Journal of Universal Computer Science, vol. 15, no. 12 (2009), 2353-2372
submitted: 15/12/09, accepted: 25/6/09, appeared: 28/6/09 © J.UCS

On the Personalization of Personal Networks - Service Provision Based on User Profiles

Ioannis G. Nikolakopoulos
(National Technical University of Athens, Greece
gnikolakopoulos@telecom.ntua.gr)

Charalampos Z. Patrikakis
(National Technical University of Athens, Greece
bpatr@telecom.ntua.gr)

Antonio Cimmino
(Alcatel-Lucent Italia S.p.A., Milano, Italy
antonio.cimmino@alcatel-lucent.it)

Martin Bauer
(NEC Europe Ltd., Heidelberg, Germany
Martin.Bauer@nw.neclab.eu)

Henning Olesen
(CMI, Copenhagen Institute of Technology (AAU), Ballerup, Denmark
olesen@cmi.aau.dk)

Abstract: In this paper, we present a user profile definition scheme featuring context awareness. Though the scheme has been designed to meet the needs of web applications deployed over heterogeneous devices, emphasis is given in the deployment of the profile scheme over Personal Networks (PNs), as the personalization of the deployed applications and services in PN environments is of great importance. The proposed scheme is presented as part of an integrated framework for user profile management that takes into account (and is therefore compliant to) the existing standardization attempts. The overall architecture and description of the profile management framework, taking into account security issues inside Personal Networks, is presented. The paper concludes by showcasing how user profiles have been incorporated in a selected pilot service of the EU IST research project MAGNET Beyond.

Keywords: context, user profile, personal network, identity, service architecture.
Categories: C.3, J.0

1 Introduction

Our daily access to information in Information and Communication Technologies (ICT) environments – in order to work, be informed and/or entertained, and communicate – happens through a variety of devices, networking interfaces, applications and protocols. The need for a unique, personalized and user-oriented approach has led to the need for the definition of user profiles. This is mandatory in order to identify the framework over which information exchange can be performed.

Up to now, work towards user profile definition has been carried out by several groups, while relevant organizations have also made attempts and recommendations for proposed ontology schemata and frameworks. A number of important standardization activities and research projects in this area are discussed in Section 2 of the paper.

Furthermore, in this paper we describe the role of user profiles in the deployment of context-aware services in Personal Networks (PNs), taking into consideration the particularities that PN environments present. A PN is a protected and secure person-centric network that includes a dynamic collection of closed or remote personal nodes and devices and provides context-aware services and applications [Lo et al., 06]. In order to extend the user-centric PN concept so as to address the frequent interactions either between multiple PN users with common interests, or between a subset of devices belonging to different PNs, the concept of Personal Network Federations (PN-Fs) has also been proposed [Niemegeers et al., 02].

The result presented here is a comprehensive framework, both in terms of definition and management of user profiles. Since there has to be an adequate infrastructure for those who participate in a federation or use a service, in this paper we also address the important issues of trust and security through the provision of a secure framework for PN-F formation.. This is a prerequisite for trusting and using context-aware structures that are based on the user profile information. Finally, the implementation of user profiles in selected pilot services is presented.

The rest of the paper is organized as follows: Section 2 presents an overview of existing approaches for personalization of web and mobile services and closes with the definition of the concept of identity. In Section 3 we describe the structure and ontology of the user profile information along with the corresponding management frame-work, as they have emerged from the work performed in the context of the European project MAGNET Beyond [MAGNET Beyond, 06]. In Section 4 we describe how user profiles have been incorporated, used and evaluated in selected pilot services. The paper concludes with Section 5, where the conclusions and future research directions are given.

2 Background on personalization of web and mobile services

2.1 Standardization work on user profiles

In order to be able to adequately meet the need for user profile standardization, we have to consider initiatives related to both the areas of web applications and next generation mobile computing. Any framework or standardization must take into account the areas of social networking, subscriber data management and identity management; all of these representing areas where concepts and comprehensive frameworks already exist. To the vantage, privacy protection and user acceptance are crucial for the success. The most important initiatives are those of the European Telecommunications Standardization Institute (ETSI) on guidelines and standardization for user profiles and profile management [ETSI, 05a], [ETSI, 09a], [ETSI, 09b], the technical specifications and service enablers developed in the 3rd Generation Partnership Project (3GPP) and Open Mobile Alliance (OMA), the OpenSocial Foundation API [Open-Social API, 08] specification for user profile and the World Wide Web Consortium (W3C) Recommendation [W3C Recommendation, 04] for description of device capabilities and user preferences. Ongoing work on user profiles in the Wireless World Research Forum (WWRF) is also aligned with the work of ETSI. The latter follows a more generic approach, trying to identify the framework under which personalized communication can be performed over next generation networks, while OpenSocial identifies the parts of the user profile that can be used in order to personalize information access over the web and provide social networking applications. W3C can be used to guide the adaptation of content which is delivered to devices.

2.1.1 ETSI, 3GPP and WWRF

ETSI's guidelines for Profile Management [ETSI, 05a] represent the most comprehensive work in the field. The corresponding document indicates that the user profile contains details about the user and his/her personal expectations, which are furthermore used by the system so as to deliver the desirable personalized behavior. Besides, it distinguishes three different profile types that are also used in order to guide the user's interaction with devices or services. In addition to the above, ETSI has released a series of technical specifications [ETSI, 05b] which define a Generic User Profile (GUP) for the 3GPP mobile system. These specifications aim at enabling the harmonious usage of user related information, originating from different domains in order to facilitate user preference management, user service customization, user information sharing, terminal capability management and profile key access. The work is continued in the ETSI Specialist Task Forces

- STF342, “Personalization and User Profile Management Standardization”,
- STF352: “Personalization of eHealth systems”, and
- STF287: “User-oriented handling of multicultural issues in multimedia communications”.

STF342 is currently working on two deliverables, an ETSI standard on standardized objects of the user profile [ETSI, 09a] and a technical specification of the architectural framework [ETSI, 09b]. The work is focused on user profile structure and management from a telecoms perspective with less focus on identity management and open Internet, and it does not so far include the aspects of service adaptation. An important part of the ETSI proposal includes the concepts of “normal” and “situation-dependent” profiles.

The 3GPP has also done a comprehensive technical study [3GPP TR 32.808] for the analysis of a common user model and of the basic structure of a Common Profile Storage (CPS) framework. The study focuses on 3GPP-based networks. In addition, they have started to develop Personal Network Management [3GPP TS 24.259].

A liaison agreement has been set up between WWRF and ETSI STF342. The work on user profiles from MAGNET Beyond has been incorporated in a joint whitepaper between working groups of WWRF, which will be published in the WWRF Outlook series [WWRF, 09]. This whitepaper further discusses the prospects of a unified profile management based on social network profiles, subscriber data and identity management frameworks, the application of user profiles and context information in service adaptation and personalization, and privacy and legal aspects of profile and identity management.

2.1.2 W3C Recommendation

W3C has also issued a recommendation regarding profiles. More specifically, the [W3C Recommendation, 04] defines a Composite Capabilities/ Preference Profiles (CC/PP) profile as a description of device capabilities and user preferences, often referred to as a device's delivery context, which can be used to guide the adaptation of content presented to that device. CC/PP Structure and Vocabularies 2.0 (abbreviated to CC/PP in the rest of this document) define a client profile data format, and a framework for incorporating application- and operating environment-specific features.

It should be noted that in the W3C Recommendation document, the term “profile” does not refer to a subset of a particular specification but rather to the document(s) which describe(s) the capabilities of a device. The Resource Description Framework (RDF) is used to create profiles that describe user agent capabilities and preferences.

A CC/PP profile is broadly constructed as a 2-level hierarchy: a profile having at least one or more components (e.g. the hardware platform, the software platform, or an application such as a browser), with each component having at least one or more attributes (that is, a sub-tree whose branches are the capabilities or preferences associated with that component). A CC/PP profile basically describes client and device’s capabilities regarding user preferences in terms of a number of "CC/PP attributes" for each component.

2.1.3 OpenSocial Application Programming Interface

The OpenSocial [OpenSocial API, 08] community enhances the state of the social web. The aim is to make it easier for everyone to create and use social applications. OpenSocial provides a standard way for websites to expose their social graph and corresponding information by taking into account the user preferences (<UserPref>) section in the Extensible Markup Language (XML) file, which describes the user input fields that are turned into user interface controls when the gadget runs. OpenSocial provides a way for application data to persist on a social networking site, and to specify the different ways that an application can be viewed within an OpenSocial container.

2.1.4 Going beyond the existing standards

When attempting to “compare” these three initiatives, one can deduce that the standards provided by ETSI and 3GPP are far more telecom-centric [Jørstad, 06], whereas others tend to be rather web-oriented. The aspects and specific characteristics of the profile types recommended by ETSI, make the 3GPP standard a suitable and useful base for the provision of personalized services over PNs. The need for ubiquitous access to context-aware services requires the definition of an integrated framework for user profile management, which takes into account the heterogeneity of networking interfaces and end user devices and which is web compliant and user/situation adaptable. From the brief presentation of the existing standardization attempts, it is obvious that an approach starting from the ETSI recommendation document that takes into account the related attempts for web profile definition seems to be the most appropriate. Following this approach, in the rest of the paper we will present our idea of a profile definition framework that harmonizes the existing standardization attempts into a compact and comprehensive user profile management scheme.

2.2 Personal data and identities

According to [ETSI, 05a], a user profile becomes a necessity when a user wants to personalize the way he/she experiences a device or a service. Starting from this, a user profile is a collection of preferences, rules, settings and generally user-and-context information. These are stored and can be modified dynamically so as to provide the appropriate behaviour of the device and other services – in the desirable format –, applicable to any situation and primarily to the user's needs.

As this becomes clearer, a profile must contain everything that is associated with the user, and, more generally, every attribute that specifies the characteristics, abilities, needs of a user and, certainly, every change in his/her status. In addition, this issue becomes more complicated as we have to take into consideration the fact that most users choose to have multiple profiles, each of them corresponding to different context (professional, personal), influenced by the user's unique lifestyle, situation and professional roles. As a result, mechanisms that automatically activate these different situation-dependent profiles should be implemented. Regarding personal user data, these can be divided into private and public parts, each one of them containing information that is either restricted to all (or most other users) or is public and freely available (and perhaps sometimes advertised). The perception of private and public information is not the same for all users and can even vary according to the circumstance. Therefore, special attention should be given when dealing with privacy issues, since they are heavily dependent on the subjective judgement of users. The case in [Camp, 04] defines the identity management as the complex process that ensures secure creation, storage and exchange of digital identities.

According to the IST FP6-Daidalos project, [Chen, 07] proposes a concept for the management of privacy and assurance of anonymity, namely the Virtual IDentity (VID). More specifically, VIDs advance the identity and policy management system to operate smoothly when data is either obscured or not associated with a real identity. The VID concept was also introduced into the MAGNET Beyond project and discussed in [MBD4.3.2, 07].

According to the above mentioned research work, the VID is a way for the user to group the policies that govern which information is disclosed from his or her PN to the outside, and which access rights are applied. The user needs to be able to act under different identities when interacting with foreign services or during the establishment of cooperation between different PNs by creating PN-Fs. Depending on the particular use cases, only parts of this information may differ from VID to VID.

The VID is equivalent to all the information that one can gather through observation and interaction with the user's PN. The types of information that formulate the user's VID and are potentially disclosed in MAGNET Beyond include the following.

- Identifier of the PN (the unique identifier is in fact the "name" of the PN that is visible to the other PNs)
- User profile (The user profile contains information regarding personal and professional details, user's settings etc.)

- Context information (The context information consists of all the situation dependent information)
- Services offered by the PN (The services offered by a user's PN and are corresponding to each and every VID.) [MBD4.3.2, 07]

2.3 User profile management frameworks

European projects such as IST Daidalos I and II [DAIDALOS, 06], and other architectures such as the one proposed by [Olivereau et al., 05], focus mostly on the incorporation of the VID into networks and also on the solution of mobility problems. Although the aforementioned works have done great progress on the identity integration, none has focalized on the formation of an integrated framework that would include a concrete management framework for user profile and context information.

In addition, works such as [Aguiar et al., 06] and [ITU-T, 04] present network scenarios over heterogeneous environments, but do not involve and thoroughly highlight the corresponding modules so as to take advantage of the user profile and context information. As it is also presented in [Gomes, 06], issues that refer to the protection of users' personal data and information, are highly important, but despite the fact that privacy issues are addressed at lower layers, application integration is not achieved.

There are works, on the other hand, that present the user profile and context information structure and definition, such as [Pinheiro et al., 08], that do not take into account the application and the usage of it so as to make the way that the user experiences his/her interaction with devices more personal.

Finally, there are approaches like [Youngjung et al., 05], that describe the user profile management framework which intends to exploit all the user–related context information, but without simultaneously considering any unthought-of parameters that might pop out during the evaluation process with real users.

Given the complexity of the work developed, the advantages of our work that helped us go beyond the existing limitations are the following:

- The implementation of real services so as to evaluate the proposed framework, and
- The simulation of real cases during the evaluation process with the use of usability and user experience tests within the MAGNET scenario.

Based on the above described information, the research that has been done in terms of the Magnet Beyond project and that we hereby present, has led to the realization of important new outcomes. The outline of these includes the demonstration of a concrete management framework for user profiles and context information, a concrete attempt to interface the PN framework with that of IP Multimedia Subsystem (IMS) and many meaningful information about user profile application, users' privacy and security concerns about the use of their personal information, as feedback from the pilot services and usability tests that were conducted.

3 User profile definition and management inside the PN

3.1 User profiles: Definition and structure

Starting from the above indicated description for personal data, the user profile follows a tree structure and consists of several subcomponents placed throughout the PN that are accessed through the “User profile” subcomponent. The list of the fundamental subcomponents of the user profile consists of the following profile subcomponents:

- Basic Profile
- Extended Profile
- Device Profile(s)
- PN-F related Profiles
- 3rd party Profiles

The basic profile component of the user profile contains the basic settings and information that characterize the user’s identity in a given time and consists of three major parts:

- Personal user information, based on user related data [Golemati et al., 07]
- Professional user information, addressing professional issues of identity and preferences
- Behaviour, related to the way the user experiences interaction and working with the personal devices

The extended user profile includes generic user settings and preferences that are based on the individuality of a user, which are not permanent and can change according to the user’s will and needs. Most entries in the user profile are part of the extended user profile, which mostly contains information that is generated over time.

The device profiles include information about device-specific preferences and characteristics. It contains numerous references to online resources and is practically a list of device descriptions, containing data for those characteristics of a device that can be seriously affected by the user’s choices or special needs, as might be for example de-vice settings for deaf users.

The PN-F part of the profile contains all the information about the user’s PN-Fs. The PN-F profile is a data structure that is created, stored and maintained by the federation creator and describes the entire PN-F with all the specific characteristics that it has, while the PN-F participation profile contains information and preferences about each specific member.

The 3rd-party part of the user profile contains preferences and information that a 3rd party service provider needs to store in the user profile such as a nickname and the score of the user.

The above described analysis of profile information has been used in the context of the MAGNET Beyond project in order to define the MAGNET User Profile (MUP) that is structured exactly as previously.

The research progress made within MAGNET Beyond in making an expansion and enhancement of existing user profile ontologies is shown in Figure 1, which splits up the MUP into different parts and identifies existing approaches.

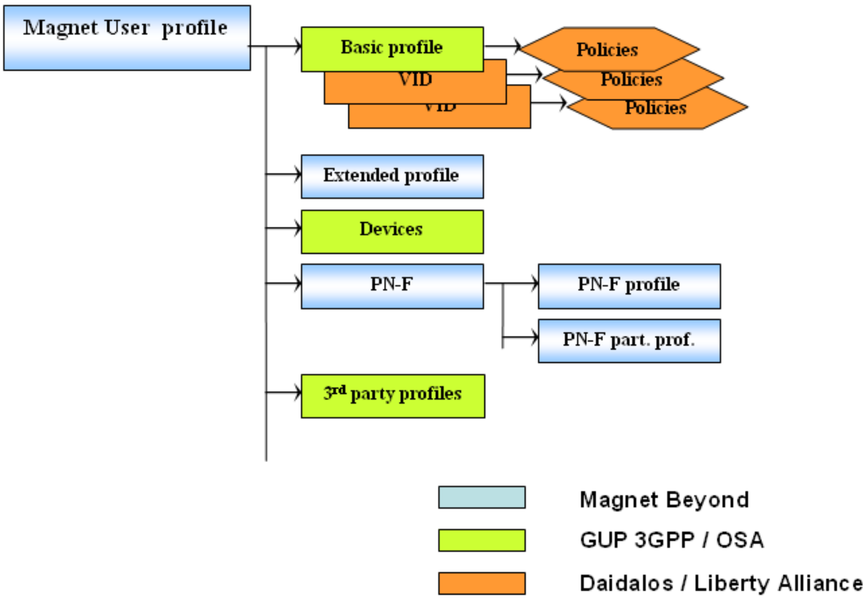


Figure 1: MAGNET user profile in a conceptual representation displaying the different categories and dependencies compared to state-of-the-art

3.2 Common ontology for user profiles and context information

In addition to the user profile information presented in the previous section, there is additional, and often more dynamic, information that may be relevant to adapting application and services to the user's needs: context information. Context information refers to the current situation of the user within his or her current environment. In [Dey, 00] it is defined as: "Context is any information that can be used to characterize the situation of an entity. An entity is a person, place, or object that is considered relevant to the interaction between a user and an application, including the user and application themselves".

In order to manage both user profile and context information, we decided that the Context Ontology should be integrated with the User Profile ontology leading to the creation of the integrated Ontology for context and user profile information management. This ontology is used as a basis for storing context and user profile information. Figure 2 shows the core concepts of the Integrated Ontology for context and user profile information. The underlying idea is to model information in the form of entities, which have attributes describing the properties of the entity and relations to other entities. Entities can be real world objects or abstract entities like profiles, policies, or roles. The entity types are modeled as concepts in the ontology and the attributes as properties. The ontology defines a hierarchy of entity types, facilitating the type-based access to context and user profile information. Its top-level concept is the *MagnetEntity*. The *MagnetEntity* concept introduces the property *hasIdentifier*. Any entity that can be uniquely identified using an identifier can thus be modeled as a

MagnetEntity. Based on the unique identifier, an index can be built, that provides the basis for efficiently accessing context information in all cases in which the specific entity is known.

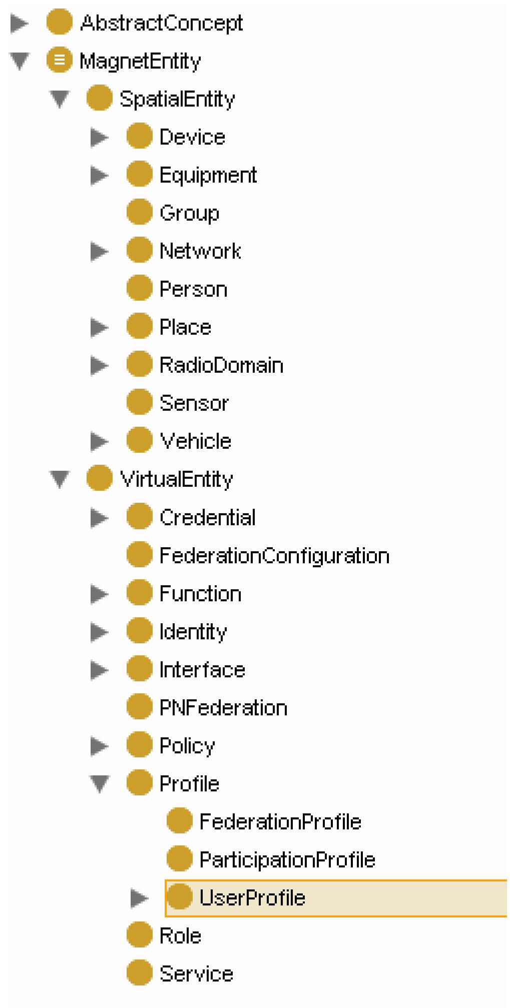


Figure 2: Overview of the Integrated Ontology

The *MagnetEntity* concept has two subconcepts, the *SpatialEntity* and the *VirtualEntity*. The *SpatialEntity* concept introduces the *hasLocation* property. The *VirtualEntity* concept comprises all types of entities that are not associated with a geographical location. *VirtualEntity* has a subconcept *Profile*, which in turn has a subconcept *UserProfile*.

The attributes of MAGNET Beyond entities are modeled as properties in the ontology. Properties can either have simple types supported as base types in the ontology such as String or Integer, or they can be complex types, in which case they are modeled as an AbstractConcept. The necessity of the usage of the AbstractConcepts can be figured out with the following example: In case the user profile contains a property "home address", there needs to be a complex structure for the whole address, as it is not sufficient to model street, post code, city, etc. separately. More specifically, the existence of multiple instances of home addresses in the same profile leads to the need of clear and unique correlation of the information to the corresponding address. On the other hand, modeling a property like address as a separate entity would have the effect that two subsequent requests would be needed for retrieving the information.

Figure 3 shows the complete BasicUserProfile, as defined in [MBD4.3.2, 07], and a part of the ExtendedUserProfile, which has the name FitnessCenterProfile and is related to a specific pilot service that has been implemented for the needs of the demonstration and evaluation process. Another pilot service named the "Icebreaker" is discussed in Section 4.1.

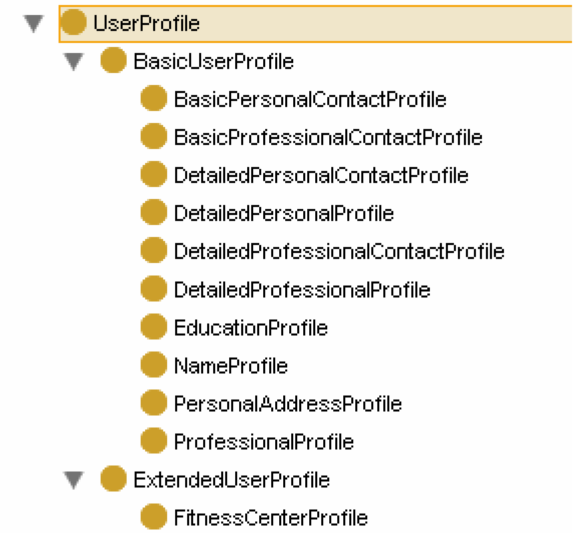
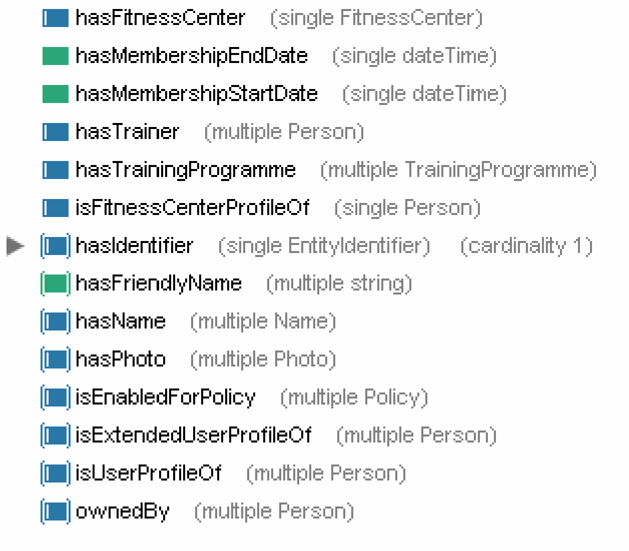


Figure 3: User profile part of the Integrated Ontology

As an example, the properties of the FitnessCenterProfile are shown in Figure 4. We also present the type of these properties and it can easily be observed that the hasTrainingProgramme property has the AbstractConceptTrainingProgramme as its type.



hasFitnessCenter (single FitnessCenter)
hasMembershipEndDate (single dateTime)
hasMembershipStartDate (single dateTime)
hasTrainer (multiple Person)
hasTrainingProgramme (multiple TrainingProgramme)
isFitnessCenterProfileOf (single Person)
hasIdentifier (single EntityIdentifier) (cardinality 1)
hasFriendlyName (multiple string)
hasName (multiple Name)
hasPhoto (multiple Photo)
isEnabledForPolicy (multiple Policy)
isExtendedUserProfileOf (multiple Person)
isUserProfileOf (multiple Person)
ownedBy (multiple Person)

Figure 4: Properties of the FitnessCenterProfile

3.3 Profile management framework

3.3.1 Description of the management framework implementation

As user profile and context information can be seen as two sides of the same coin with respect to the adaptation of applications and services, it makes sense to provide common functionality for handling this information. Therefore, the Secure Context Management Framework (SCMF) [Bauer et al., 06] [MBD2.3.2, 08] that has been developed in MAGNET Beyond manages both kinds of information in a uniform way and is used in order to store, exchange and manage securely all the above-mentioned information.

As a PN is a very dynamic environment, where the availability of nodes and network connections may be constantly changing, the SCMF was designed in such a way that the currently available nodes collectively provide the functionality and the data they can ensure. In an extreme case, this means that the SCMF is running on a single node, providing only the context and user profile information available locally. On each PN node a Context Agent is running. The interacting Context Agents on all the nodes in a PN together form the SCMF of the PN.

Figure 5 provides a high-level overview of the Context Agent. The core logic for evaluating requests is implemented in the Context Access Manager (CAM). In the storage of the Processing & Storage component (P&S) user profile information can be bestowed, whereas the Data Source Abstraction Layer provides a uniform access to local information from sensors, from the network, and the operating system. The Context Aware Security Manager (CASM) enforces privacy policies of the user, and only authorized information is thus provided, which is especially relevant when interacting with other users in a PN federation, as we explain below. The

Communication Module (NetCom) is responsible for the communication with other Context Agents.

Finally, the Context Management Inteface (CMI) implements the interface to the applications, which is based on a CALA language, encoded as XML over XML remote procedure call (RPC).

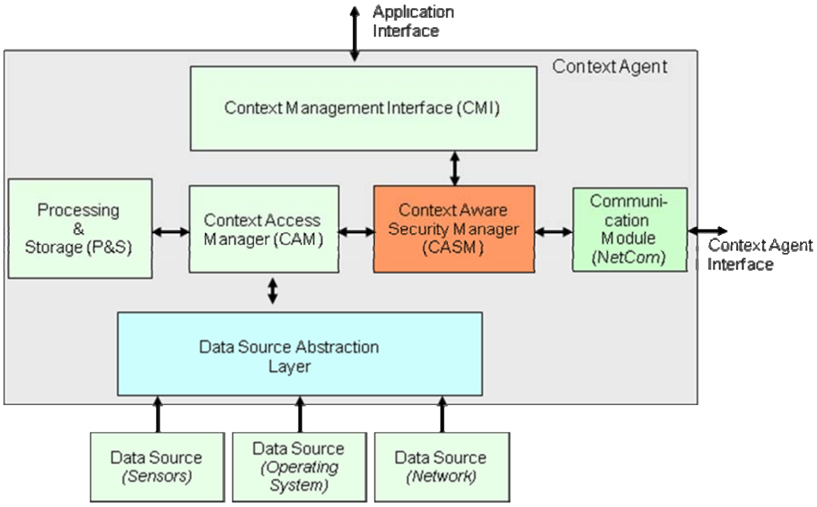

Application Interface
Context Agent
Context Management Interface (CMI)
Processing & Storage (P&S)
Context Access Manager (CAM)
Context Aware Security Manager (CASM)
Communi-cation Module (NetCom)
Context Agent Interface
Data Source Abstraction Layer
Data Source (Sensors)
Data Source (Operating System)
Data Source (Network)

Figure 5: Overview of a Context Agent with core components

Client applications use the interface for accessing context information, as well as inserting, updating and querying user profile information. Based on a scoping mechanism, they can limit the request to the local node, the cluster, the PN, PN-Fs, or external frameworks.

Figure 6 shows a setting with two PNs and one external MUP server. A PN can consist of one or more clusters shown by the dashed circles. A cluster typically comprises all personal nodes that are in proximity of each other, e.g. within wireless communication range. The PN connects these clusters using some interconnecting communication infrastructure. The context agents running on each node together form the SCMF of a PN. For the PN-F case, dedicated context agents act as Context Management Gateways (CMGs) between PNs to also allow context information sharing in PN-Fs.

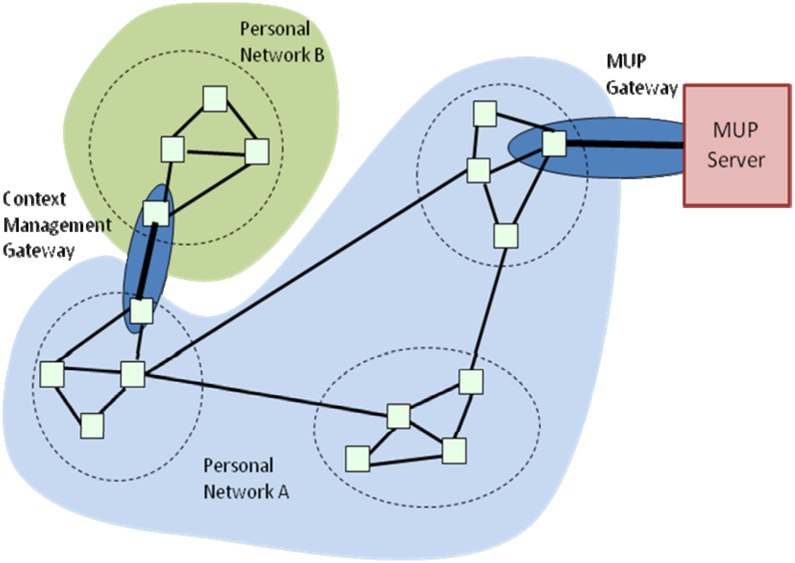


Figure 6: Example of a PN SCMF interacting in a PN-F setting with another PN and with an external MUP server

Thereby, the key functionality of the SCMF related to user profiles is its capability of storing the user profiles and making them available to all nodes in the SCMF, and, as we furthermore describe, the provision of a powerful and efficient access to user profile data distributed in the PN, when further coupled with an external MUP server.

3.3.2 Interfacing external frameworks

The SCMF targets the case where nodes in a PN have to rely on themselves. There are other scenarios where applications and services for a PN can profit from dedicated external frameworks. As far as user profiles are concerned, we have implemented an external MUP server in order to interact with the PN SCMF through a dedicated gateway. This is also shown in Figure 6.

Moreover, a centralized repository has been implemented for the MUP server, which manages both Basic and Extended User Profiles on a dedicated server infrastructure. The description of the corresponding profile schemata is based on an OWL-DL ontology. The prototype called MUP follows the GUP definition as described in [MBD1.2.1, 06], and the product is a complete Subscriber Data Management suite, called DataGrid, that handles the access to typical 3GPP data repositories, GUP and others from IMS and Internet service provider (ISP) worlds.

The MUP implemented in the project serves the following activities:

- Retrieval of User Profile data,

- Synchronization between the local and the remote instances of the Basic User Profile,
- Interface to query the OWL-DL ontology based on the standard SPARQL language (http://www.w3.org/TR/rdf-sparql-query/)
- Interface (Client) to manage specific user data based on the declarative CALA language to interact with the SCMF.

Figure 7 shows the overall architecture of the server that has been tested on a Linux configuration with MySQL.

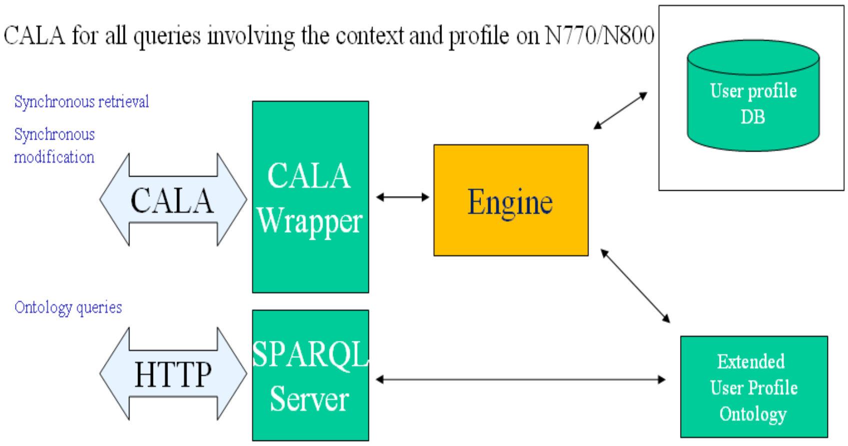


Figure 7: MUP Server – High Level Architecture

Beyond the presented example of the MUP Server, there are interesting opportunities in the combination of IMS, as a service delivery platform, with the radically new PN concept for providing user friendly and powerful new services. [Kovacs et al., 08] For example, the group management is an important IMS service enabler that can be used to access and manage XML documents in general, and contact lists or groups and their attributes in particular. OMA, Parlay, Internet Engineering Task Force (IETF) and 3GPP have specified group management functionality using different technologies such as web services (Parlay X), Session Initiation Protocol (SIP) or XML Configuration Access Protocol (XCAP) (IETF, OMA).

Concerning the access and usage of centralized groups in IMS from inside a PN, the benefits arise when the group information is not private but on the other hand shared by an organization or community. The architecture for inter-working is shown in Figure 8. The PN user application (on any device) initiates a query or updated operation that is forwarded to the context system. The latter communicates with the external IMS group enabler via a gateway to synchronize the information of the local (PN) and remote (IMS) storage system. The information is XML structured and the exchange follows the XCAP protocol.

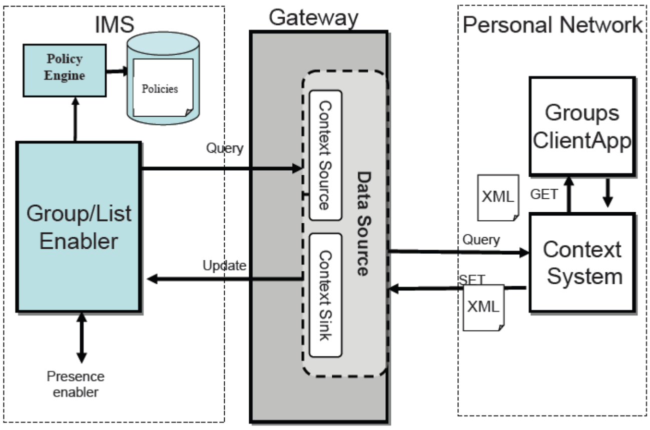


Figure 8: PN interactions with the IMS Group/Document Management Enabler

4 Platform evaluation and assessment results

4.1 Evaluation framework

When developing the Magnet Beyond platform a lot of focus was put on user centricity. As a result, the evaluation phase has also been based on usability and user experience tests of the pilot services within one MAGNET scenario.

All the pilot services that were designed and implemented for the evaluation phase of the MAGNET Beyond architecture and, especially, the one called “Icebreaker” depend highly on the user profile information. The infrastructure that was previously presented was used for the realization of the pilot services so as to provide to the users a real testbed for comprehension of the whole architecture. The MAGNET software had been installed on the mobile web tablets Nokia N770 and N800, and the users experienced through them the pilot services according to the predefined scenarios.

The “IceBreaker” is a service, which is offered to facilitate the collaboration between visitors, organizers and presenters in an event. This becomes possible with the establishment of PN-Fs between people previously unacquainted, who are located in an event area, through a matching service based on their user profiles and context. This service has been designed and implemented in order to take advantage of the user profile information so as to provide application for the socialization of the user, based on his/her individual characteristics which are depicted in his/her corresponding user profile information.

When the service is started, it subscribes to the SCMF so as to query and download the user profile information which in fact plays a fundamental role to the subsistence of the service. The interface used is XML-RPC, and the CALA queries embody the corresponding parts so as to collect personal and professional information from the basic and extended part of the user profile located in the databases.

The Graphical User Interface (GUI), shown in Figure 9, includes a button which is labeled “My Profile”, and which offers the ability to check the user’s profile and/or update it with new information. Moreover, the user can define his/her matching criteria ("Matching" button) based on the profile information that he/she wants. The matching criteria include fields that refer to personal or professional desired characteristics which are, as soon as they are defined, sent to the matching server in order to be compared with the registered user profiles. Thereinafter, the users are prompted with the Virtual Badges (VB) of the matched users. The VB consists of the PN identifier, the name and a photograph of the user. The users can then modify their Business cards (BC), using the "My Card" button, and also exchange them. The BC is filled with information that is available in the DetailedProfessionalProfile and has the following relevant attributes: hasName (Name), hasJobTitle (Job title), hasCompany-Name (Company), hasEducationalLevel (Education), hasOfficeAddress (Address), hasProfessionalContactInformation (Telephone number and Email). This information is also retrieved from the user profile, which is located in the SCMF.

As it can be concluded from the above description, the Icebreaker pilot service is meant to provide digital facilities for mobile users and thus is strongly based on the user profile information.

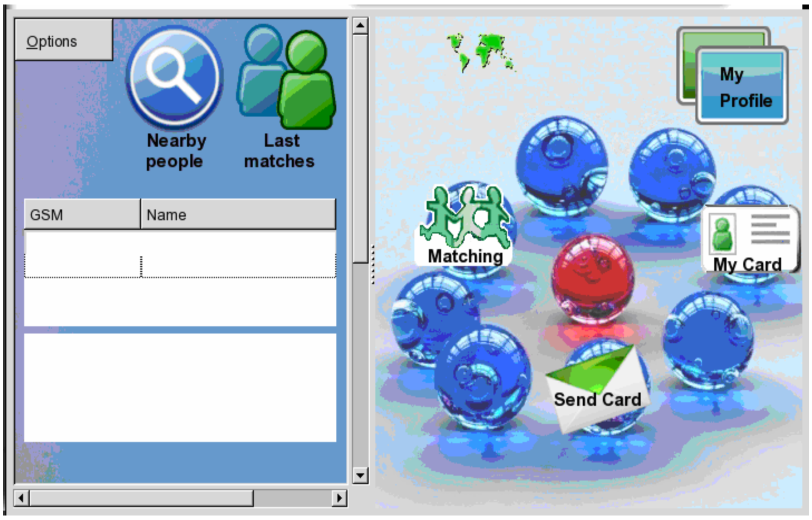


Figure 9: Icebreaker GUI

4.2 Trials involving real users

The testing procedure, the usability testing and the audit presentation of the Magnet Beyond architecture via the pilot services and especially the Icebreaker, was done in order to verify its functionality in user environments so as to provide feedback on the performance of the implemented proposals.

The critical testing criteria and parameters that were decided in advance and gave good insight into the functions and performance achieved are listed below:

- Response time,
- Error messages,

- Help functionalities,
- Information messages and
- Overall functions outcome.

So as to keep track of users' actions and performance time, the electronic data logging was used. Every time a user clicked a button, or generally whenever an event listener was called, a line containing the time, the date stamp and the action name was stored in a file. After that, the log information was analyzed and statistical results were extracted.

A complete set of basic tests were carried out in order to evaluate the performance of the platform in real life conditions. They include:

- Creation/Modification/ Deletion of a new basic user profile (MUP).
- Creation/Modification/ Deletion of a new extended user profile (MUP).
- Query/Modify to a basic or extended user profile.
- SCMF interaction (Retrieval, modification, upload of information).
- Business cards exchange via magnet networking facilities.

However, a detailed reference to the results of all tests is out of the scope of this paper. A complete report of the results has been provided in the corresponding evaluation report deliverable of the MAGNET Beyond project [MBD1.4.3, 08]. Afterwards, we present a reference to the results that are of interest in the context of the paper.

4.3 Evaluation Results- Findings

The users' evaluations of the system and the service indicated that concepts such as PNs and PN-Fs are generally accepted as a suitable way of structuring the connections between people, whenever a user wants to exchange information and data.

The PN management modules such as the SCMF and MUP server were considered as background applications, which should satisfy the user's sense of control as far as his/her personal data are concerned. Privacy and security issues should always be taken into account, as it was made clear that the users wanted to be in charge of what was shared in almost any case, apart from emergency occasions.

User profiles were well accepted by users, but concerns were raised, regarding the user's ability to control what was shown to others and potential logged history. It was important for the users that they had to approve any changes, before they were made, and also any possibility of information storage. The use of extended/basic profile and virtual ID and identities was not easy for the users to understand.

To summarize all the above and conclude with, we realize from the evaluation results that the users considered that the implemented system based on the proposed architecture is a complete and secure system platform [MBD1.4.3, 08].

Apart from the successful tests covering the operation of the MAGNET Beyond system, the corresponding tests regarding the interaction between the system's components and the Icebreaker service were also successful, and delivered to the users the desirable attitude in a sensible response time with appropriate messages or notifications about the system processes.

Hereby, the only concern that was raised, regards issues that are related to the scalability of the system so as to handle growing amounts of work in an efficient manner and to respond adequately in reasonable time under an increased load when resources are added. However, as the system is oriented towards the coverage of user needs in a personalized network, scalability issues are reduced to the level of PN support, issues that have already been addressed and lead to the production and commercial distribution of PN servers (i.e. Bluetooth servers supporting a diverse set of data including streaming media).

5 Conclusions – Future Work

The different proposals originating from both the telecom and web initiated activities, converge to a unique picture, including not only personal (static) information about the user but also data that are dynamic and correspond to all aspects of his/her activities and deployed resources. In this direction, context awareness including location, time, status, environmental parameters as well as resource usage information including devices and accessories will play an important role in the user profiles.

The work performed in MAGNET Beyond that we present in this paper, provides the framework for the definition of a clear standard towards user profiles that incorporate context-aware information management and thereby realizes a platform, which is capable of handling and delivering personalized context-aware services to users through an attempt to interface the PN framework with that of IMS. Of course, the unification of the existing proposals requires further work in order to present a core standardization proposal for user profile management which will not only deliver adequately personalized services to end users, but will also gain their trust.

Acknowledgements

The authors of this paper would like to thank all the participants of the IST FP6 project MAGNET Beyond for their contribution and support, which has assisted in the preparation of this paper.

References

[Aguiar et al., 06] Aguiar, R., Einsiedler, H., Karrer, R.: “Daidalos – The operator's vision of the next-generation Internet”, Proceedings of the Infocom 2006, Barcelona, Spain, April 23-29, 2006.

[Bauer et al., 06] Bauer, M., Olsen, R. L., Jacobsson M., Sanchez, L., Lanza, J., Imine, M., Prasad., N.: “Context Management Framework for MAGNET Beyond”, Proceedings of the 15th IST Mobile & Wireless Summit Communications Summit, Myconos, Greece, 2006.

[Camp, 04] Camp, L. Jean: “Digital Identity”, IEEE Technology & Society, 23, 3, 34–41, 2004.

[Chen, 07] Chen, Zhikui: “A Scenario for Identity Management in Daidalos”; Proceedings of CNSR '07, Fifth Annual Conference on Communication Networks and Services Research, New Brunswick, Canada, 2007.

[DAIDALOS, 06] IST FP6 Integrated Project Daidalos: http://www.ist-daidalos.org.

[Dey, 00] Dey, A. K.: “Providing Architectural Support for Building Context-Aware Applications”, PhD thesis, Georgia Inst. Tech., USA, 2000.

[ETSI, 05a] ETSI Guide: "Human factors (HF); User profile management", EG 202 325 v1.1.1, 2005.

[ETSI, 05b] ETSI Guide: "Universal Mobile Telecommunications System (UMTS); Service Requirements for 3GPP Generic User Profile (GUP)", Stage 1 (3GPP TS 22.240 Release 6), Stage 2 (3GPP TS 23.240 Release 6), Stage 3 (3GPP TS 29.240 Release 6), 2005.

[ETSI, 09a] ETSI Guide: "Human Factors (HF); Personalization and User Profile Management; User Profile Preferences and Information", ETSI draft standard ES 202 746, Retrieved May 3, 2009, from http://portal.etsi.org/stfs/STF_HomePages/STF342/ES_202_746_V16.doc.

[ETSI, 09b] ETSI Guide: "Human Factors (HF); Personalization and User Profile Management; Architectural Framework", ETSI draft technical specification TS 102 747, Retrieved Feb. 4, 2009, from http://portal.etsi.org/stfs/STF_HomePages/STF342/draft_TS_102_747_V21.doc.

[Golemati et al., 07] Golemati, M., Katifori, A., Vassilakis, C., Lepouras, G., Halatsis, C.: "Creating an Ontology for the User Profile: Method and Applications", Proceedings of the First IEEE International Conference on Research Challenges in Information Science (RCIS), Morocco, 2007.

[Gomes, 06] Gomes, D., Aguiar, R.: "Privacy through Virtual Hording", Proceedings of the Globecom 2006, San Francisco, USA, December, 2006.

[ITU-T, 04] ITU-T Y.2011: "General principles and general reference model for next generation networks", 2004.

[Jørstad, 06] Jørstad, I., van Do, T., Dustdar, S.: "Personalization of Next Generation Mobile Services", Proceedings of the 4th International Workshop on Ubiquitous Mobile Information and collaboration Systems (UMICS), co-located with CAiSE 2006, Luxemburg, 2006.

[Kovacs et al., 08] Kovacs, E., Kraft, D., Cimmino, A., Bessler, S., Ghader, M., Gavrilovska, L.: "Personal Networks as Distributed Clients for IMS", Proceedings of the ICT-MobileSummit 2008 Conference, Stockholm, Sweden, 10-12 June 2008.

[Lo et al., 06] Lo, A., Jacobsson, M., Prasad, V., Niemegeers, I. G.: "Personal Networks: An Overlay Network of Wireless Personal Area Networks and 3G Networks", Proceedings of the Third Annual International Conference on Mobile and Ubiquitous Systems: Networking & Services, San Jose, California, 2006.

[MAGNET Beyond, 06] IST FP6 Integrated Project MAGNET Beyond: http://magnet.aau.dk/.

[MBD1.2.1, 06] Olesen, H. (ed.): "The conceptual structure of user profiles", IST-027396 MAGNET Beyond deliverable, Sept. 2006, Retrieved June 16, 2009, from http://www.magnet.aau.dk/public+deliverables.

[MBD1.4.3, 08] Schultz, N. (ed.): "Usability testing of pilot services", IST-027396 MAGNET Beyond Deliverable D1.4.3, June 2008, Retrieved June 16, 2009, from http://www.magnet.aau.dk/public+deliverables.

[MBD2.3.2, 08] Jacobsson, M. (ed.): "MAGNET PN secure networking frameworks, solution and performance", IST-027396 MAGNET Beyond Deliverable D2.3.2, Sept. 2008, Retrieved June 16, 2009, from http://www.magnet.aau.dk/public+deliverables.

[MBD4.3.2, 07] Kyriazanos, D., Olesen, H. (eds.): "Specification of user profile, identity and role management for PNs and integration to the PN platform", IST-027396 MAGNET Beyond Deliverable D4.3.2 (D1.2.2), March 2007, Retrieved June 16, 2009, from http://www.magnet.aau.dk/public+deliverables.

[Niemegeers et al., 02] Niemegeers, I. G., Heemstra de Groot, S.: “From Personal Area Networks to Personal Networks: A user oriented approach”, Journal on Wireless and Personal Communications, 22, 175-186, 2002.

[Olivereau et al., 05] Olivereau, A., Gómez Skarmeta, A., Lopez, R., Weyl, B., Brandao, B., Mishra, P., Hauser, C.: “An advanced Authorization Framework for IP-based B3G Systems”, Proceedings of the 14th IST Mobile and Wireless Communications Summit, Dresden, Germany, June 19-23, 2005.

[OpenSocial API, 08] OpenSocial API Specification v0.7, 2008, Retrieved May 27, 2008 from http://code.google.com/apis/opensocial/docs/0.7/spec.html.

[Pinheiro et al., 08] Pinheiro, M. K., Villanova-Oliver, M., Gensel, J., Berbers, Y., and Martin, H.: “Personalizing Web-Based Information Systems through Context-Aware User Profiles”, Proceedings of the Second international Conference on Mobile Ubiquitous Computing, Systems, Services and Technologies - Volume 00, UBICOMM, IEEE Computer Society, Washing-ton, DC, 231-238, 2008.

[W3C Recommendation, 04] W3C Recommendation: “Composite Capabilities/ Preference Profiles (CC/PP): Structure and Profiles 2.0”, 2004, Retrieved May 15, 2007 from http://www.w3c.org/Mobile/CCPP.

[WWRF, 09] Olesen, H., Noll, J., Hoffmann, M. (eds.): “User profiles, personalization and privacy”, WWRF Outlook series, Wireless World Research Forum, May 2009, Retrieved June 16, 2009, from http://www.wwrf.info/fileadmin/sites/default/files/publications/Outlook/Outlook3.pdf

[Youngjung et al., 05] Youngjung, Suh and Woontack, Woo: “User Profile Management for Context-aware Applications in ubiHome Environment”, IPSJ SIG Technical Reports, 60, 281-286, 2005.

[3GPP TR 32.808] 3GPP Technical Specification Group Services and System Aspects TR 32.808: “Study of Common Profile Storage (CPS) Framework of User Data for network services and management (Release 8)”, Version 8.0.0, June 2007.

[3GPP TS 24.259] 3GPP Technical Specification, 3GPP TS 24.259: “Personal Network Management (PNM); Stage 3”, version 8.1.0, Release 8, Mar. 2009.