniK, Kjeller, Norway,
[josef,mohammad,gyorgy]@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 relations enabling service access. A prototype using over-the-air key distribution demonstrates the capabilities of the suggested approach.
Key Words: Semantics, privacy, social communities, key distribution, mobile, identity
Category: F.3.2, K.4.1, H.4.3.

1 Introduction

Current developments in service delivery have the focus on Mobile Service Delivery and Semantic Service Delivery. Current reporting from The World Factbook states two to three times as many mobile users as Internet users in UK, France and China [World factbook 2006]. Taking into account that mobile users are always available as compared to an average PC usage of just above 2 h/day[1] shows the importance of mobile service access [Ball State 2006]. This paper explains the principles of the I-centric [Arbanowski et. al. 2004] and service centric world in sect. 2. It then introduces in sect. 3 an identity architecture. Based on the social relations of a user, it will then in sect. 4 provide a concept for role-based service access and a prototypical implementation.

2 I-centric service provision in a social community

The key challenge in personalised service access is the handling of user preferences, context, devices, and connectivity. Personalisation should 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 [Noll 2006]. The mobile phone has a central place in this picture, as it supports seamless authentication, out-of-band key distribution, presence and location information. Semantics are introduced to describe user preferences and relations and to characterise the social context of the user as indicated for a

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

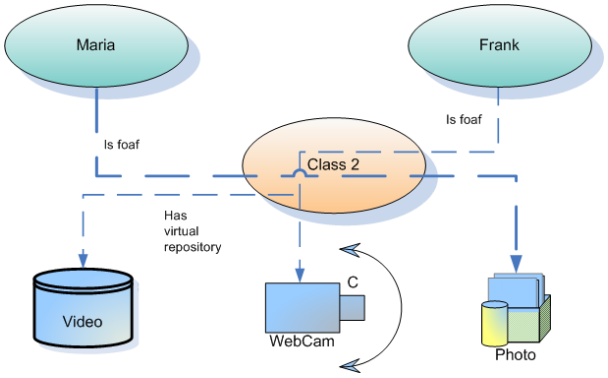

Figure 1: Virtual data and service repository

school scenario. Paul and Anna are members of class two of Sogn school, and their parents, here: Frank and Maria, are linked to the class 2 through a social graph. This paper uses social relations to enable content and service access. We use the semantic description of social relationships to define service/document access rights as presented in fig. 1. Through the relation (here: 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. Our approach is to use the mobile phone for authentication services, here based on short messages (SMS) to distribute keys.

3 Identity based service access

In the virtual world identity handling has to take 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 [Roccas and Brewer 2002]. 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. Identity mechanisms as suggested by e.g. Microsoft, Sxip and Liberty Alliance 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 per-

son in real life [Chowdhury and Noll 2007]. Users are authenticated by identity providers using keys. These keys were distributed only among the members of the group using the mobile environment. They then access the social contents using the proposed role-based ontology with differential access rights. The generic architecture is illustrated in fig. 2. Our service scenario builds on the relation

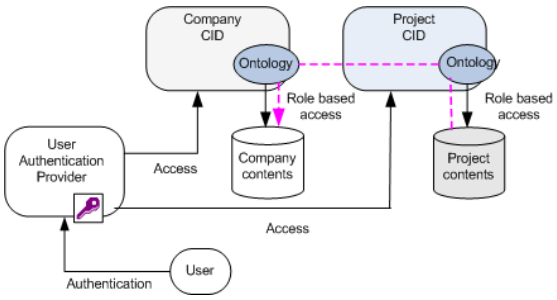

Figure 2: Generic architecture on seamless authentication and role-based service access for a corporate scenario.

between the members of a social community, and establishes access rights to contents and services. The 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 Prototypical implementation of key distribution

As a key of identity management in our proposal, a mobile based key exchange demonstrator was built [Noll 2006]. The key generation and distribution was modified to support requirements of social communities. The authentication system transmits the authentication keys through the mobile phone system to the mobile terminal. The terminal can either access services based on that key or perform a user identification In our scenario the user wants to get access to remote content. The access request is sent (1) and the access control system of the data service sends (2) a message to the Service Centre. This entity acts sends down (if needed) the required application (3) and a binary key (4). The key is stored in the integrated SmartMX card of the phone and can be transmitted over the NFC interface (5) to use the remote content. Our implementation uses Nokia 3320 mobile phones and keys distributed through Telenor's Innovation lab

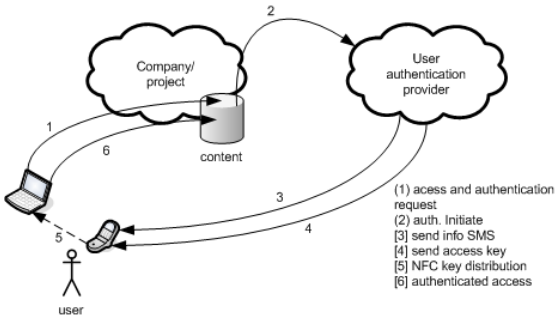

Figure 3: Prototype of key handling for content access control

PATS[2] .

5 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 and social relations describing the identity of the user. Sensitive information is suggested to be stored in the SIM card of the user's personal device, while preferences and social relations are stored in the network. Authentication is the key issue for role-based document and service access. A SMS-based key distribution demonstrates how access or group keys can be distributed through the mobile network and used for contactless authentication.

References

[Arbanowski et. al. 2004] 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

[Ball State 2006] 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]

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

[Noll 2006] J. Noll, "Services and applications in future wireless networks", Telektronikk 3/4.2006, pp 61-71

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

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

[2] `http://www.pats.no`