User-centric Identity Management in Open Mobile Environments

Mario Hoffmann

Fraunhofer-Institute for Secure Telecooperation (SIT)

mario.hoffmann@sit.fraunhofer.de

Abstract

Two levels of identity management can be determined. The first level considers Enterprise Identity Management which is currently on the roadmap of most companies dealing with huge knowledge bases of employees and/or customers. In this area identity management means (1) to provide employees with role-based access to documents and ressources and (2) to consolidate and concatenate partial customer identities for simplifications in customer administration.

Nearly at the same time the second level of identity management occurred. Personalised context-aware services have begun to enter, particularly, the mobile communication market and, obviously, detailed user profiles are essential to provide reasonable personalised services. These services are based on the user's current location, his environment, and personal preferences. Here, identity management becomes a key technology in order to keep those additional information under control. However, this pursuit of control, finally leads to severe implications on the users' side.

Hence, a third level of identity management has to be introduced: User-centric Identity Management. User-centric identity management allows the user to keep at least some control over his personal data where several different approaches have to be discussed. Specifically, a framework will be described which adds user-centric identity management to a context-aware mobile services platforms. This platform has been already designed to support and dynamically combine services especially of small- and medium-sized service providers which are not part of a centralised web portal.

Introduction

With the roll-out of UMTS and public WiFi hotspots in several European countries the usability and acceptance of Location Based Services (LBS) will finally succeed; the higher bandwidth promises Quality of Service (QoS) for video and audio streaming. Moreover, after the development and evaluation of LBS since the hype in 2000 the market is expecting a high penetration of so-called context-aware services in the next step. Whereas, context comprises not only the user's location but also the current time, the user's environment (in terms of additional sensor information based for example on RFID, cp. [WSRE2003]), the corresponding preferences, and the user's service history (cp. [BHT2003]).

On the one hand, in order to provide specific personalised value-added services the collection, the analysis, and the management of user related information is mandatory. The more service providers know from their customers the more precise they fulfil and predict the user's needs. Basically, identity management is assumed to be the key technology to bring together,

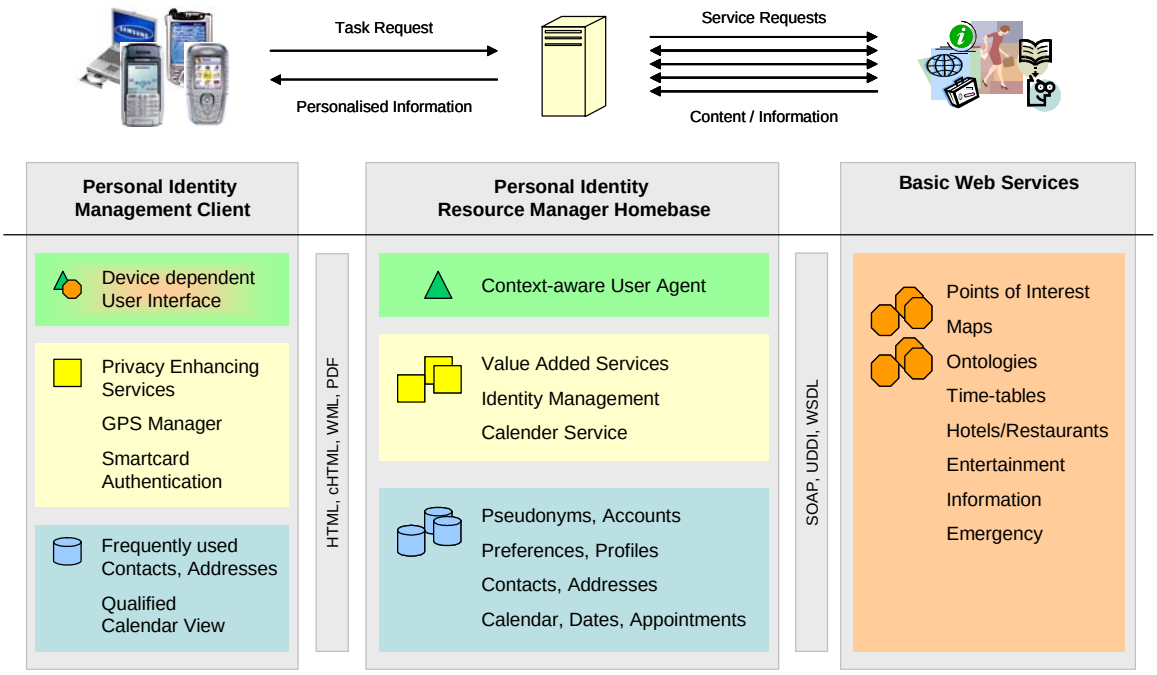

Figure 1: User-centric Identity Management Framework Architecture

consolidate, and analyse available information and partial identities of users and costumers (cp. [BFR2003]).

On the other hand, especially, in "old Europe" protecting one's privacy is not only a discontinued model, although Sep 11th also has left after-effects in keeping telecommunications and the Internet under specific surveillance. However, keeping the balance between security requirements and privacy constraints of *all* involved parties is still one of the key concepts and paradigms in our Institute's research work. Thus, so-called multilateral security (ref. [Rann2001]) serves as the basic security concept of a framework for context-aware mobile services. Especially, this framework enables corresponding platforms to realise user-centric identity management (cp. [HPP02]).

A Privacy Enhancing Framework

In principal, the overall architecture of the framework can be divided into three parts representing three different areas of trust that will be discussed in detail in the next paragraphs. The first area comprises the user's mobile device which contains small databases of frequently used contacts and addresses, and a qualified calendar view instead of the hole history of dates and appointments like in current implementations. So-called privacy enhancing services take care of user authentication and authorisation in case of accessing personal settings, preferences, and the *homebase*. Any kind of personal information is securely maintained by taking advantage of Smartcard technology and biometry. Each class of mobile devices is supported by a resource dependent user interface, i.e. taking into account different display resolutions, browser capabilities, and user preferences. The mobile device with an enabled *Personal Identity Management Client* is considered as providing enhanced control mechanisms.

In order to get access to context aware services the user triggers the corresponding user agent residing at the *Personal Identity Resource Manager Homebase*, the second area of trust. The homebase is, first, characterised by databases containing the hole set of the user's pseudonyms, preferences, contacts, and calendar entries. Moreover, value-added services consolidate incoming content from *Basic Web Services*, an identity manager balances grant and rejection to

personal identity information, and a calendar service manages dates, appointments, and their dependencies. Finally, the homebase is featuring a context-aware user agent which coordinates the activities between the different modules and prepares all results and service information depending on the user's current mobile equipment.

Control mechanisms and, thus, the level of trust highly depends on the location of the homebase. There is several opportunities: First, the homebase might be managed by the user himself on a personal server, e.g. the PC at home. However, this solution assumes a highly skilled and experienced user. Second, the user might take advantage of a personal homepage administrated by his company – many companies offer such a personal service for their employees. Third, Internet Service Providers (ISPs) specialised on managing and maintaining user identities could offer an appropriate service. Fourth, according to ISPs, Mobile Network Operators (MNOs) might take advantage of their huge subscriber community and could provide enhanced identity management services. Two well known approaches already introduced are Passport by Microsoft and the concept of federated identities by the Liberty Alliance Project (cp. [Pfit2004], [PfWa2004]).

However, nowadays most users are at least aware of threats concerning the Internet such as viruses, worms, and trojan horses. In addition, recent strategic security analyses of web-portals of Mobile Network Operators (MNOs) have shown that even those portals can be easily misused in order to spy out the user's preferences and personal configurations, to order mobile services and additional mobile phones for free, and even to enter mobile devices with malicious code. Nevertheless, especially mobile devices are still be considered as save and secure, although, there is neither integrated reliable encryption of application data or communication channels nor trustworthy service authentication nor additional user authorisation.

In contrast, in the proposed framework value-added services are only performed at the homebase. The homebase receives the necessary information by particular Basic Web Services based on the users' preferences. Those specialised services provide a combination of useful low-level information such as a city map, emergency services, points of interest, and for example the schedule of the public transport system.

In general, this approach has several advantages. On the one hand, the user's privacy is warranted by consolidating and analysing basic information at the homebase where value-added services such as the planning of a business trip can be provided. At that place under the user's control, finally, the current location based on a passive positioning system such as GPS will be added. Therefore, the exact position of the user never leaves the user's area of trust comprising the device and the homebase. On the other hand, small- and medium-sized specialised service providers – for example hotels and restaurants – are no longer restricted to only one single-sign-on-portal (often considered as single-point-of-failure) where they offer their services together with hundreds of others. They simply describe and provide their services and information in a standardised form based on Web Service technology and can be finally found at so-called UDDI repositories.

Conclusion & Outlook

At that point, the question of the business case can only partially be answered. The business model for Basic Service Providers is as simple as efficient. Only standardised information have to be offered and could be charged depending on their preparation cost. Much more difficult is the business case regarding ISPs and MNOs, although they obviously scent the big market by managing identities and offering value-added services as described above. However, chained identity information, customer loyalty, and targeted marketing are the other side of the story.

Currently, Open Source seems to have a head start considering a feasible and reasonable model to further develop the different components of the user agent's homebase. Although, applications developed under the paradigm of Open Source, indeed, are not free of bugs. At least, the fact that everybody can participate in the development, testing, and debugging process

is a promising approach to provide a service platform in respect of the user's security requirements and privacy constraints.

Both simplifying service provisioning and establishing privacy protection are only two advantages identified. Others still have to be elaborated and realised. For example, digital rights management (DRM) offers adequate mechanisms not only for protecting digital content such as video and audio files but could also be applied to identity management; users could associate their partial identities with specific purposes and an expiration date. Furthermore, mobile devices might be enhanced with the Trusted Computing Platform (TCP) in order to protect the access to Smartcards or biometry sensors. However, this is subject of forthcoming research work.

References & Related Material

[BHT2003] Bemmel, Jeroen van; Hoffmann, Mario; Teunissen, Harold; "Privacy and 4G Services: Who do you trust?"; 10th Meeting – Wireless World Research Forum, New York, NY, USA, Oct 27-28, 2003; http://wireless-world-research.org

[BFR2003] Bizer, Johann; Fox, Dirk; Reimer, Helmut (Hrsg.); DuD – Datenschutz und Datensicherheit; „Schwerpunkt: Identitätsmanagement"; 09/2003, Vieweg Verlag, 2003, ISSN 0724-4371

[Gröt2003] Grötker, Ralf (Hrsg.); „Privat! – Kontrollierte Freiheit in einer vernetzten Welt"; Telepolis, Heise Verlag, 2003, ISBN 3-936931-01-1

[HBC+2004] Hansen, Marit; Berlich, Peter; Camenisch, Jan; Clauß, Sebastian; Pfitzmann, Andreas; Waidner, Michael; "Privacy-Enhancing Identity Management"; Elsevier Information Security Technical Report (ISTR), 9(1):35-44, 2004; http://www.sciencedirect.com/science/journal/13634127

[HeSt2003] Hengartner, U.; Steenkiste, P.; "Protecting Access to People Location Information"; Proc. of First International Conference on Security in Pervasive Computing (SPC 2003), Boppard, Germany, March 2003, pp. 25-38; http://www-2.cs.cmu.edu/~uhengart/spc03.pdf

[HPP2002] Hoffmann, Mario; Peters, Jan; Pinsdorf, Ulrich; "Multilateral Security in Mobile Applications and Location Based Services", ISSE - Information Security Solutions Europe, Paris, France, Oct 2002; https://www.eema.org/isse.asp#papers

[JeKrZu2002] Jendricke, Uwe; Kreutzer, Michael; Zugenmaier, Alf; "Mobile Identity Management", Technischer Bericht 178, Institut für Informatik, Universität Freiburg, Okt 2002, Workshop on Security in Ubiquitous Computing, UBICOMP 2002, ftp://ftp.informatik.uni-freiburg.de/documents/reports/report178/report00178.ps.gz

[PAMP2003] Hulsebosch (Ed.); "PAMPAS – Pioneering Advanced Mobile Privacy and Security", IST-2001-37763, Final Roadmap; http://www.pampas.eu.org

[Pfit2004] Pfitzmann, Birgit; "Privacy in enterprise identity federation – policies for Liberty 2 single signon"; Elsevier Information Security Technical Report (ISTR), 9(1):45-58, 2004; http://www.sciencedirect.com/science/journal/13634127

[PfWa2004] Pfitzmann, Birgit; Waidner, Michael; "Federated Identity-Management Protocols –Where User Authentication Protocols May Go –"; 11th Cambridge International Workshop on Security Protocols, Cambridge (UK), April 2003, proceedings to appear in Springer, 2004; http://www.zurich.ibm.com/security/publications/2003/PfiWai2003FIM-BBAE-Cambridge.pdf

[PRIM2004] EU 6th Framework Program; Project Identifier IST-2002-507591; "Privacy and Identity Management for Europe"; http://www.prime-project.eu.org/

[Rann2001] Rannenberg, Kai; "Multilateral Security – A Concept and Examples for Balanced Security", New Security Paradigms Workshop, Proceedings of the 2000 Workshop on New Security Paradigms, Ballycotton, Country Cork, Ireland, pages 151-162; ACM Press New York, NY, USA, 2001, ISBN 1-58113-260-3

[RAPI2003] Huizenga, Jan (Ed.); "RAPID – Roadmap for Advanced Research in Privacy and Identity Management", IST-2001-28210, Final Report; http://www.rapid.org

[WSRE2003] Weis, Stephen A.; Sarma, Sanjay E.; Rivest, Ronald L.; Engels, Daniel W.; "Security and Privacy Aspects of Low-Cost Radio Frequency Identification Systems"; Proc. of First International Conference on Security in Pervasive Computing (SPC 2003), Boppard, Germany, March 2003; http://theory.lcs.mit.edu/~sweis/spc-rfid.pdf

[Wörn2003] Wörndl, Wolfgang; „Privatheit bei dezentraler Verwaltung von Benutzerprofilen", Dissertation, 2003, http://tumb1.biblio.tu-muenchen.de/publ/diss/in/2003/woerndl.pdf