The role of user profiles in PN services and context awareness

deliverable D1.2.3, IST project MAGNET Beyond (My personal Adaptive Global NET and Beyond)

Olesen, Henning; Hammershøj, Allan; Olsen, Rasmus Løvenstein; Fleury, Alexandre; Cimmino, Antonio; Bessler, Sandford; Bauer, Martin; Patrikakis, Charalampos Z.; Nikolakopoulos, Giannis; Thuvesson, Henrik

Publication date:
2008

Document Version
Publisher's PDF, also known as Version of record

Project no.:	**IST-027396**
Project full title:	**My Personal Adaptive Global NET and Beyond**
Project Acronym:	**MAGNET Beyond**
Deliverable no.:	**D1.2.3**
Title of the deliverable:	**The role of user profiles in PN services and context awareness**

Contractual Date of Delivery to the CEC:	30th June 2008
Actual Date of Delivery to the CEC:	30th June 2008
Author(s):	**H. Olesen**. A. Hammershøj, R. L. Olsen, A. Fleury (AAU), A. Cimmino (ALA), S. Bessler (FTW), M. Bauer (NEC), C. Patrikakis, G. Nikolakopoulos (NTUA), H. Thuvesson (TS)
Participant(s):	AAU, ALA, FTW, NEC, NTUA, TS
Work packages contributing to the deliverable:	WP1, WP2
Est. person months:	4 mm
Dissemination level:	PU
Nature:	P
Version:	1.0
Total number of pages:	60

Abstract:

This deliverable is the final report on the development and application of user profiles in MAGNET Beyond. The profile structure, the Virtual Identity (VID) concept and the common ontology for user profiles and context information are presented. Management of user profiles in the PN architecture is discussed, including the MAGNET User Profile (MUP) server for access to foreign services, and the actual utilization of user profiles in the pilot services is described. The concept of activities is shown to be a useful approach for GUI adaption and personalization, which should be further developed. The potential of the user profile for service adaptation and control of resource sharing is highlighted, and several future business opportunities based on user profiles are discussed.

Keyword list: User profile, identity, Virtual Identity, user preferences, context, context awareness, ontology, privacy, access control, identity management, personalization, profile management, activity, access policies, policy engine, Personal Networks, Personal Network Federation, service providers, Generic User Profile, Liberty Alliance, IMS, 3GPP, subscriber data management

Table of contents

EXECUTIVE SUMMARY **4**

1 INTRODUCTION **5**

2 MODELLING OF USER PROFILES **6**

2.1 DEFINITIONS 6
2.2 USER PROFILES AND CONTEXT INFORMATION IN MAGNET BEYOND 6
2.2.1 Personalization and service adaptation *6*
2.2.2 Different PN scenarios *7*
2.3 OVERVIEW OF THE STRUCTURE OF USER PROFILES 9
2.4 VIRTUAL ID AND SUPPORT FOR PN SERVICES 11
2.5 USER PROFILES IN PN FEDERATIONS 13
2.6 COMMON ONTOLOGY FOR USER PROFILES AND CONTEXT INFORMATION 16

3 USER PROFILE MANAGEMENT **19**

3.1 SCMF AND THE PN SERVICE ARCHITECTURE 19
3.2 ACCESS CONTROL TO USER PROFILES AND MANAGEMENT OF TRUST RELATIONS 20
3.2.1 Option 1: Policy Decision and Enforcement using the CASM entity *21*
3.2.2 Option 2: Policy Decision using the semantic policy engine (PE) *22*
3.3 INTERFACE TO AN EXTERNAL, CENTRALIZED GENERIC USER PROFILE 23

4 APPLICATION OF USER PROFILES IN SELECTED PILOT SERVICES **27**

4.1 THE ICEBREAKER SCENARIO 27
4.2 THE GYM SCENARIO 29
4.2.1 The user profile *30*
4.2.2 Interaction pattern with bicycle and profile storage *31*
4.2.3 Interaction with the scale *32*
4.2.4 Distance collection and notifications *33*
4.3 THE PRESENTATION SERVICE 34
4.4 THE ACTIVITY CONCEPT AND ASSOCIATED GUIS 35

5 FUTURE PERSPECTIVES **40**

5.1 STANDARDIZATION WORK ON USER PROFILES 40
5.1.1 ETSI *40*
5.1.2 3GPP *40*
5.1.3 OMA *40*
5.1.4 W3C *41*
5.1.5 OpenSocial Foundation description *41*
5.1.6 Conclusion *41*
5.2 FUTURE APPLICATIONS OF USER PROFILES 42
5.2.1 Modalities (MODs) *42*
5.2.2 PN Service Creation Environment using MODs *42*
5.2.3 Environment interactions *44*
5.2.4 Privacy and protection for the end users *45*
5.3 FUTURE BUSINESS OPPORTUNITIES 46
5.3.1 Provisioning of PN services and user profile administration *46*
5.3.2 Pilot services *49*
5.3.3 IMS Group Management *50*
5.3.4 Offering personalized and blended services *50*

6 CONCLUSIONS 54
REFERENCES 55
ABBREVIATIONS 57
LIST OF FIGURES 59

Executive summary

This deliverable reports the status of user profiles in the PN architecture at the end of the MAGNET Beyond project. It reviews the overall structure of the user profile and the common ontology for user profiles and context information, which has been developed. It also describes the management framework for this information, aiming at two main cases: PN Federations and interaction with foreign services. Some of the key elements are the Secure Context Management Framework (SCMF) and its Processing and Storage (P&S) module, the policy engine, and the MAGNET User Profile (MUP) server. The concept of Virtual Identities (VIDs) is also enabled and facilitated by the management framework.

The MUP server is an adapted version of the 3GPP Generic User Profile (GUP) approach [3GPP GUP], aiming at handling user profile specific tasks in a PN towards other users or service providers, where the user already has defined the policies to handle the different situations. The MUP architecture is created to basically take the processing load of the user's devices, which in many cases are battery-powered mobile devices. The MUP server is also designed with the purpose of being the server, where an updated user profile can be temporarily stored, when user sessions are transferred between different devices in the PN.

In most chapters of this deliverable we focus on the final target system of MAGNET Beyond and how the concepts are foreseen to be implemented and working. Even though parts from the PN architecture are fully described in the document, the underlying software components do not necessarily support all functionality. An example is the ontology for the user profile, which is well defined and implemented but not fully enabled in the pilot services due to limitations in other middleware components. The parts of the user profile, which are enabled in the various pilot services, are described in Chap. 4. All in all, we describe how user profiles have been applied in the pilot services and discuss ideas for future extensions of the work, in particular the issues of incorporating intelligence and learning in the user profile and context management framework, and the prospects for performing advanced context-aware personalization and service adaptation.

1 Introduction

MAGNET Beyond[1] has developed a comprehensive framework for managing user profiles, context information and security. The conceptual structure of the user profile has been developed in Task 1.2, but we have put emphasis on integrating the user profiles into the overall enabling framework of PN services to maximize the benefits of user profiles. The first deliverable, D1.2.1, "The conceptual structure of user profiles" [MBD1.2.1], was completed as a joint cross-WP deliverable (as foreseen in the Technical Annex), and this contributed significantly to achieving a common view and consensus within the project. The cross-WP collaboration was continued, and it was proposed and agreed to merge 2 deliverables, D1.2.2 and D4.3.2, into a single deliverable named D4.3.2, "Specification of user profile, identity and role management for PNs and integration to the PN platform" [MBD4.3.2]. This deliverable was completed just before the start of the pilot services in Task 1.3 and formed the basis for applying the proposed concepts and building blocks in the pilot service implementation.

In order to fully describe the role of user profiles in the context of MAGNET Beyond, and especially in the deployment of PN context-aware services, the consortium has studied the existing state-of-the-art approaches in user profile definition. The impact of both telecom-oriented approaches (such as ETSI and 3GPP recommendations) and web-oriented initiatives (W3C, OpenSocial) have been taken under consideration, in parallel with the particularities that the Personal Networking environments present. The result is a comprehensive framework, both in terms of definition and management of user profiles, but also the implementation of user profiles in selected pilot services. Issues of importance such as trust and security are also addressed in this deliverable, while following the application of user profiles, the document advances in presenting future perspectives for the deployment of user profiles focusing on future applications, and business opportunities, with respect to privacy and personal information protection.

In general, there are 2 time horizons in the project:

- the **pilot services**, which represent the actual implementation of the PN architecture with building blocks, enablers and selected applications for demonstration. Naturally, due to limited resources, these are only showing a subset of the functionality, which have been selected to demonstrate the overall potential of the PN concept. The underlying system is also a partly implemented version of the final target system as defined in [MBD1.1.1].
- the **target system**, which represents the status at the end of the project and contains several ideas, concepts and suggestions for future work.

Both of these are covered in this deliverable, but most of the chapters focus on the target system.

The deliverable is organized as follows: Chapter 2 presents an overview of the modelling of user profiles, the concept of Virtual Identities (VIDs), and the common ontology that has been developed for user profiles and context information. In Chapter 3 we describe the management of user profile information in the PN, in particular the Secure Context Management Framework (SCMF) and the MAGNET User Profile (MUP) server that has been developed in the project to link to the operator's domain and facilitate access to foreign services. Chapter 4 describes how user profiles have been incorporated and used in selected pilot services, including the activity concept and the GUIs. Finally, in Chapter 5 we position the work on user profiles in MAGNET Beyond in relation to other ongoing activities and discuss the business potential of user profiles together with ideas for future work, and Chapter 6 gives the conclusions of the work.

[1] MAGNET Beyond is the follow-up project of the initial IST MAGNET project (2004-2005), and it builds on ideas, concepts and solutions from that project. Throughout this deliverable we shall primarily refer to the results developed in MAGNET Beyond. However, for simplicity, we will occasionally use terms like: MAGNET-enabled users, MAGNET user profile, MAGNET GUIs, etc., even though the results originate from MAGNET Beyond.

2 Modelling of user profiles

2.1 Definitions

From the previous deliverables [MBD1.2.1], [MBD4.3.2] we repeat the definitions of user profiles and context:

- **User Profile**: the total set of user-related information, preferences, rules and settings, which affects the way in which a user experiences terminals, devices and services. [ETSI 2005a]
- **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. [Dey00]

In this deliverable we put focus on the added value, which is provided by the user profile (together with the context information), and we discuss how this has been implemented in the pilot services as well as ideas for future work.

2.2 User profiles and context information in MAGNET Beyond

The work on user profiles is seen as an essential part of the general Personal Network (PN) framework. Being equipped with a PN, the users are empowered and assisted in carrying out their tasks under varying conditions in their everyday life. The objective is to take advantage of knowing the user's preferences, the context of the user and any other relevant information to optimize services for the user in any given situation. This must be done while safeguarding the user's privacy and keeping the user in full control of his or her resources and personal information.

To be able to make better use of services, especially in situations where the user is on the move, has his focus on other activities, or has a device with limited input/output capabilities, the services need to adapt to the situation and how the user typically uses the service, most likely as a combination of both, i.e., how the user uses the service in a given situation. The information to adapt the services in this way can be found in the user profile and the context information, which can be seen as two sides of the same coin, as both are needed to adapt the service for providing a better user experience. Therefore, it also makes sense to use the same middleware for making them accessible, which is why we decided in MAGNET Beyond to store user profile in the Secure Context Management Framework (SCMF) and use the same mechanisms to access the information.

The SCMF is the key element within the PN, which acquires and stores the user profile and context information and controls the access to this information and the sharing of personal resources. This has been described extensively in previous deliverables [MBD1.2.1], [MBD4.3.2] and is briefly reviewed in Sect. 3.1.

2.2.1 Personalization and service adaptation

Services can be adapted in different ways to user profile and context information. In the following, we list some examples:

- The information presented to the user can be adapted based on profile and context information, e.g., relevant information may be different when the user is at work or at home, and again different when the user is on a trip, e.g., present the local weather, possibly in addition to the weather at home.
- How the information is presented may differ according to the situation, preferences, and the device available. For example, navigation information could be displayed differently on a PC than on a mobile phone, and also differently depending on the situation of the user, whether she is standing or running, in which case the output could be reduced to easy-to-grasp arrows.

- Available services may be pre-configured with parameters used in the past or which are relevant in the current situation, e.g., the wake-up call in a hotel could be preconfigured to the room of the user.
- Services may be executed automatically depending on the user profile and the situation, e.g., calling a doctor in an emergency situation.

In the general case, it is a complex undertaking to decide which part of the entire available user profile and context information that is relevant and useful for performing service adaptation. Organizing the information in an ontology (cf. Sect. 2.6) is a step on the way, as it supports reasoning and decision-making, but there is a lot more research to be done on how to combine this with intelligent application logic and policies that provide a proper protection of user privacy.

2.2.2 Different PN scenarios

Two main scenarios are considered throughout the project:

- PN Federations (PN-Fs), which can be seen as an advanced, well-controlled peer-to-peer interaction between two or more users within the same or different domains, and
- Access to foreign or 3rd party services, where improved personalization and service adaptation is facilitated by the PN.

In the PN-F scenario, Figure 2-1, the user has full control over the resources that he or she wants to share with the federation in order to achieve the common goal of the federation, in other words avoiding exposing or revealing more personal information and content than needed. More details about PN-Fs are given in Sect. 2.5 below.

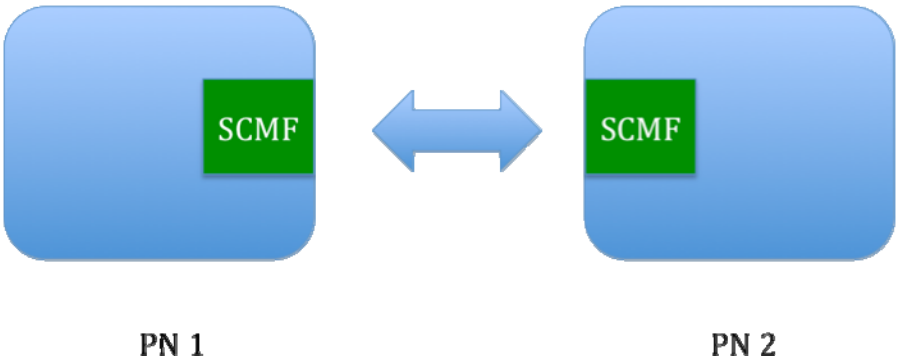


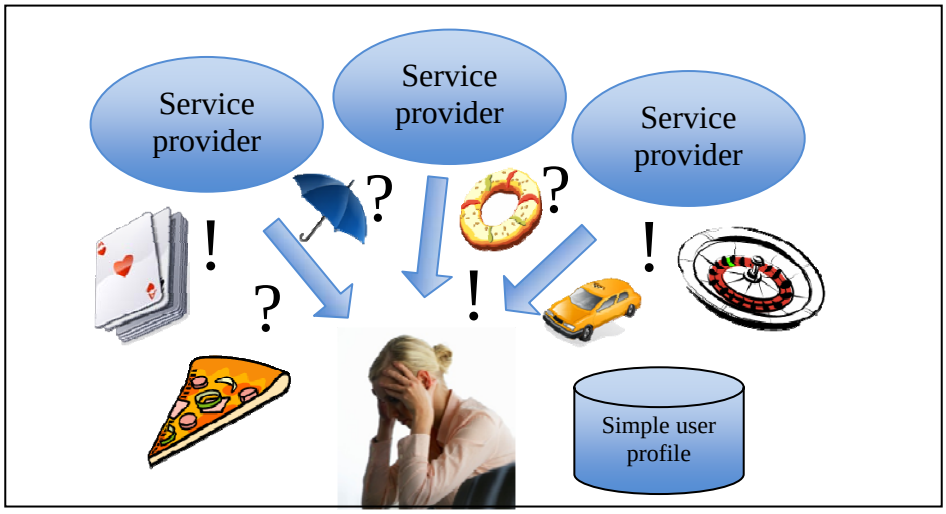
Figure 2-1: Basic PN-F scenario.

In case of accessing foreign services (push or pull type), a MAGNET-enabled user also has much better control of the personal information and can decide where the right balance lies between protection of privacy and revealing of personal information. Today, a large number of web sites offer users or subscribers a basic level of personalization, cf. Figure 2-2a. This can be initiated, when the user signs up for the first time, where typically a set of personal data such as name, address, e-mail address, phone number(s) etc. may be requested, and the user chooses a user-ID and password to access the personalized services later on. Furthermore, the user is often given the option of ticking various preferences or areas of interest.

More sophisticated services will collect data about the usage history and based on this perform some "intelligent" processing in order to provide relevant information or offers to the user.

Today, the large number of 3rd party profiles have to be handled independently by the user, and the personalization benefits are somewhat limited.

a)



b)

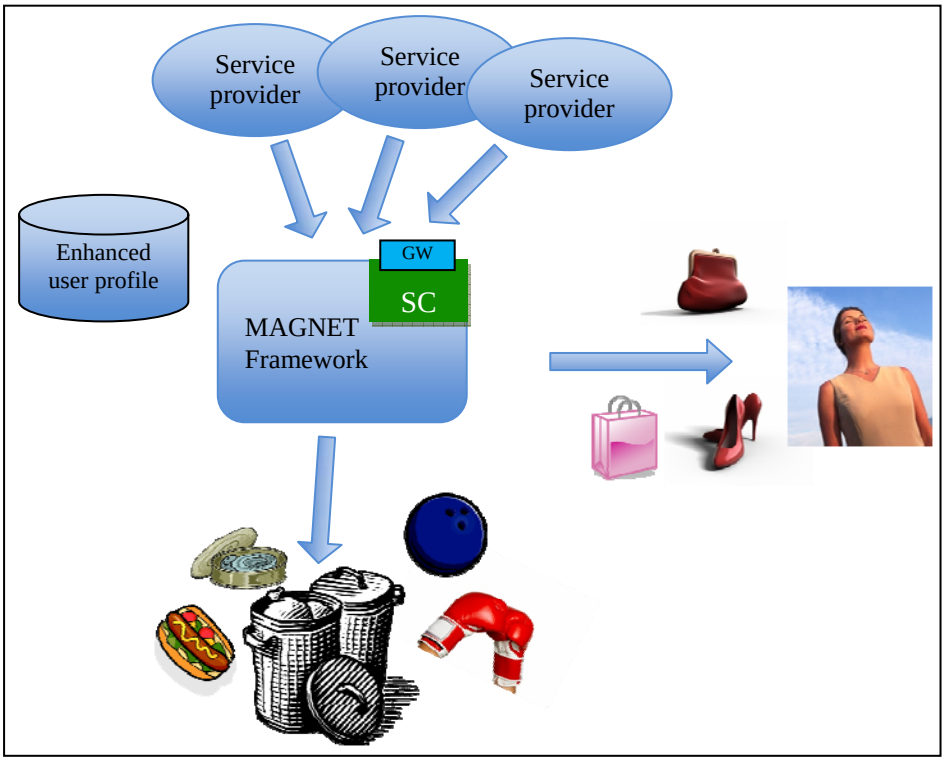


Figure 2-2: Access to third party services. a) Basic personalization targeting a standard user. b) Enhanced personalization targeting a MAGNET-enabled user.

For a MAGNET-enabled user, Figure 2-2b, we may envision that the service provider will be informed when dealing with a "more sophisticated" user, which in turn will enable a better personalization. The template of the user profile might be publicly available, so a service provider would know, what kind of personal information is *potentially* available, and hence be able to query the user for a certain part of this. However, the information may not have been filled in, or it may not be accessible because of the policies attached to the user profile. But if the information can be accessed, the service provider can use it to customize or personalize the service to this particular user. The MAGNET framework can assist the user in filtering and navigating huge amounts of contents, services and offerings. This provides better value for the user and better revenue options for the service provider. To fully take advantage of the PN, a service provider would need to adapt services significantly, but some

benefits of PNs in terms of personalization and service adaptation are readily available as discussed above.

As the name implies, Personal Networks are personal, i.e. they belong to a user, and there is only one user in a PN. However, users often deal with "non-personal" networks or collections of resources, e.g. facilities in an office environment or in a conference centre. Instead of being personal these resources may belong to the premises, and they are typically managed by a system administrator. In order to extend the management framework of MAGNET Beyond to cover such cases as well, we have introduced to concept of a **Service Provider Network (SPN)** [MBD4.3.2, Chap. 6.2]. We can then apply similar procedures to govern access to and sharing of resources between a user's PN and an SPN as in a PN-F between two or more users.

2.3 Overview of the structure of user profiles

In accordance with the definition in Sect. 2.1, a user profile is a record of preferences, rules, settings and other relevant user information that are saved and changed dynamically so as to provide the appropriate personalized behaviour to the device, the services and the whole PN. Dynamics of the PN composition is very important when devices and services come and go.

As described in the previous deliverable [MBD4.3.2, Chap. 4] and shown in Figure 2-3, the user profile can be structured in a tree and consists of several subcomponents that are placed throughout the PN and accessed through the "User profile" subcomponent, which contains references to the other subcomponents. The fundamental subcomponents of the user profile are the following:

- Basic profile
- Extended profile
- Device profiles
- PN-F profiles
- 3rd party profiles

The **basic profile** component of the user profile contains the basic information about the user and is divided in three major parts:

- Personal user information, based on user related data
- Professional user information, addressing professional issues of identity and preferences
- Comportment, related to the way the user experiences working and interacting with the personal devices [MBD4.3.2]

The **extended profile** includes generic user settings and preferences that are based on the individuality of a user, but 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 profile** information includes information about device-specific settings, preferences and characteristics. It also contains numerous references to online resources.

The **PN-F profile** (see Sect. 2.5) 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, while the PN-F participation profile contains information and preferences about each specific member. Strictly speaking, only the participation profile is part of the user profile.

The **3rd-party** part of the user profile contains preferences and information that the 3rd party service provider needs to store in the user profile.

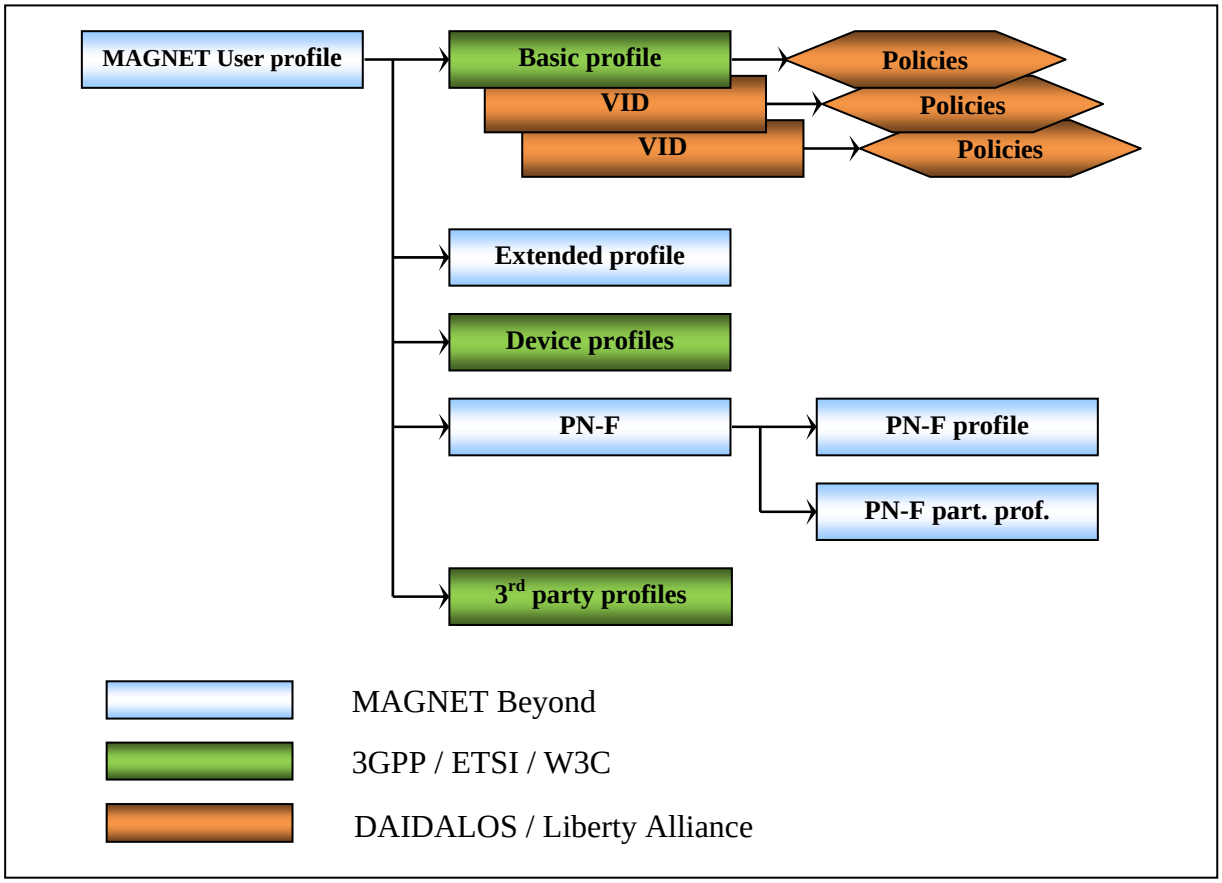


Figure 2-3: MAGNET user profile in a conceptual representation displaying the different categories and dependencies [MBD4.3.2], compared to state-of-the-art.

Previous work done on user profiles was probably missing an important requirement, namely the formation of federations of user communities, which care about all personal clusters and devices linked with them. The user centricity is expanded to such a dimension that the user becomes an entire communication cluster made by the user himself with his personal resources (devices, personal clusters and personal federations). The research in MAGNET Beyond ended up with an expansion and enhancement of existing user profile ontologies, and the project has highlighted the key aspects behind the definition of an innovative user profile, which can cope with requirements such as:

- Heterogeneity of access, communication infrastructures and domains
- Multi-device scenarios
- Personal Networking
- Federations of PN user communities
- User centricity
- Personalisation
- Preferences
- 3rd party services & access policies.

Most of the above requirements, apart from the PN-related ones, are to some extent already discussed and proposed in 3GPP [3GPP GUP], Liberty Alliance [Liberty], W3C and the DAIDALOS project[2].

[2] http://www.ist-daidalos.org

As already described in [MBD1.2.1], instead of defining a new user profile concept, the approach has been to extend existing architectures defined in these other projects or standardization bodies and adapt them to match the PN scenarios. Figure 2-3 compares the various parts of the MAGNET user profile with existing standardization approaches, and the proposed structure can thus be seen as an evolution of existing scientific or industrial approaches in defining user profiles towards a global profile including personalisation and federation concepts. More details on ongoing standardization activities are given in Sect. 5.1.

2.4 Virtual ID and support for PN services

The concept of virtual identity (VID) is a way for the user to be presented to the outside world from a security point of view. As already stated, it was defined and described in the project DAIDALOS and continued in DAIDALOS II, and it was decided to adopt and further develop it in MAGNET Beyond [MBD4.3.2], [MBD4.3.3].

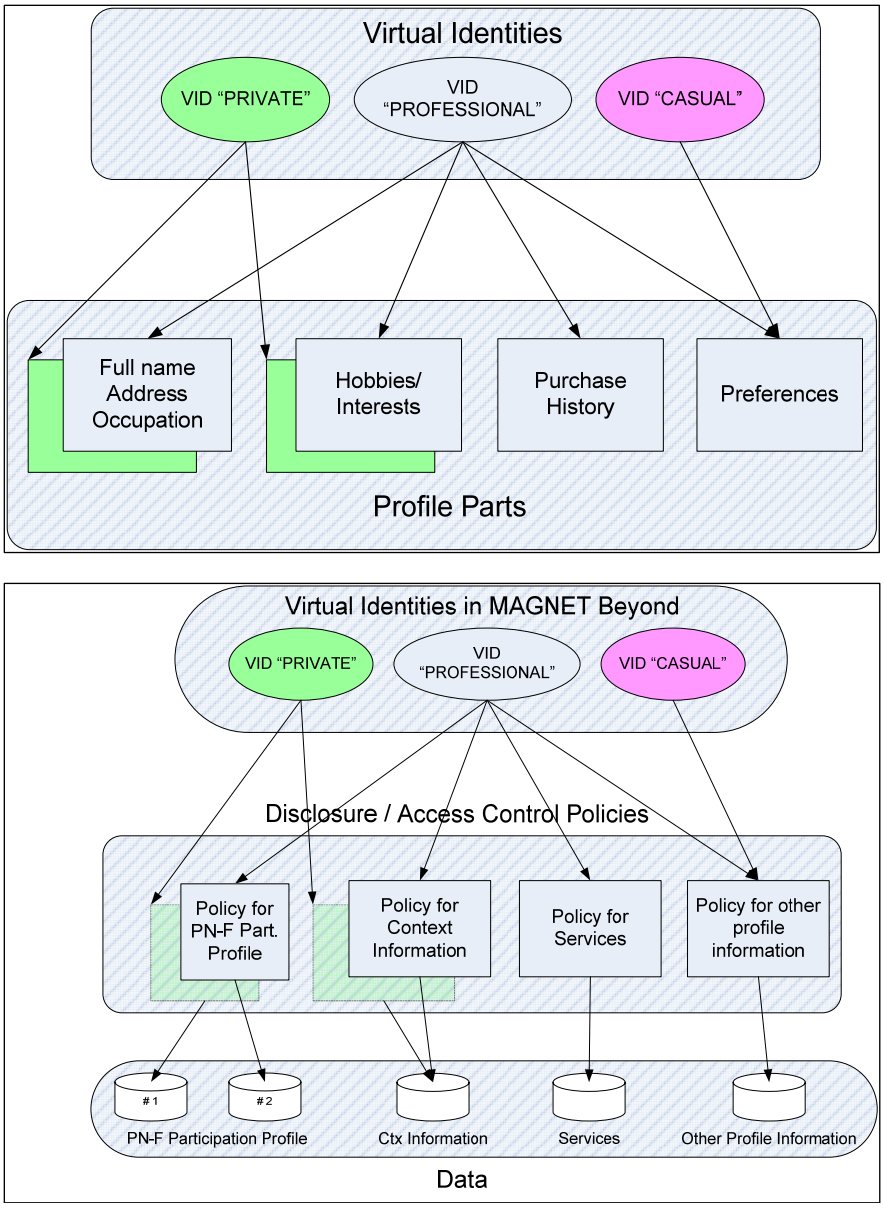


Figure 2-4: Conceptual structure of the VID in MAGNET relating to both user profile (upper part) and policy data (lower part).

Basically the VID consists of an identifier that the user selects (a sort of nickname) and a set of policies, which determine what information or services, may be disclosed during the usage of a VID. This is the plain and simple definition. The VID is composed of information from the user profile, meaning that the VID rather contains pointers to the relevant information than the data itself. If relevant data is edited in the user profile, the same data is automatically changed in the VID also. However, it is possible for a user to have multiple instantiations of each profile part (see Figure 2-4 and Figure 4-13), and fill it with different values if wanted.

The VID is divided into three main unlinkable categories depending on the use of the VID. These categories are:

- "Private": This VID only contains the group {full name, address, occupation} and {hobbies, interests}
- "Professional": This VID contains all four profile parts.
- "Casual": This VID contains only a single profile part, namely the user's preferences like dining

and as shown in Figure 2-4 they consist of different levels of data relating to user information and security and policy settings. The figure shows an example of how VIDs are composed and the information about the user is grouped into four profile parts and how they map to policies and other information from the user profile. More details and security aspects of VIDs can be found in [MBD4.3.3].

In [MBD1.4.1] the concept of **activity** is described. This has been applied in the usability tests (see Sect. 4.1) and leads to user interfaces that are carefully tailored to the activity, thereby making services intuitive and user-friendly. In the following the activity concept will be linked to the use of VID. What should also be mentioned here is the concept of modalities or MODs as introduced in [MBD4.3.2, Chap. 6] and further discussed in Sect. 5.2. The original idea of a user being in a modality relating to the given purpose of the user's interaction with the device is coherent with the idea of all interaction being activity- and tool-dependent. The tools concept together with the "Digital Butler" concept from [MBD4.3.2] can to some extent be compared with the idea of service creation in the MODs (Sect. 5.2). Actually these two concepts could be considered two of a kind, if the activity concept was expanded to be more service creation-oriented and cover visual customization of the entire MAGNET GUIs and the device itself, e.g. the content, functionality and look of the desktop.

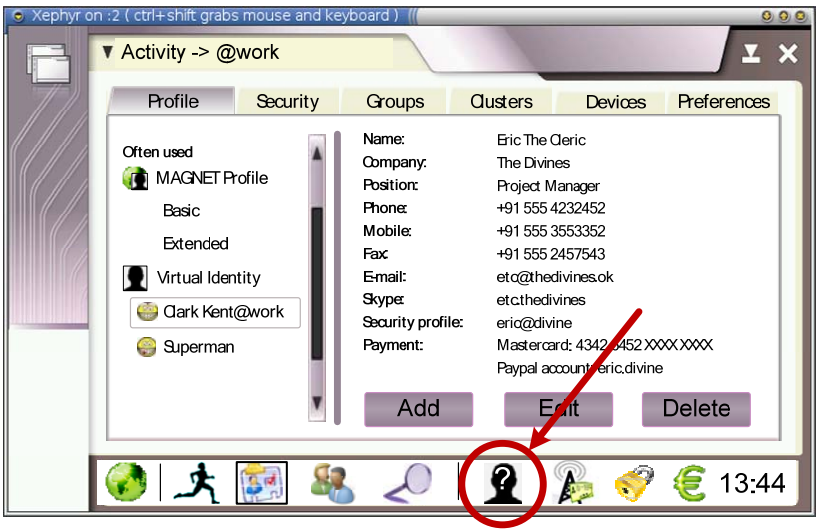


Figure 2-5: Conceptual MAGNET GUI design where the red circle marks the VID icon of the user.

The VID of a user literally has many faces and to understand how this is presented to the user an example is shown in Figure 2-5. The red circle with corresponding arrow shows the actual VID of the user corresponding to the activity the user is currently in. In the figure an anonymous VID has been selected and a thumbnail or silhouette of an avatar is chosen. It is defined in the concept of VID that a user might switch the VID to exchange the PN's identifier by a random value in order to provide unlinkability. Also a "one-time" VID with default policies can be applied and this will then be unlinkable to any of the user's VIDs. The silhouette could be an example of one of these cases.

Every VID has its own picture to indicate the currently selected and to distinguish between the different ones in a visual way. The user can freely shift between the VID while still being in the same activity, as they are not linked. If the user switches between different activities, the VID will also switch to the default VID of the activity as defined by the user when creating the activity. The VID demonstrated here is related to the way the user is presented to other PN users using the Virtual Badge application as defined in [MBD1.1.2]. The selected VID in the given activity is not directly linked to the different VIDs used in the many PN-Fs the user can have. They can be, but do not have to be. When a PN-F is created, a predefined VID is either selected or created from scratch using a template or based on an already custom-made VID with specific policy settings for the given federation. This is to accommodate the design criteria of [MBD4.3.3].

A PN-F is called a group from a user perspective in the MAGNET GUI system. The groups consist of the users selected to participate in the federation and the owner (which could be the user him- or herself). Here the user can freely edit or change the VID for the different groups, which will not influence the VID in the other groups. If a VID is used more places, the user should be prompted if the changes should apply to all other places, or a custom VID with the new settings will be created.

2.5 User profiles in PN Federations

PN-Fs are, similarly to conferences, temporary associations between two or several PNs in order to exchange information and share documents and other resources, such as services. The mechanisms for advertising a federation about a certain topic, to invite another PN or to respond to such an invitation, are all heavily based on the use of special profiles: the PN-F profile and the PN-F participation profile.

The information from these profiles is used in a reasoning component, the policy engine, to support decisions such as (see Figure 2-6):

- Can the federation be started with only, say, three partners or not
- Should the join request from a participant be accepted or not
- Should the invitation be accepted by the participant or not

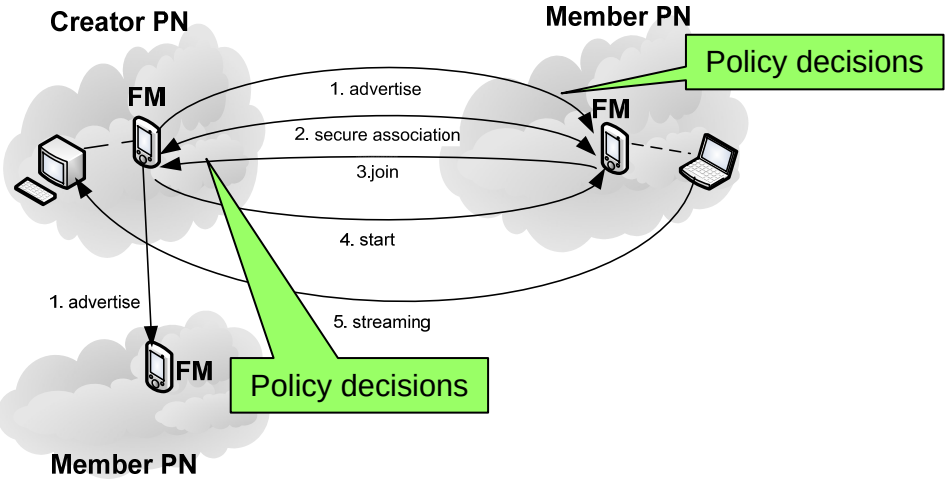


Figure 2-6: Policy decisions in the PN-F life cycle.

In the following we describe in detail the elements of the mentioned profiles. The **PN-F profile** has a public part, that is exchanged before a secure, encrypted connection between the two PNs is established, and a private part.

```
<PublicFederationProfilePart>
<PnfCreator>
<PnIdentifier> pnid_creator</PnIdentifier>
<PointOfContact>poc_creator</PointOfContact>
<FmAddress>localhost:8088/fmem</FmAddress>
<UserName>Creator</UserName>
</PnfCreator>
<PnFederationDescription>This is my special PN Federation
</PnFederationDescription>
<PnFederationIdentifier> f8df8d8787ea4e75b89af1b23fcba8eb00000000
</PnFederationIdentifier>
<PnFederationName>Special Federation</PnFederationName>
<PnFederationPrefix>10.0.94.0/24</PnFederationPrefix>
<PnFederationPublicPolicy>:policy a :public_policy. :policy :join :yes
</PnFederationPublicPolicy>
</PublicFederationProfilePart>
```

Figure 2-7: Public part of the PN-F profile.

The public part, see Figure 2-7, contains the PN_ID of the creator PN, point of contact, that is, the IP address to reply to the creator of the PN-F, and the creator's username (nickname). They are followed by the federation name and a short description of the topic, the PN-F identifier, a prefix for routing purposes and the semantic description of the policy rules applied by the creator for answering the federation invitation or advertisement. This is a powerful mechanism, since the participant can in this way decide, under the circumstances described by the policy, if the participant does or does not wish to continue and create a secure connection with the creator.

```
<PrivateFederationProfilePart>
<Certificate>SerializedCertificate</Certificate>
<PnfAgentReference>localhost</PnfAgentReference>
<PnFederationStateInfo> InternalState</PnFederationStateInfo>
<PnFederationMember>
<PnIdentifier>pnid_member</PnIdentifier>
<PointOfContact>130.125.224.5</PointOfContact>
<FmAddress>localhost:8088/fmem</FmAddress>
<UserName>Alice</UserName>
</PnFederationMember>
<PnFederationMember>
<PnIdentifier>6ba1f454449b481a8088bfa6b7a2fcf7</PnIdentifier>
<PointOfContact>130.188.225.125</PointOfContact>
<FmAddress>130.188.225.225</FmAddress>
<UserName>Alice</UserName>
</PnFederationMember>
<PnFederationMember>
<PnIdentifier>7ba1f454449b481a8088bfa6b7a2fcf7</PnIdentifier>
<PointOfContact>130.188.225.126</PointOfContact>
<FmAddress>130.188.225.226</FmAddress>
<UserName>Bob</UserName>
</PnFederationMember>
<PnFederationPrivatePolicy>:policy a :private_policy. :policy :join :yes
</PnFederationPrivatePolic
</PrivateFederationProfilePart>
```

Figure 2-8: Private part of the PN-F profile.

The private part of the PN-F profile, Figure 2-8, contains in the currently implemented version authentication information in form of a certificate, the address of the PN-F agent, needed by all members in order to register the resources they bring in, and later for the lookup for those resources and services. The state of the federation at the creator is communicated as well. If the federation is open only to certain members, their names, points of contact and PN identifiers are given in this profile part. Based on the information, the member decides to join or not join the federation by using additional policy information.

The participation profile is the counterpart of the PN-F profile, as it is created by a participant for handling automatically an incoming invitation or advertisement - the user can however also be asked. The participation profile may identify a certain PN-F name that is positively answered. In this case the four member information attributes as mentioned above are given.

In general the exchange of profiles is controlled by the Federation Manager (FM) entity and integrated in the federation formation protocol, which is an application protocol between the FMs of the creator and the participants (members).

Concerning the creation life cycle of those profiles, the PN Manager offers a user interface for the creation of those profiles from templates. The FM is involved in this process and the Secure Context Management Framework (SCMF) is used to store and retrieve the profiles as needed.

2.6 Common ontology for user profiles and context information

As discussed above and in previous deliverables, building a common ontology for user profiles and context information has been an important objective of the project. This has been successfully accomplished and applied in the pilot services.

Figure 2-9 shows the core concepts of the Integrated SCMF Ontology for context and user profile information. It is used as a basis for storing context and user profile information in the SCMF, which is briefly described in Sect. 3.1.

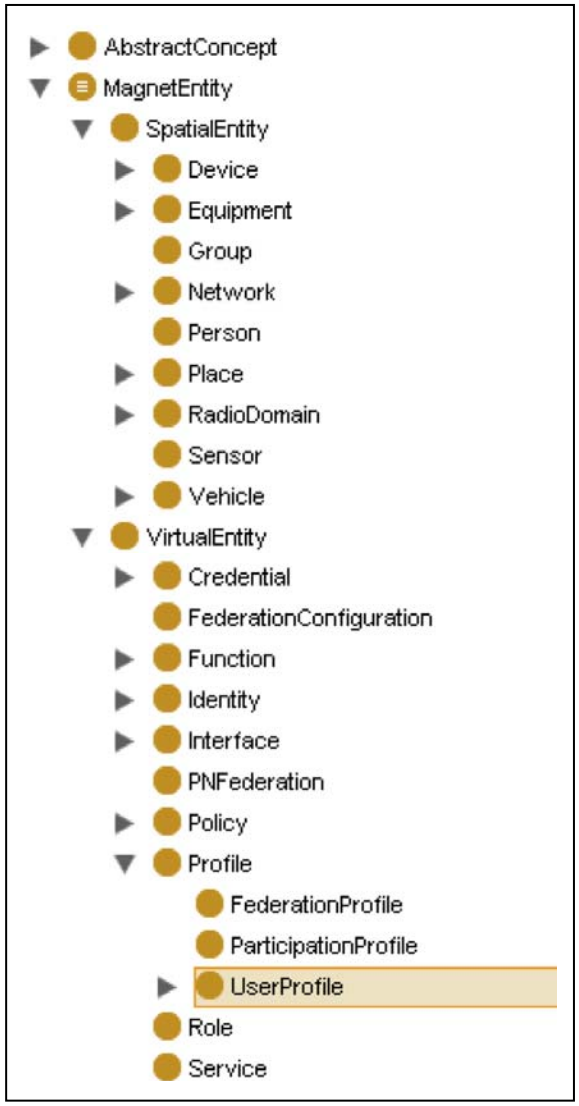


Figure 2-9: Overview of the Integrated SCMF Ontology.

The underlying idea of this ontology is to define a hierarchy of entity types, facilitating a 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 modelled as a *MagnetEntity*. Based on the unique identifier an index can be built to provide the basis for efficiently accessing context information in all cases in which the specific entity is known.

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 subsconcept *Profile*, which in turn has a subconcept *UserProfile*.

The attributes of MAGNET Beyond entities are modelled as properties in the ontology. Properties can either have simple types supported as base types in the ontology such as Strings or Integers, or they can be complex types, in which case they are modelled as an AbstractConcept. For the user profiles we have made heavy use of these AbstractConcepts as they determine the units that can be retrieved by the SCMF. For example, if the user profile should contain a property “home address”, there must be a complex structure for the whole address. It is not sufficient to model street, post code, city, etc. separately. Especially if there could be multiple instances of home address in the same profile, it needs to be clear which information belongs to which address. On the other hand, modelling an address as a separate entity would have the effect that two subsequent requests to the SCMF would be needed for retrieving the information.

As shown in Figure 2-10, the SCMF currently supports the complete BasicUserProfile as defined in Figure 2-3 and [MBD4.3.2], and also the FitnessCenterProfile, which is an ExtendedUserProfile, so that the Gym application described in Sect. 4.2 can run within a PN/PN-F setting, without access to external components like the MUP server.

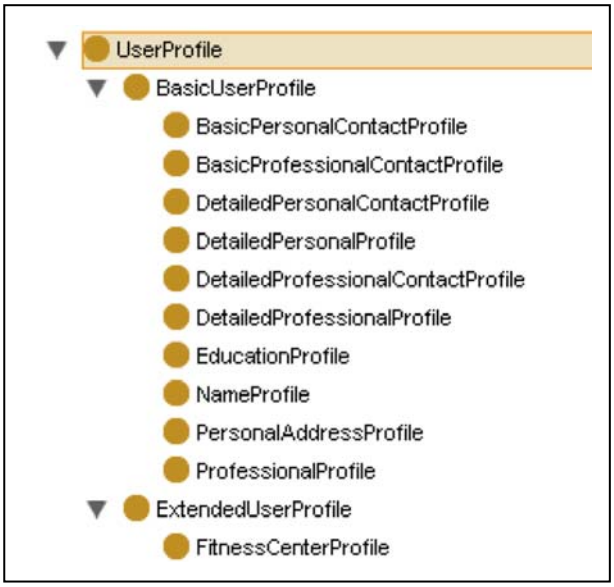


Figure 2-10: User profile part of the Integrated SCMF Ontology.

The *FitnessCenterProfile* has the properties shown in Figure 2-11. Of special importance is the *hasTrainingProgramme* property which has the *AbstractConceptTrainingProgramme* as its type, which will be described in some more detail in Sect. 4.2.

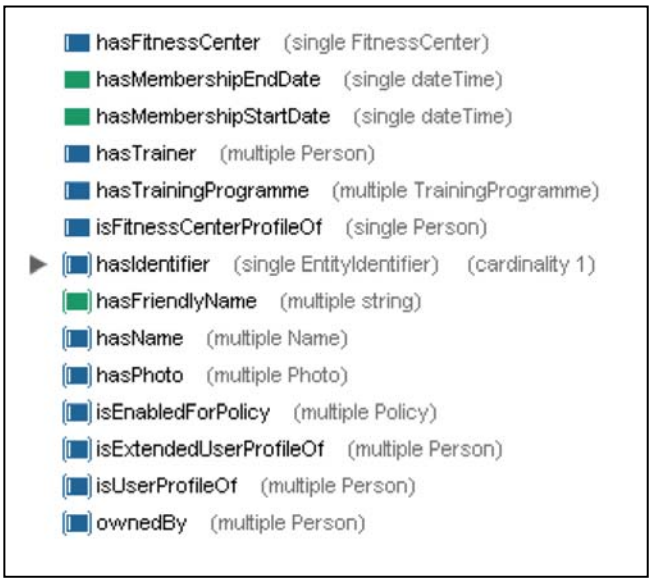
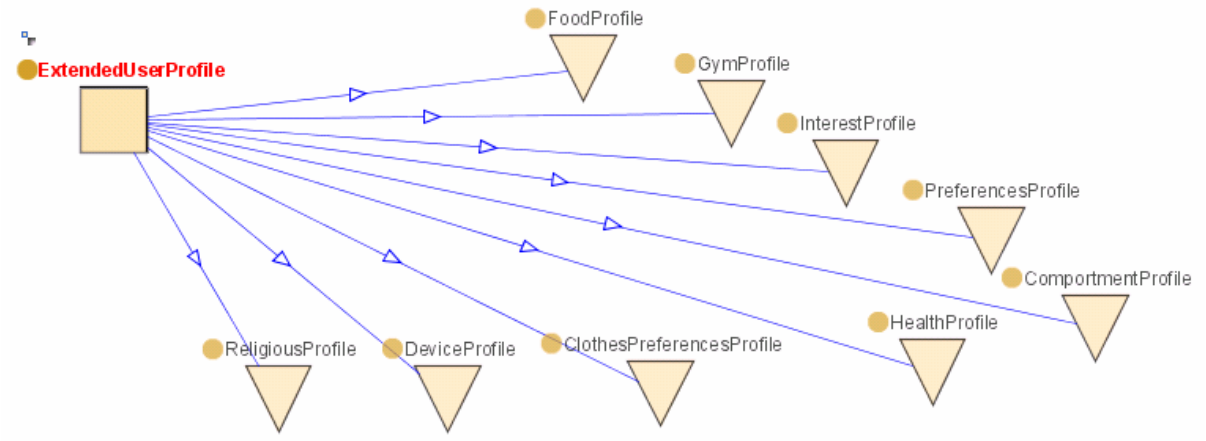


Figure 2-11: Properties of the FitnessCenterProfile.

Figure 2-12 shows an expanded view of the other parts of the extended user profile, which have been conceived, in this example, to store a variety of additional fields and preferences that might be used to cope with other roles and needs of the user. The complete extended profiles shall be available only through the MUP, cf. Sect. 3.3, and all its settings shall always be provided by the owner of the profile.



b)

Figure 2-12: MUP Extended User Profile.

3 User profile management

3.1 SCMF and the PN service architecture

Context management is an important aspect in supporting applications, service and other networking components with the aim of achieving context awareness. Thus, context awareness is not an uncommon goal when developing software entities, as it allows for intelligent response to the circumstances, not just relying on assumptions set by the program developer during implementation. For the personalization concept envisioned in MAGNET Beyond context plays an important role, as personalization complements and acts together with context awareness. Some persons prefer no adaptation at all; others may prefer their application to be able to change functionality to a certain limit and so on. As PNs are mobile, and in fact a large-scale ad-hoc network type, adaptation is virtually a requirement in order for PNs to be really useful for a user.

In order to support context awareness and personalization in MAGNET Beyond, a dedicated Secure Context Management Framework (SCMF) has been developed. The preliminary architecture was described in [MBD2.3.1], but further enhancements, development and research have been conducted since then, as described in details in [MBD2.3.2]. This section aims only to provide a brief overview of the framework, and how it is used with respect to user profiles and support context awareness.

The framework is focused around the entity called Context Agent as shown in Figure 3-1, which runs on each node in the Personal Network. Together, the interacting Context Agents form the SCMF.

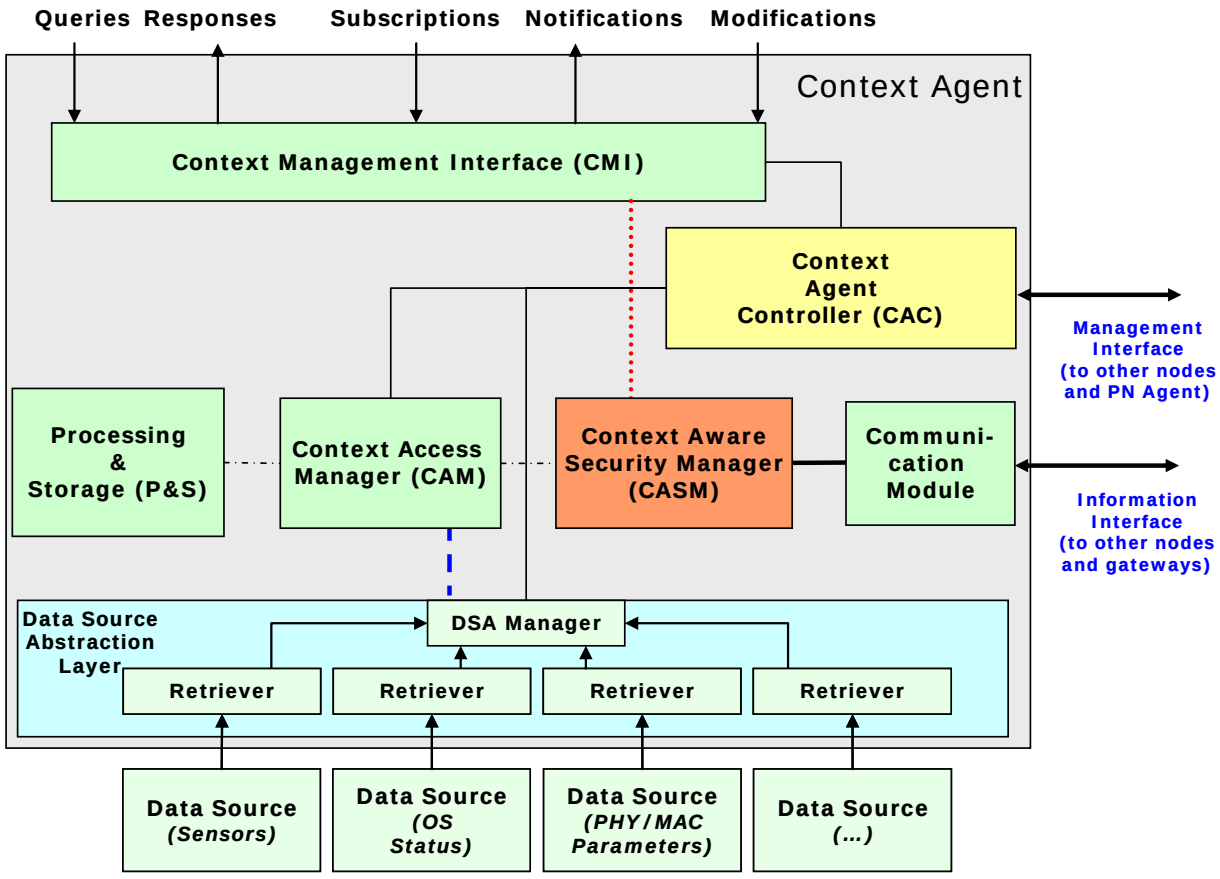


Figure 3-1: Overview of a Context Agent with active components.

Using a dedicated declarative access language named CALA[3]; a client application is capable of accessing context information as well as inserting, updating and querying user profile information. CALA queries are executed through Remote Procedure Calls (RPC). The Context Agents are distributed on all nodes in the PN (with different configuration depending on the capabilities of the device it is running on), and dedicated agents may act as gateways between PNs to allow sharing also of context information in PN-Fs [MBD2.3.2]. Thus, a configuration of Context Agents could be as shown in Figure 3-2.

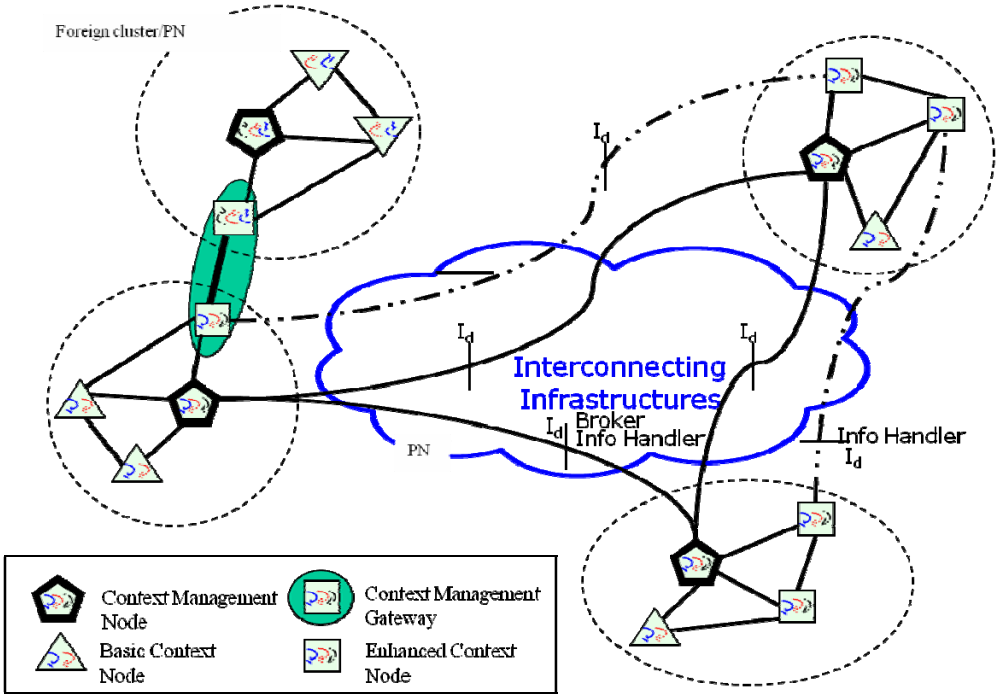


Figure 3-2: Example configuration of Context Agents in a PN with connection to another PN in a PN-F scenario.

Context information is accessed though retriever components shown at the bottom of Figure 3-1, from where the raw data is translated into a MAGNET Beyond specific data format. The Context Access Manager enables the Context Agent to efficiently distribute knowledge of what information is available where in the PN. Furthermore, the **Processing and Storage (P&S) component** provides local storage as well as additional processing capabilities for e.g. inference of context information. The detailed interaction and communication patterns are described in [MBD2.3.1] and [MBD2.3.2].

The key functionality related to user profiles is its capability of storing the user profiles and making them available to all nodes in the SCMF, and when further coupled with the interaction of the MUP system described in Sect. 3.3, the framework provides a powerful and efficient access to user profile data distributed in the PN.

3.2 Access control to user profiles and management of trust relations

User profile data is very sensitive information and should be protected in the PN, especially when applications provide the possibility of external access to the profile data. Two options have been proposed and researched in the project as described in the following, one using the Context Aware Security Manager (CASM) and one using an external Policy Engine (PE). Both of these PN elements were described in [MBD4.3.2] and the latest updates can be found in [MBD2.3.2] and [MBD4.3.3].

[3] Context Access LAnguage, an XML-formatted query language specified in [MBD2.3.2].

3.2.1 Option 1: Policy Decision and Enforcement using the CASM entity

Within the SCMF, the Context Aware Security Manager (CASM) is the component responsible for enforcing policies regarding access control, privacy and context information filtering on PN and the (from a security point of view) more interesting PN-F level. Security policy enforcement follows the flow chart presented in Figure 3-3.

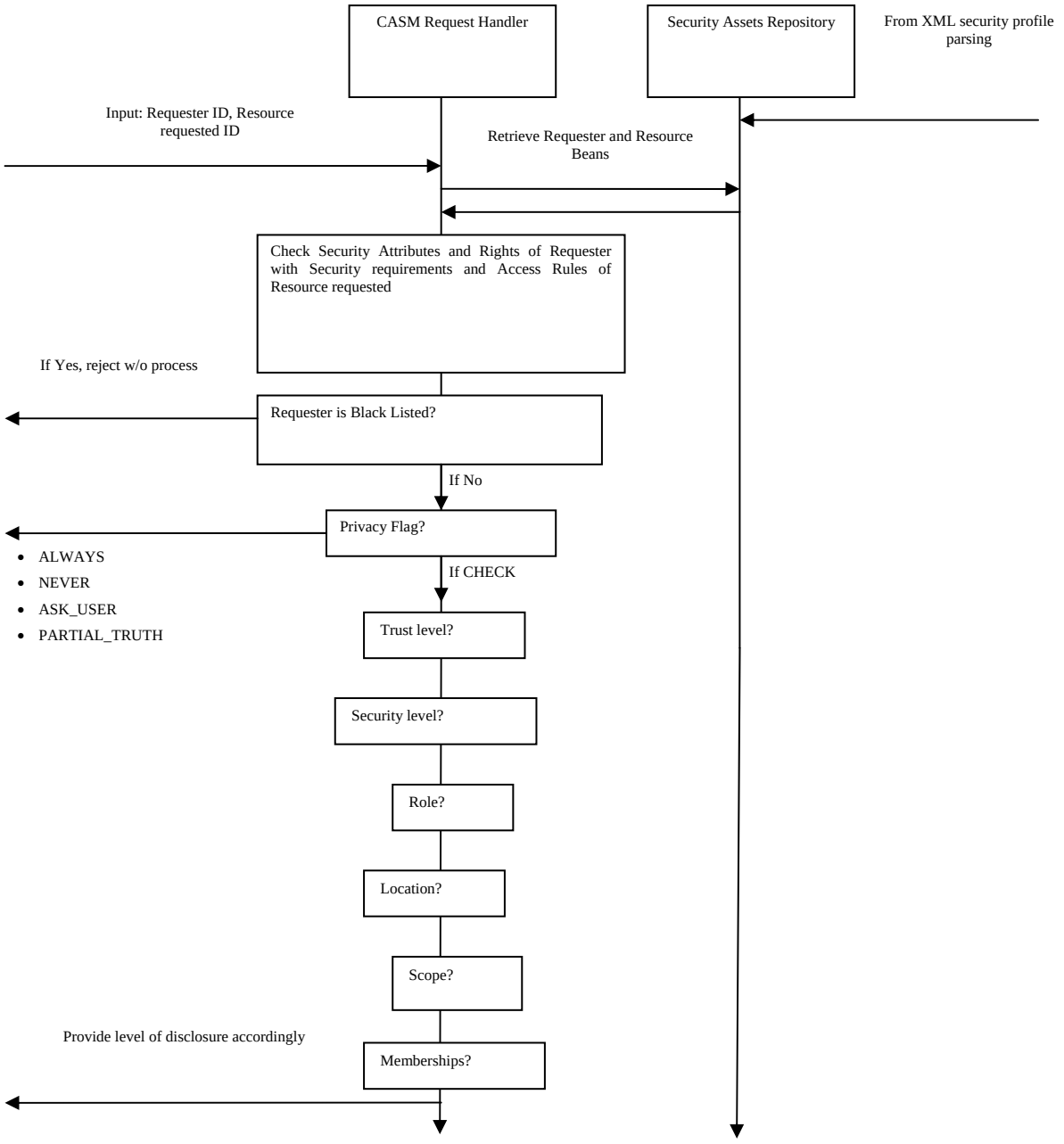


Figure 3-3: Security Policy Enforcement Algorithm [MBD4.3.3].

Security policy enforcement therefore includes the following functionalities:

- Black lists for nodes and users reported for suspicious, illegal and/or abusive behaviour
- Privacy flags for tagging information according to the security requirements and personal security needs
- Levels of trust, group memberships and security roles for more efficient trust and user management
- Location and context-specific policies (e.g. security level of infrastructure used)
- PN can be divided into more security domains and clusters through the "scope" attribute of the security policy. This promotes more efficient policy management.

More information on the architecture, specifications and functionalities of CASM can be found in [MBD4.3.2], [MBD1.1.1] and [MBD4.3.3].

3.2.2 Option 2: Policy Decision using the semantic policy engine (PE)

The inter-working between the SCMF and the semantic policy reasoner is envisaged to achieve two major goals:

1. To provide an advanced rule and policy framework for the protection of context, especially when external users and applications request it.
2. To provide a dynamic, context-oriented basis for policy decisions

The high-level interactions in Case 1 are sketched below:

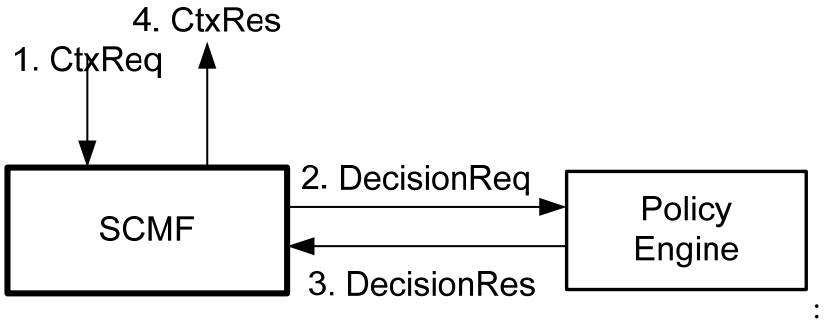


Figure 3-4: Policy decision point for the protection of context.

The interface between the SCMF and the Policy Engine is that to a Policy Decision Point (PDP):

```
int getDecision(String sourceId, String entityId, String entityType,
String attributeName)
```

The main parameters needed by PE for a decision are:

- sourceID: PN-ID, or for external services IP:port of the requestor. A rule may use known users address books to estimate the trust level.
- entityId, AttributeName: this combination allows to decide based on the requested object
- entityType, AttributeName: this combination allows to prove more general rules

Case 2 is already implemented. It allows loading dynamic context information on demand in order to perform the reasoning.

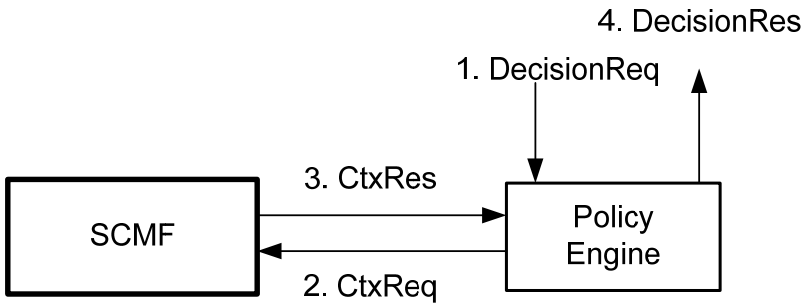


Figure 3-5: Context-based reasoning.

3.3 Interface to an external, centralized Generic User Profile

In the framework of WP1 and together with the effort allocated in WP6, a centralized repository for both Basic and Extended User Profile schemas has been delivered. In particular the description of the profile schemas is based on OWL-DL ontology. The prototype called MAGNET User Profile (MUP) follows the 3GPP Generic User Profile (GUP) definition [3GPP GUP], [MBD1.2.1], and the full-blown solution would handle access to typical 3GPP data repositories, GUP and others from IMS and ISP worlds.

The distributed nature of the GUP system architecture is displayed in Figure 3-6. Different applications (like 3rd party services or others) query information about the user through the GUP server. The GUP server does not contain the actual user profile data, but knows where the newest information is available from. The GUP server can then (based on the implementation) get the data from the repository using the Repository Access Function (RAF) of the different repositories. The interface to the repository itself can be proprietary, but the communication with the RAF is standardized. This distributed concept has been adapted in MAGNET Beyond, and a security layer with policy enforcement has been added making all user profile queries secured to prevent leakage of unwanted user profile information. The MUP is only maintaining the distributed user profile and not enforcing the policies. This is done by the PE in the PN (cf. Sect. 3.2).

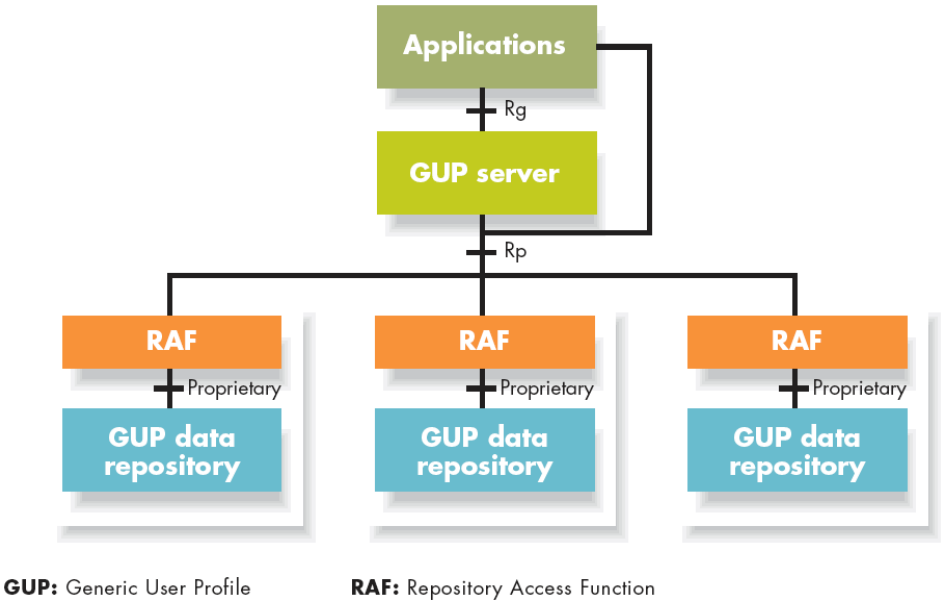


Figure 3-6: The basic GUP architecture [ucentric], [MBD1.2.1].

The architecture shown in Figure 3-7 uses the functionality offered by the PN-F SCMF gateway to interact with the external MUP server. This requires that the MUP server uses CALA in both directions, i.e., can get user profile information from the SCMF as well as provide access to its user profile information for the SCMF.

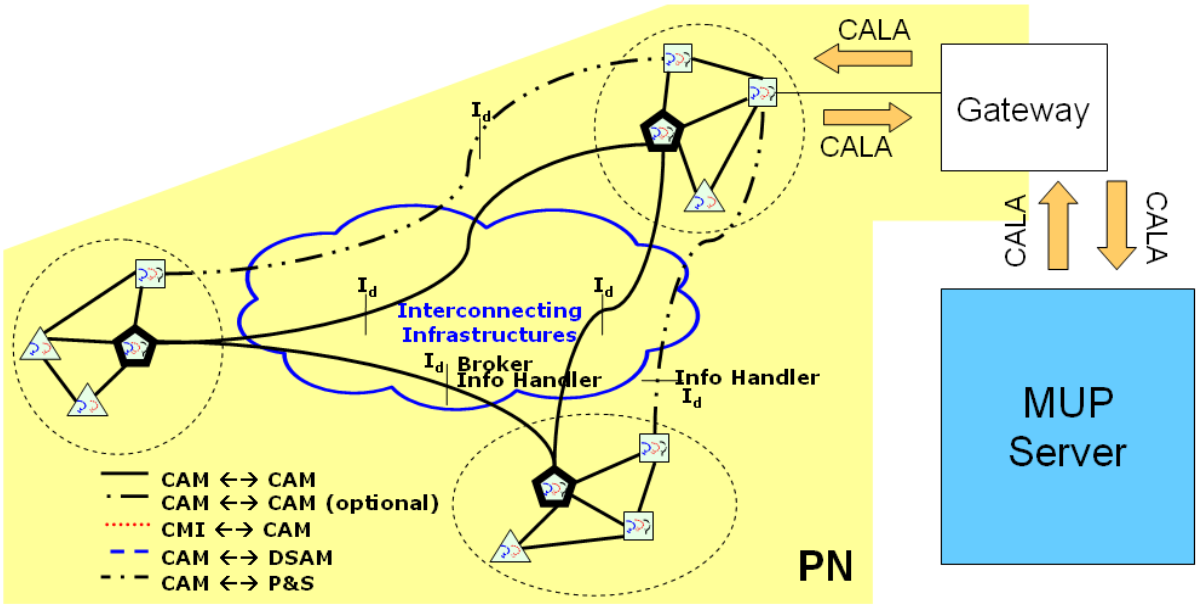


Figure 3-7: PN agents forming the SCMF and communicating with the MUP server through a gateway using CALA.

The MUP realized in the project represents the main access point for retrieving user profile data, synchronization between the local and the remote instances of the basic user profile and an interface to query the OWL-DL ontology based on the standard SPARQL language[4], and an external interface (CALA client) to manage specific user data based on the CALA language (see Figure 3-8).

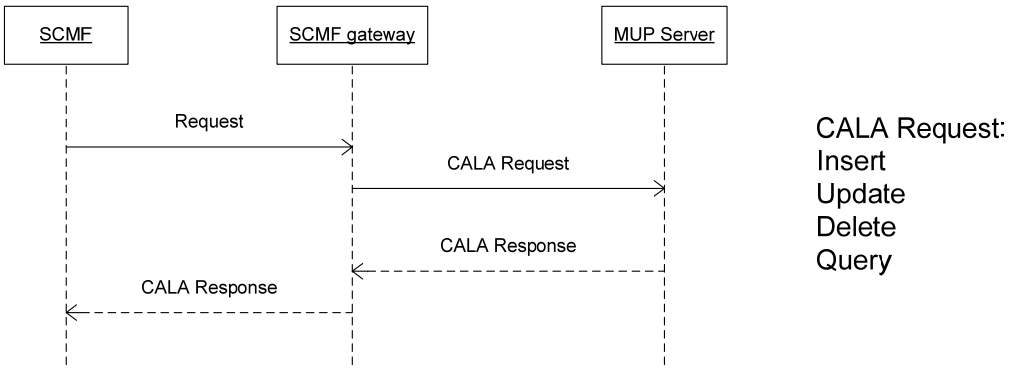


Figure 3-8: Message sequence chart showing the interactions of the SCMF, gateway and MUP server.

This client can be installed on other nodes in the PN for queries and updates. The following figure shows the basic functions and profile accesses applicable to the MUP demonstrator.

[4] http://www.w3.org/TR/rdf-sparql-query/

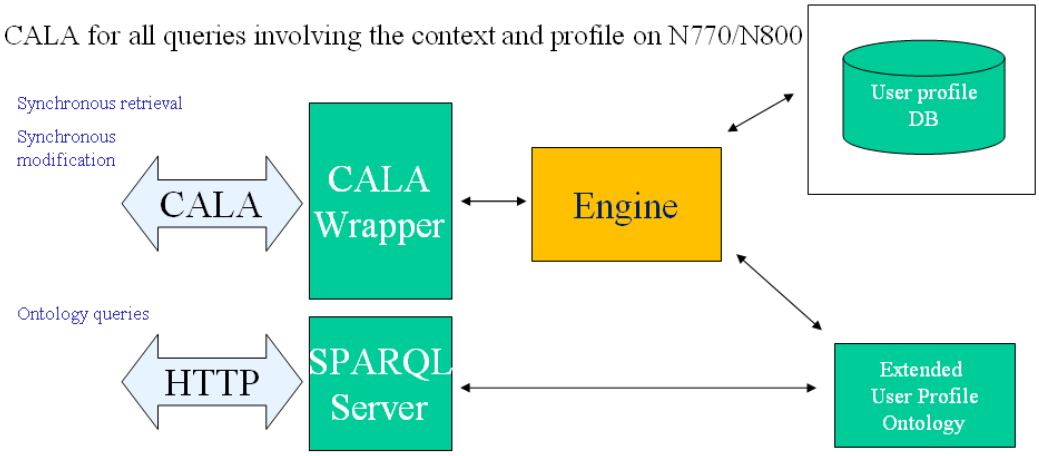


Figure 3-9: MUP server high-level architecture.

For test purposes, the Eclipse environment[5] has been used, which allows detailed traceability and debugging. The administration OSS interface under the responsibility of the PN provider or generic subscriber data administrator is interfaced using the HTTP. Therefore, the MUP server in some way can be included into the space of the web services and consequently its business model analysis can refer to this space as well. The MUP system implemented consists of following software packages:

- MUP server Database
- MUP server Data structures
- MUP server Engine
- MUP server Gateway attendant
- MUP server Tests
- MUP server Utilities

The middleware and the databases are strongly based on the use of ontologies in a seamless way to access all different data repositories. In fact, it does not hold any data, but gives the impression of holding all the data by being able to answer queries. An important database included into this architecture is the GUP. Based on this architectural approach, MAGNET Beyond has specified and designed IMS pilot applications for health care and professional sectors utilizing external profile server (MUP) storing profile information of PN users. MAGNET Beyond offers a service platform that leverages new ways for IMS technology to deliver improved, context aware and personal services for end-users increasing revenue opportunities for service providers and operators who wish to turn their commodity-priced service bundling into a highly competitive one. The opportunity for an operator to provide quadruple play (triple plus mobile) enhanced with context-aware PN capabilities may become the key success point in a Web 2.0 Internet world.

The concept of a Digital Butler was originally presented in [MBD4.3.2] and refers to the functionality, that a user can have an online entity as a sort of Personal Identity Provider (PIP), which is a contraction of an Identity Provider (IdP) and a Personalisation Provider (PeP). With relevant user profile information the Digital Butler surfs different 3rd party services and reveals only disclosed user information to the service provider with the intention to personalize or value-add the service before presenting it to the user. The Digital Butler is a sort of a filter that uses information about the user to customize a service to better suit the user.

[5] http://www.eclipse.org/

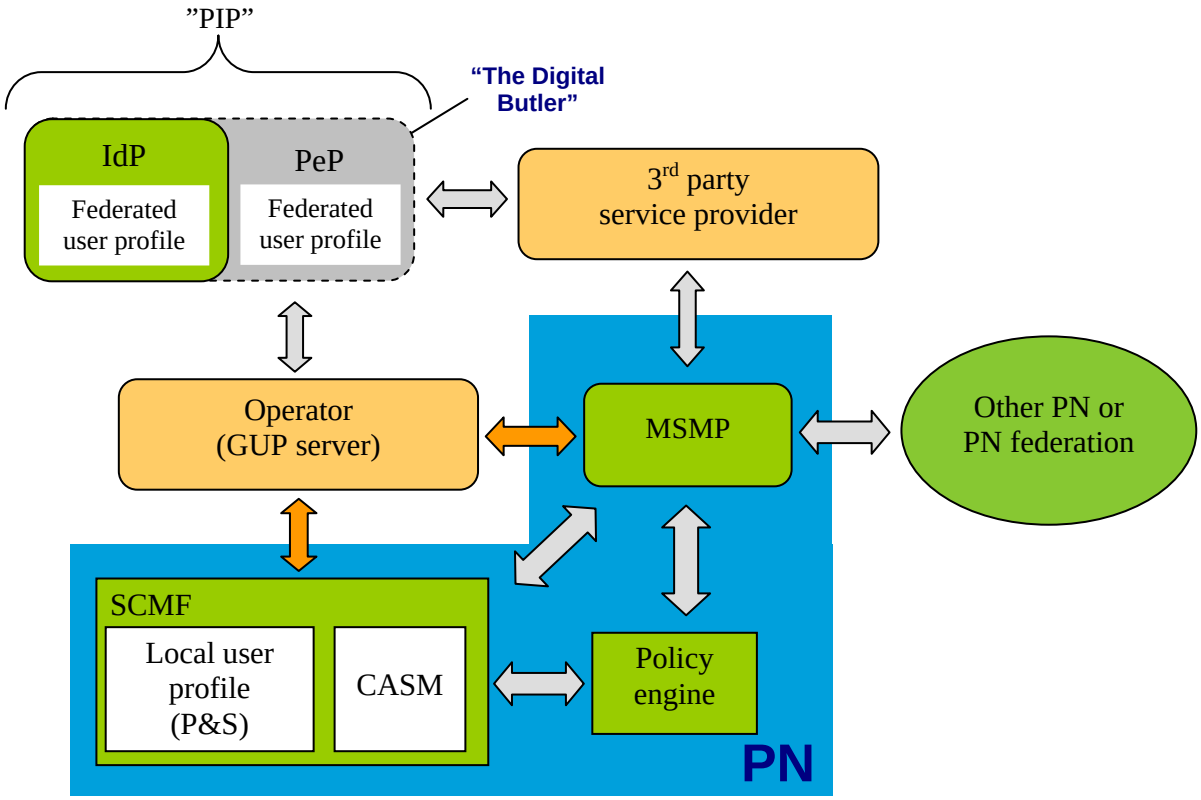


Figure 3-10: Overview of a MAGNET-enabled user with an optional "Digital Butler" communicating with a 3rd party service provider. The orange arrows are only meant as the components having connectivity [MBD4.3.2].

The original design in Figure 3-10 can be compared to the design of the MUP described in Figure 3-9. In both cases the functionality of an operator is not considered, but the communication between the different blocks can be compared. The communication in Figure 3-9 uses either CALA or HTTP. This could be used in Figure 3-10 between the 3rd party service provider and the Digital Butler or the MSMP, where HTTP would be the communication protocol. The Digital Butler would be an entity and a part of the engine that handles the queries and all communication towards the SCMF would be handled using CALA. The queries would be policy-enforced in the PN by the PE and only user information that the user allows to be readable is returned to the service provider, using HTTP. This is just an example of the actual implementation. Other communication protocols towards the Digital Butler are also possible. The HTTP solution is only for the pilot service implementations to demonstrate the functionality.

4 Application of user profiles in selected pilot services

This chapter mainly deals with the application of user profiles in the pilot services. With reference to three of the pilot scenarios, the Icebreaker, the Gym and the Presentation Service, we discuss the relevant parts of the ontology, the GUIs that have developed, and the interaction with the SCMF and the PN service architecture. Furthermore, we discuss the concept of activity in relation to MAGNET Beyond. The strength of this concept is that it makes use of the user preferences to emphasize the relevant information for the user in a given situation and enables a more user-friendly interaction with the PN.

The pilot services are described in [MBD1.3.1] and early ideas for the application of user profiles were discussed in [MBD4.3.2]. At the time of writing the present deliverable, the pilot services are in essence completed. Some of them make heavy use of user profile information, and in the following we present some of the highlights, which illustrate the benefits of the user profiles and the management framework.

In the pilot services the user profile information is accessed through the Context Agent on the local device, cf. Sect. 3.1. This provides access to all information stored in the SCMF, but also in the external MUP system.

It should be emphasized that the user profile and associated concepts developed in the project have a much greater potential than what has actually been implemented and demonstrated in the pilot services. Nevertheless, the examples serve their purpose of showing how useful the user profiles and the PN service architecture are for the personalization of services and user interfaces and facilitating a variety of tasks for the end users.

4.1 The Icebreaker scenario

The Icebreaker service has been designed and implemented in order to take advantage of the user profile information to provide application for the socialization of the user. This is based on his/her individual characteristics, which are depicted in the corresponding user profile information.

Figure 4-1: Icebreaker GUI.

When the Icebreaker service (consisting of the Community Building, Matching service and Presentation service) is started, it subscribes to the SCMF in order to query and download the user profile information, which plays a fundamental role to the subsistence of the service. The interface used is XML-RPC, and the CALA queries embody the corresponding parts in order to collect personal and professional information from the basic and extended part of the user profile.

The Graphical User Interface (GUI) in Figure 4-1 shows the button labelled "My Profile", 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, name, and a photograph of the user. The users can then modify their business cards (BC), using the "My Card" button, and exchange them.

The BC is initially filled out with the following information, retrieved again from the user profile, which is stored in the SCMF:

- Name
- Job title
- Company
- Education
- Address
- Telephone number
- E-mail

The information needed is available in the *DetailedProfessionalProfile* that is highlighted in Figure 4-2.

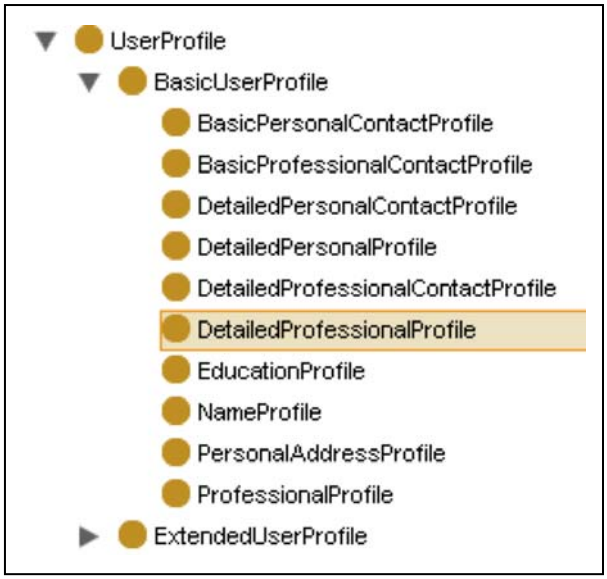


Figure 4-2: Basic User Profile.

The relevant attributes are *hasName* (Name), *hasJobTitle* (Job title), *hasCompanyName* (Company), *hasEducationalLevel* (Education), *hasOfficeAddress* (Address), *hasProfessinalContactInformation* (Telephone number and E-mail), which are shown in Figure 4-3.

Figure 4-3: Attributes of *DetailedProfessionalProfile*.

As 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.

4.2 The Gym scenario

The Gym scenario implemented as a pilot service consists of five larger devices/components:

- A scale
- A bicycle
- A node being used as a client to the user (here a Nokia 800)
- A node being used as Context Management Node (here a laptop)
- An external positioning system

The scenario, which has been primarily designed for usability experiments, is described in details with user test details in [MBD1.4.2]. Here, we only give a short overview on how user profiles are used in the scenario, and how the SCMF is involved for accessing the context and profile storage. The scenario can be divided into a number of steps, namely

1. The user enters the gym and wants to start the gym program (see [MBD1.1.2] for an overview of GUIs in this application)
2. The user goes near the scale, as he/she is supposed to weigh him/herself before and after the exercises

3. The system detects the presence and availability of a nearby scale and informs the user about this
4. The user weighs him/herself and stores the weight in the user profile
5. The system now detects an available bicycle and tells the user to step onto it
6. If the bicycle has set capability, user profiles are used to auto adjust the bicycle setting according to the user's personal training program
7. The user starts pedalling, from which data is gathered and shown online on the user's mobile device
8. Upon exercise completion, end results (e.g. amount of km driven, calories spent etc.) are stored as a part of the user profile in the SCMF
9. Other equipment can also be executed in similar way, according to the program for the user
10. When the user is done, (s)he is asked to use the scale again (see step 2-4)

In the following we take a closer look at important aspects of the user profile and the interaction with the involved components.

4.2.1 The user profile

The properties of the FitnessCenterProfile have already been shown in Figure 2-11. As discussed there, the *hasTrainingProgramme* property is the most relevant for the Gym application. The properties of the *AbstractConceptTrainingProgramme* are shown in Figure 4-4. A training programme consists of multiple exercises, which is reflected by the fact that multiple instances of the property *TrainingProgrammeExercise* can be part of *TrainingProgramme*.

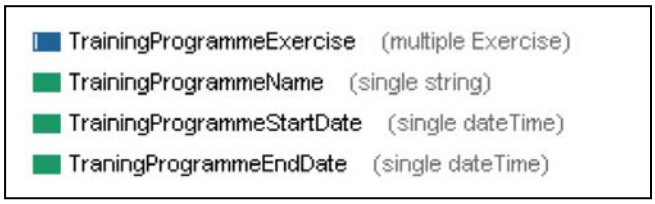


Figure 4-4: Properties of the TrainingProgramme.

An exercise in the training programme has the properties shown in Figure 4-5.

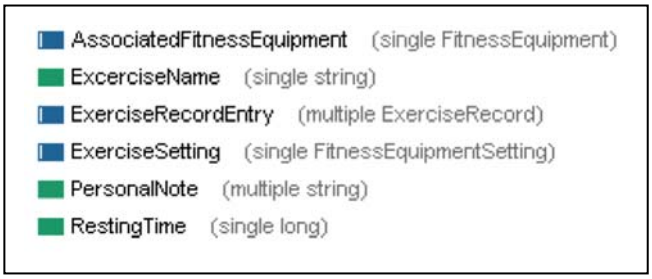


Figure 4-5: Properties of the Exercise.

For each exercise the setting for the relevant fitness equipment can be stored. Also for each execution of the exercise a record is stored, according to which the progress of the user can be followed.

4.2.2 Interaction pattern with bicycle and profile storage

Figure 4-6 illustrates how profile data are exchanged with the bicycle.

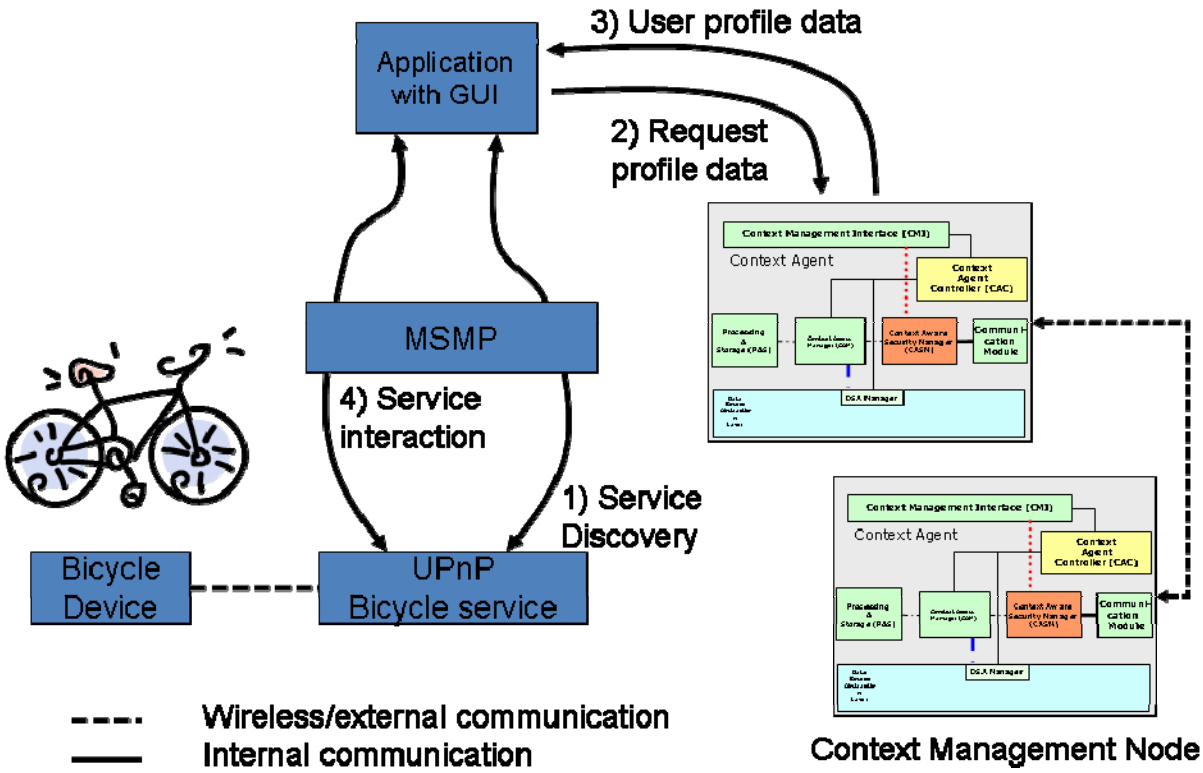


Figure 4-6: Interaction model with bicycle and illustration of how the SCMF is being used for storing and distributing user profiles related to the bike settings and training program.

In this part of the scenario it is the MAGNET Service Management Platform that is used to 1) discover the bike service, and later in 4) interact with it. As seen, the first thing being done is using the service discovery platform to discover the bike service. Once the gym application has been informed about the presence of the bike, it accesses in 2) and 3) the relevant profile information with respect to the current training program and bicycle settings needed (ExerciseSetting in Figure 4-5). The user profile for the bike is not necessarily stored locally on the respective local Context Agent, meaning that this needs to communicate with the Context Management Node to retrieve information about the user profile. Once the exercise is finished, an exercise record (ExerciseRecordEntry in Figure 4-5) is stored in the user profile.

4.2.3 Interaction with the scale

Figure 4-7 shows how the scale is being used in order for the application to obtain the user's live weight.

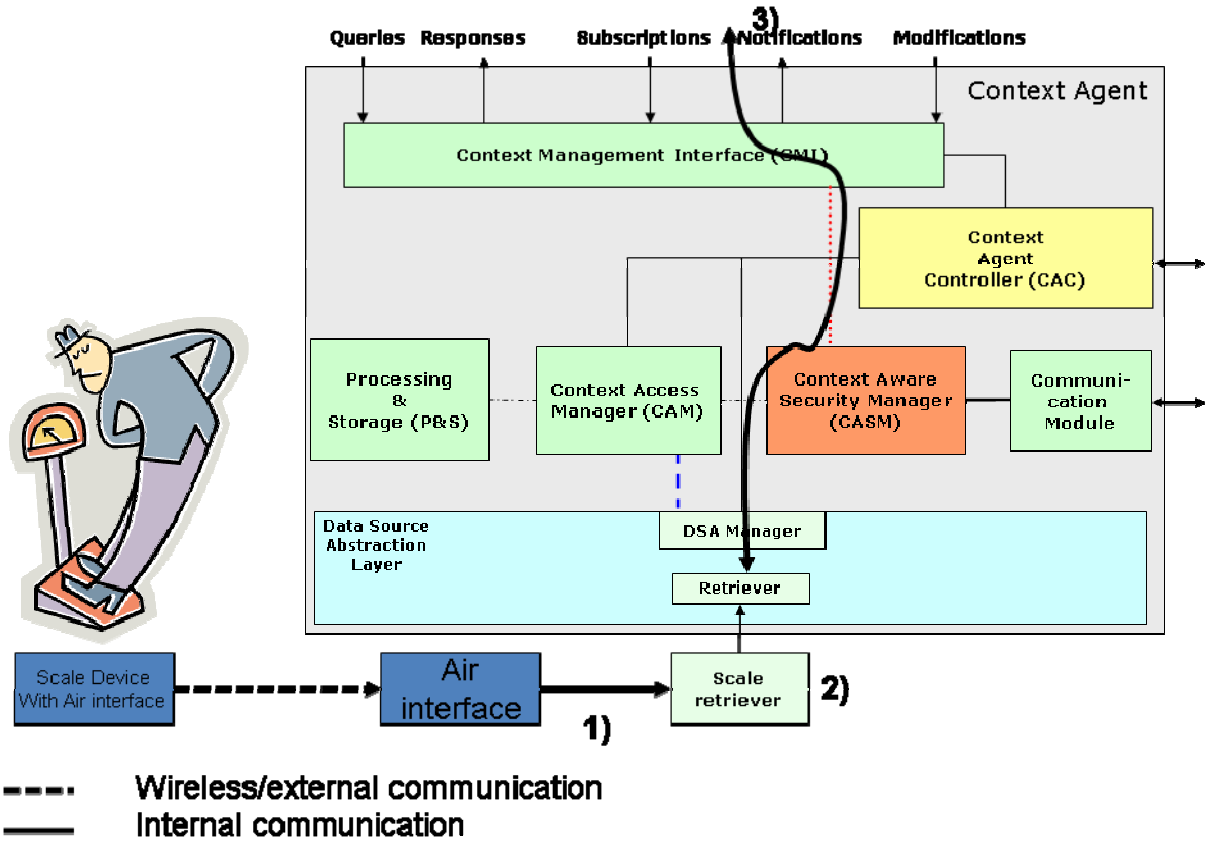


Figure 4-7: Overview of how the weight of the user is obtained through a scale retriever and made accessible through the SCMF.

At first, the scale is discovered by the air interface being used (device discovery). The retriever is put in a wait state before this happens and responds to any request in that time period by an "unavailable" status. Once discovered, and connection is established between the scale and retriever, the scale transmits constantly a simple datagram to the retriever, which interprets this datagram. From the datagram the retriever is capable of seeing whether the scale is in use or not, or if the weight is unstable (when a person is stepping onto or from the scale, the weight measured is unstable and unusable), or if the data is valid. Only when it is valid, the client application can request for the weight successfully. It is also possible to subscribe to a stable weight. Details of the retriever are given in [MBD2.3.2, Appendix C]. Once the weight has successfully been provided to the gym application, it later stores this information as a part of the user profile (ExerciseRecordEntry in Figure 4-5).

4.2.4 Distance collection and notifications

For both the scale and bike the application is triggering certain parts of the GUI and changes internal states depending on the user position in relation to the involved device. Thus access to position information is needed, which is done through the Context Agent as seen in Figure 4-8.

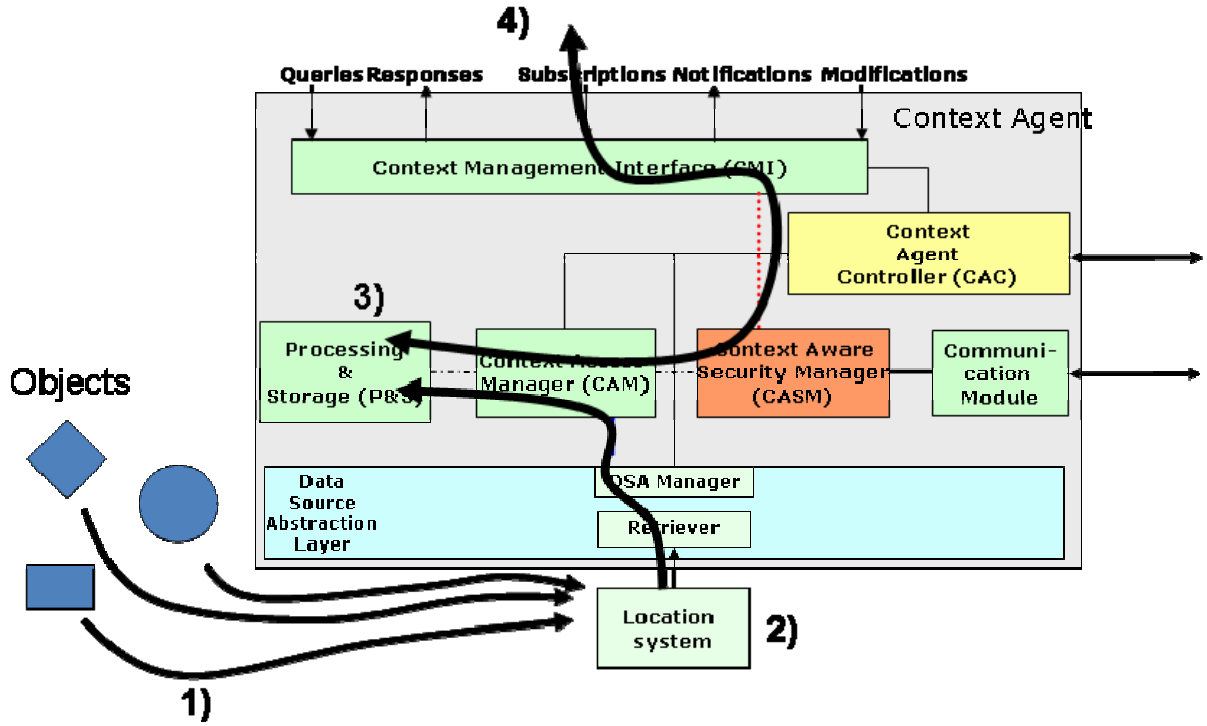


Figure 4-8: Illustration of how the distance between objects are obtained and used to trigger events at the application when being near the specified object, here the bicycle and the scale.

The location system is based on triangulation between a set of motes (details of the implemented system can be found in [MBD2.3.2, App. C]), from which 1) the position of a tracked object is obtained through a dedicated retriever, which provides the distance between a "base" (the device computing the location) and a "target" (the user). Since it is the distance between the user and the device that is needed, and not the actual position, we use a simple Processing Unit (PU) in 3) to calculate the distance between the desired objects (this is mainly done to show the feasibility of the system). The application is then able to subscribe to notification on the distance being below a certain threshold. When this happens, the subscriber is notified in 4). Since the PU needs the position of the user in order to calculate the distance, the PU either sends requests or subscribes for positioning information from the retriever in 2).

4.3 The Presentation Service

In the pilot service application called Presentation Service the user profile is used in the booking system and the Presentation Service itself. The specific entries of the user profile enabled relate to information about the user's name and phone numbers stored in the profile.

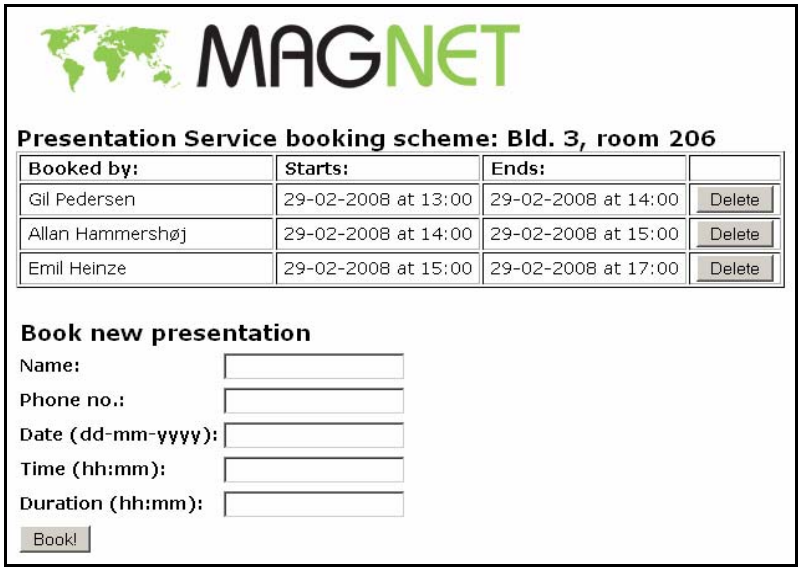


Figure 4-9: The booking system of the Presentation Service. The phone number is not displayed when the booking is registered, but the booking is stored under this identifier.

When a booking is made the user enters a phone number as a unique identifier. If this phone number is registered somewhere in the user's profile (i.e., in *hasProfessionalContactInformation* in *DetailedProfessionalProfile* as shown in Figure 4-2 and Figure 4-3*)*, the Presentation Service can use it to verify if the user has any active bookings. The Presentation Service fetches all phone numbers from the basic user profile and queries all valid bookings with the different phone numbers found. If one or more bookings belong to the user, the time slot or slots are returned from the booking server to be displayed in the MAGNET GUIs and used to enable moderator rights on the Presentation Service server, if the time slot is the current time of the day (see [MBD1.1.2] and [MBD1.4.3]).

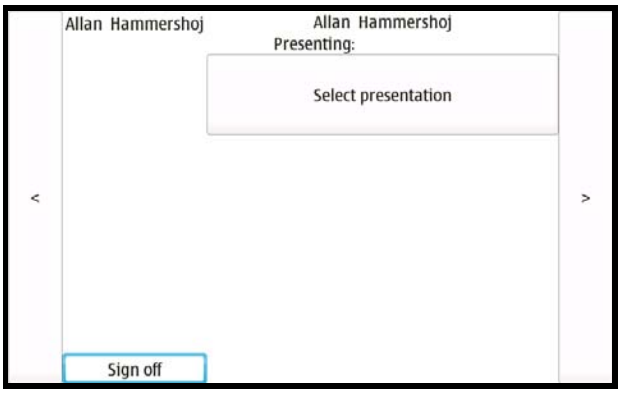


Figure 4-10: The main screen of the Presentation Service where the user has signed in. The name is automatically fetched from the user profile and the current virtual identity.

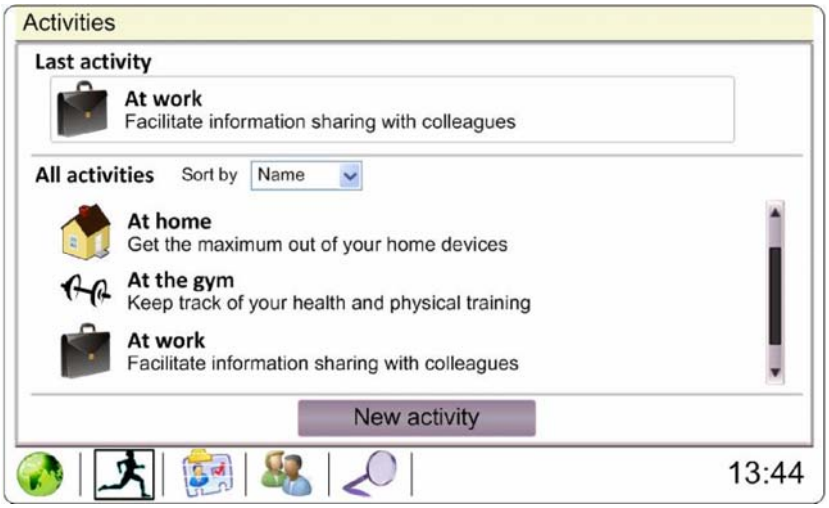
The user profile is also queried when the user signs up to give a presentation in the Presentation Service. Here the user name is queried, and the answer is based on the virtual identity the user has chosen in the given activity (see Sect. 4.4).

4.4 The activity concept and associated GUIs

As already discussed in Sect. 2.4, the activity concept developed during MAGNET Beyond and thoroughly described in [MBD1.4.1] is supported by the MAGNET user profile and the conceptual description originally presented in [MBD4.3.2]. In the following section screenshots from the actual implementations of the GUIs, prepared for the user test carried out in the final stage of the project and documented in [MBD1.4.3], will be explained from a technical point of view, illustrating how the different parts of the user profile support the design.

The conceptual design of the user profile in Figure 2-3 is capable of handling all of the different cases, in which the user profile is enabled, but for the sake of simplicity the detailed content of the different entries are not displayed in that figure. The basic profile data is mandatory and must be available in an up-to-date version on the user's device in order to actually have the PN framework running. Due to the concept of **activities** it contains more than just personal knowledge of the user. In the project, everything the user wants to do with a device is called activities, and these are accessed by the user as shown in Figure 4-11.

a)



b)

Figure 4-11: a) The activity menu on the user's device. Last activity was "At work". b) The manager screen. A tool called "Calendar" is selected. This tool is shared with three people and only visible in the activity "At work".

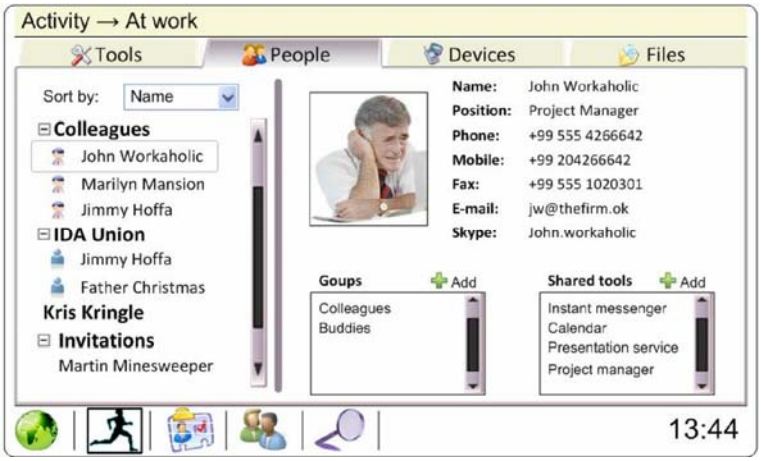
The activity concept is introduced to once and for all make up with the concept of everything being application dependent for the user. In the project, all applications are instead called **tools**, and services can enable the tools, as they are needed. The user gives or edits a presentation, in contrast to a traditional operating system like Windows, where the user opens a Microsoft PowerPoint file or so. Depending on what activity you are in, the amount and types of tools can vary. This does not mean that the tools are only available in a given activity, but they are rated individually, depending on their relevance for the given activity, and are per default hidden for the user. The user can select, whether the tools should be available or not. For example, if a user is currently in the activity "At work", tools relevant to the work are visible, but tools concerning private issues are not. The content, which is available using the tools, is also dependent on the activity. If the user wants to write an e-mail in the activity "At work", the e-mail will be sent using the business signature and card. Also mails relating to work are displayed. If searching for pictures only pictures relevant to the activity are found and not private pictures, if the activity is still "At work".

The tools can also be shared with other PN users if they are in a PN-F. This concept is shown in Figure 4-11, where a tool called "Calendar" has been added at some time, either by a service or manually by the user, when this was needed. The tool is shared with three MAGNET-enabled friends and the individual calendars can be read depending on the security settings of the PN-F. The tool is only visible in one activity, but can however at any time in any given activity be accessed with a few extra clicks. The different tool settings and the different activities with specific attributes all go into the basic user profile. However, if some of the services have extra data (apart from those defined that need to be stored), it will go into the 3rd party profiles of the user profile. This could e.g. be something like the user's history with the specific service.

The overall concept also goes for having different contacts and devices that relate to different activities. However, they all contain a lot of specific extra data for each entry.

An example of a MAGNET user available to another and how this user is handled is displayed in Figure 4-12. All MAGNET-enabled contacts are stored in the "Basic profile", but the devices are stored in the specific entry called "Devices". However, information on what groups and devices to be shown in a given activity is stored in the activity entry in the "Basic profile". The term "groups" refer to the titles "Colleagues" and "IDA Union" in Figure 4-12. They are called groups to the users, but they are technically speaking camouflaged PN-Fs, meaning that the users displayed in the different groups are members of a given PN-F with all necessary attributes stored in the PN-F profile and PN-F participation profile (PN-F part. prof.) as shown in Figure 2-3. When a new group is created by the user, the user can choose members and specific security settings, which all go into the PN-F related entries of the user profile. The device screen in the same figure shows an example of a laptop that is available in the given activity. It is called a preferred device, and this information is stored in the activity profile. The device profile displayed here is just user-friendly information. A lot more metadata on screen resolutions and other hardware profiling is stored in the "Device profiles" entry of the user profile (see Figure 2-3).

a)



b)

c)

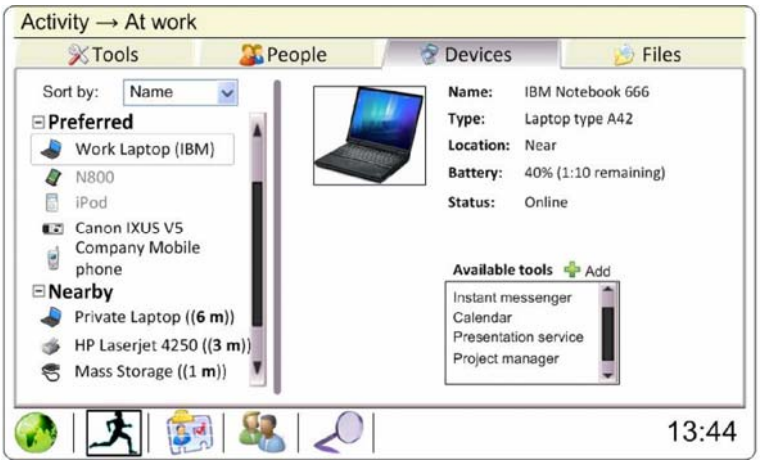


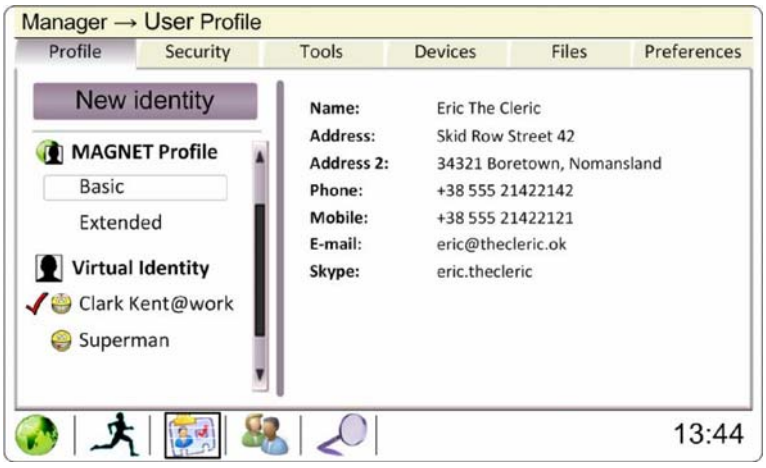
Figure 4-12: Screen displays. a) The different MAGNET users available in different groups. The user selected is available in two groups and has a lot of shared tools. b) The manager of the same person where specific information can be edited. c) An example of a MAGNET-enabled device with attributes and tools available.

Information about the user is handled in the manager of the MAGNET GUIs under the category “Profile”. Here, the personal data is divided into categories, which fit the user profile in Figure 2-3, as they have the same names. These categories or entries are called “Basic”, “Extended” and “Virtual Identity”. However, as an exception, the editable entry of 3rd party services goes into the entry of the same name in the user profile. The virtual identities are subsets of the basic profile with some data from the extended profile also, such as payment information etc. However, they are still stored in the same entry called VID with a unique entry per virtual identity.

The basic user profile information shown in the editor (see Figure 4-13) consists of personal information such as name, phone number and general contact information. In the extended profile information of payment methods and attributes relating to specific services are stored. The VIDs can be based on information from the basic and extended profile but can be fully customized if the user wants them to be. They even have an attribute called “Display name”, if the user wants to be presented with another name to other PN users, providing some degree of anonymity.

The last parts of the user profile are the security settings, which relate to all other user profile entries. These security parameters describe what data is available to whom or to what service. These parameters can vary depending on the selected VID or service and the PN user trying to interact with the user. These security parameters are called “Policies” in Figure 2-3 and are presented as subsets of the basic user profile and VID. This is just for the clarity of the figure. The settings also adapt to all other entries in the user profile as previously stated.

a)



b)

c)

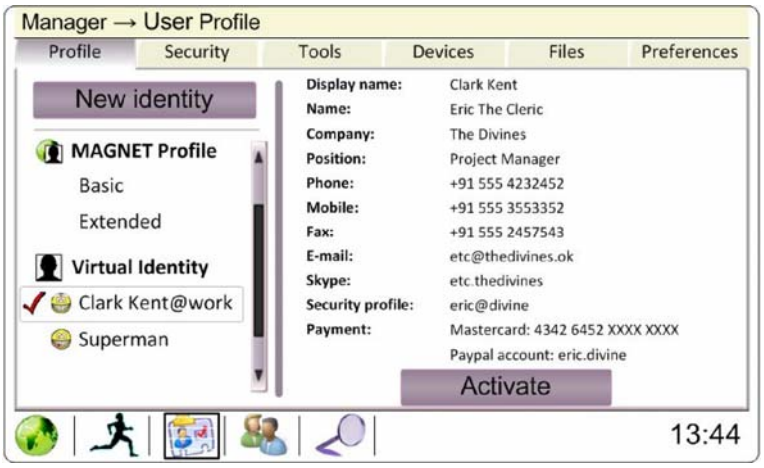


Figure 4-13: User profile editor for personal information about the user. The screens show an example of metadata in the a) "Basic", b) "Extended" and c) "Virtual Identity" entries.

5 Future perspectives

In this chapter, several future perspectives of personalization and applications of user profiles are discussed. The research carried out in this project relates to ongoing standardization activities, and Sect. 5.1 briefly reviews the status of these. As already discussed, the concepts and ideas developed in MAGNET Beyond have a lot of potential for advanced personalization and adaptation of services, if it is supplemented by the proper application or service logic, and some of these are discussed in Sect. 5.2. The concept of modalities (MODs) could form the basis for future service creation for service providers as well as end users. Other environmental interactions and current trends on social networking and privacy protection are also discussed. Finally, Sect. 5.3 addresses several future business opportunities that might originate or be based on the personalization concepts of MAGNET Beyond.

5.1 Standardization work on user profiles

In order to be able to adequately meet the need for user profile definition both for web applications and next generation mobile computing, we should consider standardization approaches from both of these areas. An early review of related initiatives and research projects was included in [MBD1.2.1], and the following is an update of that information. The most important initiatives are considered to be the European Telecommunications Standards Institute (ETSI) guidelines for User Profile Management, the technical specifications and service enablers developed in 3GPP and OMA, the W3C recommendations for description of device capabilities and user preferences, and the OpenSocial Foundation API specification for user profile. ETSI follows a more generic approach, trying to identify the framework under which personalized communication can be performed over next generation networks, while W3C 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, and the work of OpenSocial Foundation can be used to guide the adaptation of content delivered to devices.

5.1.1 ETSI

ETSI proposes guidelines for User Profile Management [ETSI 2005a] and suggests that details of the user and their personal requirements are included in a user profile, in a way that the system may use them to deliver the required behaviours and information in a profile. This may also be included for sharing a device or service with another person, while it distinguishes three different types.

5.1.2 3GPP

3GPP has released a series of technical specifications [3GPP GUP], which define a Generic User Profile (GUP) for 3G mobile systems. The ulterior goal of those specifications is to enable harmonized usage of user-related information originating from different domains. They aim at facilitating user preference management, user service customization, user information sharing, and terminal capability management as well as profile key access. In addition, they have started to develop Personal Network Management (PNM). The technical realization is focused on cellular network systems, IMS, WCDMA, (U)SIM and should be ready in H2 2008. The PNM standard is so new that it hasn't been analyzed in MAGNET Beyond.

5.1.3 OMA

OMA has many requirements in the user profile area. Most OMA service enablers reference and reuse XML Document Management (XDM) and shared XDM [OMA Shared XDM] that describes the data format and XCAP application usage for the shared document. In addition, there are discussions about starting a new OMA standardization effort around Converged Personal Network Service (CPNS) [OMA CPNS]. CPNS will enable services that use mobile phone or device as a hub of converged networks composed of cellular networks and Wireless Personal Area Network (WPAN) networks. The new work aims to investigate and analyze gaps with existing OMA enablers and other specifications (e.g. PNM in 3GPP) to clarify the necessity of the OMA CPNS service enabler. This OMA investigation is so new that it hasn't been analyzed in MAGNET Beyond. However, MAGNET Beyond has

been referenced as one R&D project in the area. As already mentioned in [MBD1.2.1] OMA also specifies the User Agent Profile [OMA UAP].

5.1.4 W3C

W3C has also issued a recommendation regarding profiles. More specifically, the [W3C CC/PP] defines a Composite Capabilities / Preference Profile (CC/PP) 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. The CC/PP Structure and Vocabularies 2.0 (abbreviated to CC/PP in the following) defines a client profile data format and a framework for incorporating application- and operating environment-specific features.

It should be noted that in [W3C CC/PP], the term “profile” does not refer to a subset of a particular specification, but rather to the document(s), which describe the capabilities of a device. The Resource Description Framework (RDF)[6] 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, an application such as a browser), and 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 and includes user preferences in terms of a number of "CC/PP attributes" for each component.

5.1.5 OpenSocial Foundation description

The OpenSocial [OpenSocial API, 2008] community is advancing the state of the social web. The aim is to make it easier for everyone to create and use social applications. Nowadays continuously more and more devices and gadgets need to give users a way of supplying user-specific information.

OpenSocial, a non-profit foundation jointly proposed by Yahoo, MySpace, and Google, provides a common way for websites to expose their social graph and more, by taking into account the user preferences (<UserPref>) section in the XML file describing 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, as well as specifying the different ways that an application can be viewed within an OpenSocial container.

5.1.6 Conclusion

When attempting to “compare” these initiatives, one can deduce that the guidelines and standards provided by ETSI and 3GPP are far more telecom-centric, OMA is network-agnostic, but with a mobile focus, whereas W3C and OpenSocial Foundation 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 work that has been done in the context of the MAGNET Beyond project, which focus on the provision of personalized services over Personal Networks.

Both OMA’s User Agent Profile and W3C’s CC/PP are examples of device profiles, which might be available from online repositories and retrieved to the “Device profiles” part of the user profile. For the user, however, the device settings and preferences are equally important as the device capabilities.

[6] http://www.w3.org/RDF/

5.2 Future applications of user profiles

5.2.1 Modalities (MODs)

The modality (MOD) concept introduced in [MBD4.3.2] follows the same idea as that of activities (cf. Sect. 2.4), and it would be possible e.g. to define specific GUIs based on the family of services selected for running in that moment. For example, if the user switches to an e-health application, one can easily foresee several activities related to patients, medical experts and support services. Specific alarms could be visualised on the device, if a doctor is needed, and subsequently set up a PN-F to solve a specific urgent health rescue.

Another possibility is to conceive a dynamic generation of GUI based on on-line generation engines installed on the device. In this case, again the User Profile can carry the relevant information for the generation of GUIs because it holds the information on policies and preferences.

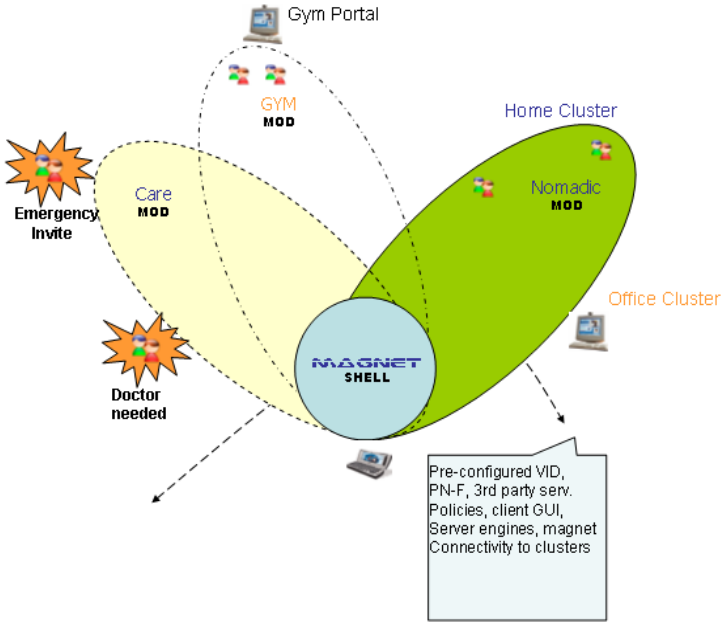


Figure 5-1: Examples of MODs based on user profile and context.

5.2.2 PN Service Creation Environment using MODs

With the advent of IP voice, services now are not restricted just to the domain of telephone calls (such as toll-free calls or voice VPN, etc.), but are moving toward integrated telephony and Internet services [Varshneya]. Providers must be agile, offering the right service features to the customers in a short time. Therefore, a service infrastructure is required that enables providers to create simple and relevant services quickly for their customers by hiding complexity.

This service infrastructure must give the carrier the ability to provision network services rapidly, and to enhance the order-management system and subscriber profile-management system to manage data used by the services. It must also enable the carrier to enhance the management systems to handle newer services, as well as the billing infrastructure to charge for such services.

Last, but not least, the carrier must be able to create the service logic for the new service. There are many proposals on how to create services and the two primary methods for developing the service logic: GUI-based development and "hand-coding".

Therefore in line with the above future work introduced on MODs and activity-based GUIs we consider in the following a possible PN Service Creation Environment (PN-SCE) for Pilots and related GUIs.

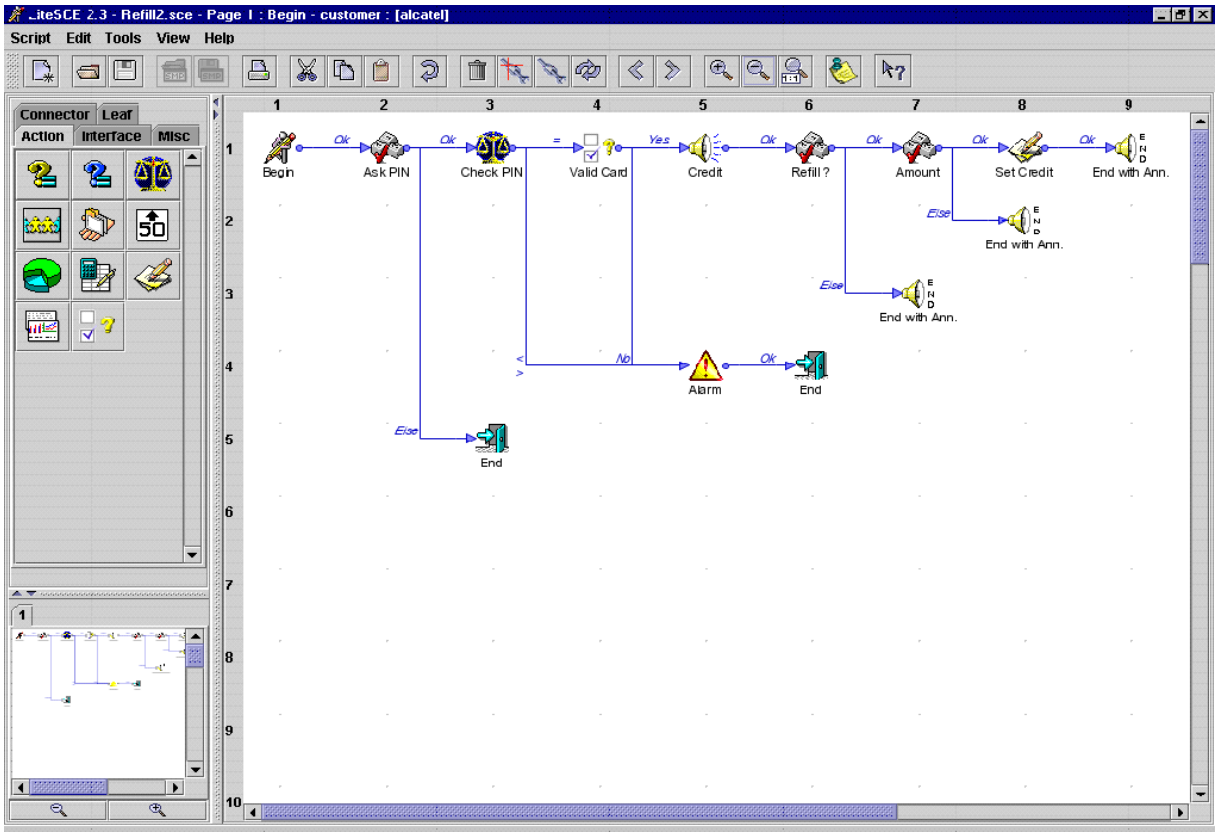


Figure 5-2: GUI based SCE example.

Some analogies with old-fashioned SCE for voice networks and Intelligent Networks can be found, because the concept of the call / session is still available in the pilots dealing with health care and GYM applications [MBD1.1.2]. The only difference is that many sessions would be initiated or terminated by the embedded systems or equipments available in the Pilot. For example, a drug dispenser could be the terminating device of a session initiated in the pilot engine based on the time. The user will accept the invitation to the session by retrieving the pills. The ring tone or alerting messages will be delivered on the mobile user device instead.

In the service-provider networks of today there are a number of different ways in which service features are incorporated into the service infrastructure, but they could all be put into the category of service creation. No matter what kind of service-creation system is used, they all involve creating service logic, i.e. the complex sequence of actions to deliver the features. Creating the service logic means implementing the flow of network protocol interactions, data modifications and control-flow decisions to deliver the intended features to the end user. Various scripting languages, such as CPL, SCML, and JAIN TM Service Creation Environment, are also used to specify the flow of the service feature, thus forming another mechanism for service creation.

Most service-logic execution environments (SLEEs) provide two mechanisms for writing service logic: a service-creation environment (SCE) based on a graphical user-interface (GUI) and hand-coding by programmers for the service-logic execution environment's APIs.

A key concept behind GUI-based service-creation environments is that of service-independent building blocks (SIBs). SIBs were software components that perform a well-defined function, i.e. a function that is a unit of execution in a service. Service logic is specified by designing a flow graph of connected SIBs. For the PN pilots specific SIBs could be conceived and eventually organized per family of applications like care, professional, lifestyle, or autonomic SIB components could be used in all kind of applications.

Requirements for the design of a PN-SCE should take into account that many originating and terminating points would be involved in a multi-session and that some of them will be processes and PN devices. Therefore, compared to a classical SCE, we expect that a PN-SCE would be more complex. In addition, if we take into account that the device GUIs may be activity-based, the service creation should probably also be designed to generate GUIs off-line. This is because of the distributed nature of the pilot applications and thus service creation environments may generate plug-ins/uplets for the user device impacting the GUIs as well.

The user profile ontology and its current setting may be also taken into account for the creation process, and the entire SCE may generate specific user profile templates for actors involved in a specific pilot.

5.2.3 Environment interactions

The user profile, here defined for PN purposes, is also in some way seen as an enabler of the interaction and preferences of the user vs. other environments having its own access network. The profile dedicated for examples to the 3rd party services could also host information to interact with these other environments. In particular, if we consider the access environment of health care and domotics (automation and controls of home/office) these are characterised by crescent level of embedded intelligence and security control functionalities (Figure 5-3). Sessions can be initiated from these environments and terminated for example to the users (alarms, push info, location-based info, security and news info, environment guidance). The user profile could include flags, identifiers, or white/black lists for allowances and data/device formats requirements. The result would be an enhancement of the user experience that will be also less fragmented in such a highly automated environment. In addition, the user profile will be a key factor for the convergence of other environments with standard telecommunication environments (data, voice, broadcasting and PN).

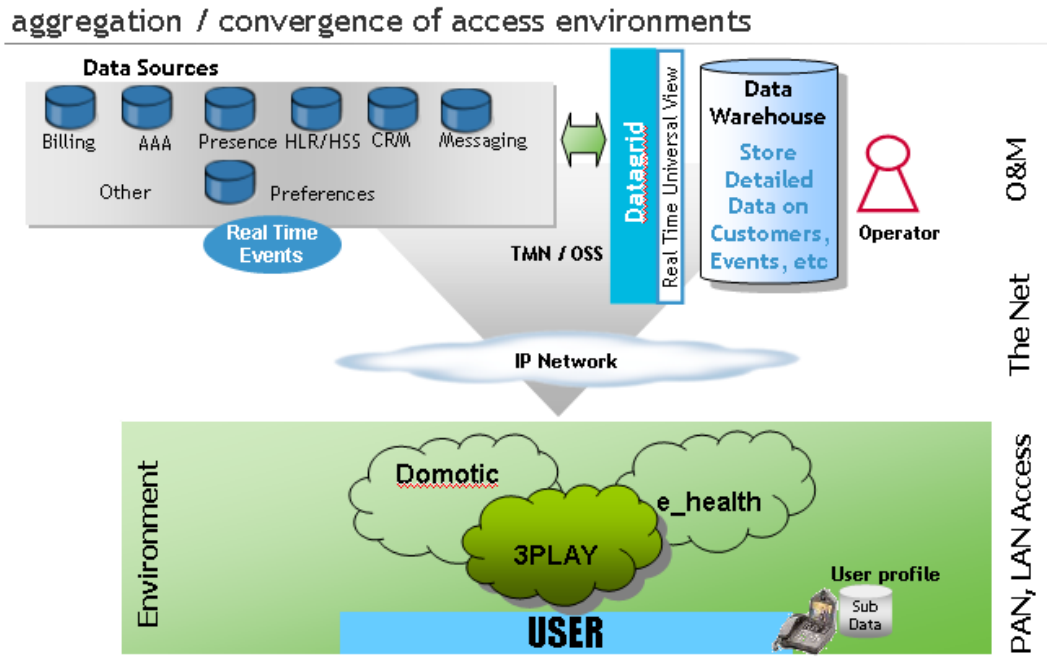


Figure 5-3: Interaction with other environments.

Figure 5-3 shows an example, where a user is included in a surrounding environment represented by local and personal access networks. Inside this environment we have depicted three relevant infrastructures: 3play (voice, data, broadcast), domotics and e_health. These infrastructures today and in the near future will contain distributed intelligence that will yield an enhancement of traditional, session-based user interactions. Therefore in addition to the hypothesis of using the user profile for han-

dling the PN interactions, there may be the needs to involve the user profile for other environments that for user safety and security reasons will need to communicate with users. Today, the standardization and industrialization of e_health, 3Play (telcos) and domotics is progressing with different paths although they are all based on ICT. It is important to define a kind of convergence between all the access environments around the PN users. The user profile should also play a key role towards these new processes and to enforce the role of service providers in overall.

5.2.4 Privacy and protection for the end users

The user profile is foreseen as an essential part of the PN framework to optimize services and networks for the user in given situations, while safeguarding privacy, especially when applications provide the possibility of external access on the profile data. But there is another aspect, namely that of costs.

A PN or PN-F owner, provider or administrator such as a private user, gym owner, a university or employer wants to keep down the costs of maintenance, content, development etc. and maybe hope to get some revenues. End users of both PN and PN-Fs might want to use services and networks free of charge.

Social networking is a kind of PN-F, which leverages user content and preferences. Most social networking sites and related Internet services are free and primarily based on advertisement and sponsorship revenues.

The same model will probably apply to some PNs and PN-Fs in the MAGNET Beyond scope. For example, for MAGNET Beyond´s Gym scenario, the gym owner wants to keep a low gym service cost and might want to use advertisement and sponsors to decrease the PN-F application costs and to pay maintenance and development of the gym PN-F service. Gym owners can offer companies to purchase user behaviour data and user profile preferences that they can use to target key groups. So personalized advertisement will be presented besides the normal application data.

However, this involves interfering user activities with a number of user privacy issues and recently the amount of unique visitors as well as the visiting time have dropped to several community services. Privacy seems to be one of the key user issue to any personal network and especial for PN-Fs. The press has outlined many privacy issues such as:

- tracking user behaviour on other websites such as Facebook´s Beacon
- searching persons by organizing search results from all over the web on one web page as Wink.com. Most people don’t know their profile, and the profiles are often wrong or mixed by several persons.
- building a user profile around a search pattern that is revealing quite a lot of a person's lifestyle. Many people search for their own name from time to time and coupled with other indicators many searches could be associated, rightly or wrongly, with individuals as previously done by AOL.

MAGNET-enabled users will probably be better prepared for privacy control. Users will have the freedom to create and customize their profiles and policies. Default values should be accurate. For example the parameters to open up user profiles for advertisement should be shut off from the beginning. It is also important to clarify if a specific service is provided within the home PN domain or offered by a service provider outside the relative more secure home PN domain.

However, there is also a need to increase the user awareness and knowledge about the privacy issues. Advertisers need to know how far they could go, as long as a service is free of charge. How could advertisement be more relevant and subtle enough to not offend users? Operators, Internet players, service providers, content owners etc. could e.g. in partnership develop an access control that parents can use to block access to unsuitable social networking services.

The solution to find a balance between protection of privacy and sharing of user profile preferences and information is possibly a mix of technology (as described in Sect. 3.2), education/public awareness and collaborations.

5.3 Future business opportunities

The identification of business opportunities is carried out by investigating the value proposition of the solutions being proposed. According to [MBD1.5.4] there are many different roles for different players and of course combinations. Future business models will even increase the flexibility of roles and actors and the borders will blur. But what are the roles of user profile?

User profiles can be seen as a supporting enabler – directly or indirectly – for:

- mobile operators to get better ability to service and content provision and other management features based on user profile data. Mobile operators will get better ability to provide value-added services (internal or external) personalized by user profile data.
- PN providers to integrate different services and to offer them as one simple package to users based on user profile and other user related information. The PN provider is also a possible stakeholder for management and storage of user profiles (see below).
- service providers to acting as a personalization provider (PeP) working in collaboration with the relevant identity providers (IdPs) to define unique mobile value-added services [MBD4.3.2]. The service provider is among the stakeholders that are most dependent on the content of the user profile, as many services can be adjusted according to it.
- Identity Providers to be able to access the MAGNET user profile for relevant data. Identity provider can act as a digital representative predicting the needs of a user, finding the relevant services, exchanging user information based upon the user's policies and making the service value-added before presenting it to the user.
- device manufacturers and content providers to be able to offer independent device-based services from networking to applications and client software based on user profile data.
- content providers to get better ability to adapt content to user requirements depending on device, location and user preferences.

Some of the business areas are described in more detail in the following.

5.3.1 Provisioning of PN services and user profile administration

MAGNET Beyond has studied possible scenarios suitable to create a business for the actors involved in provisioning and federation of Personal Networks. Besides the marketability of the PN/WPAN-based services like those described in this deliverable and deployed as pilot services, a possible candidate for business analysis could be the **subscriber data administration**, i.e. the possibility for a PN Service Provider to handle the subscriptions of users, who are using the MAGNET Beyond technologies and services available in the PN or PN-F. The utilization of a synchronized external user profile server such as the MAGNET User Profile (MUP) would give the possibility to administrate off-line profile info, settings and preferences and will provide global multimedia mobility to the subscriber. In addition to this, some cross-queries and overall search functions over entire communities of PN subscribers would be possible only by utilizing a server approach methodology, since all single profiles would only be stored within the personal devices of the users.

The MUP is considered an option that will be introduced for scenarios, where there is a need to administrate subscriber data and extended user profile information, which does not need to be storable in the user's device(s). This is the case when it only applies to data needed for access to another PN or SPN. As stated earlier, the MUP server would also be the place to store the newest version of the entire user profile, when switching from one main device to another in the PN or more precisely in the dynamically created P-PAN. However, if the device with the newest profile is not online with the MUP server

when switching device, versioning problems could occur. Hence, a simple versioning system is mandatory to ensure that no updates are lost.

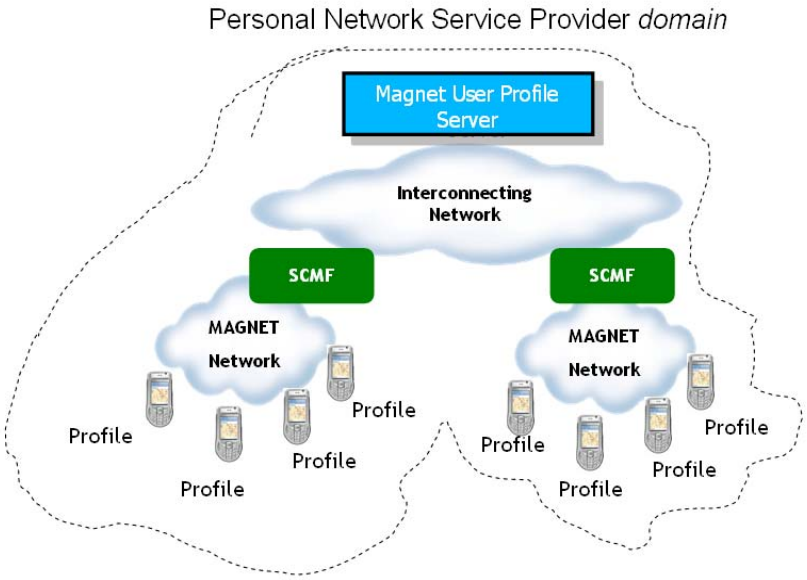


Figure 5-4: MUP-based scenario.

Some big Internet players like Google, Yahoo and eBay are already acting as trusted brokers for basic user information and preferences. There are in fact many Internet services or portals that require users to be already subscribed with the above players (acting as brokers), giving the advantage for this portal of reduced costs for the administration of the profiles. Therefore, in addition to the PN-only scenario (Figure 2-1) there will be a scenario where a community of PN users subscribes to a PN provider that will manage the profiles and will provide a bouquet of applications or services, including the possibility of forming PN-Fs.

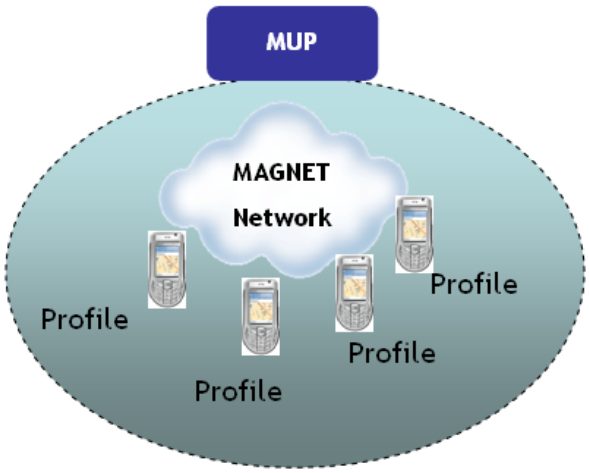


Figure 5-5: PN Service Provider domain.

The above figure shows a medium-term scenario, where an operator will administrate the subscriber data, including PN profiles, of all its customers. Probably the operator will have either or both the role of access and PN service providers. As said above the additional role would also be as broker towards 3rd party services.

In addition to the possibility of having a domain where the subscriber data are administrated by a single provider, there would also be a scenario with more than one domain as shown in the next figure.

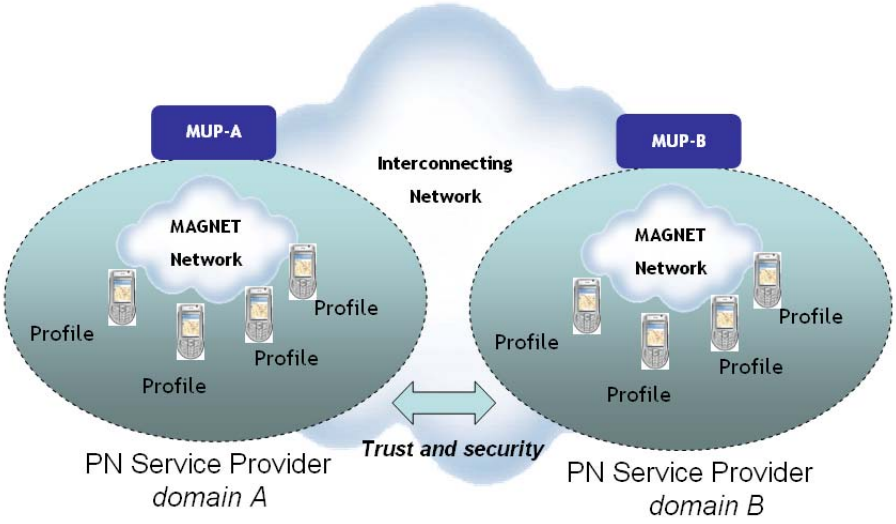


Figure 5-6: Interaction between PN Service Provider domains.

The figure shows a long term PN business evolution, where two domains belong to different providers. This scenario is similar to the current situation about mobile operators or virtual mobile operators that have the need to administrate subscriber data and profile information of large user communities dealing with multimedia services and personalization.

It is clear that two main players could be imagined around the network personalisation:

- Application providers: Providers and administrators of specific applications (i.e. care, professional, life style, gym, workshop servers) based on PN technologies that will serve communities of users with MAGNET-enabled devices and PN services like the pilot services described in this project. The access to these services probably will be done via clients having security, gateway functionalities and access to the core MAGNET network. We can also say that those servers will be MAGNETized.
- Core PN service providers: Providers of core MAGNET software. Probably the main role for them is to deliver an update of clients and ensure compatibility between networks and devices. Once a kind of common standard is defined at least for the network layer of the PN, it is possible that an overlay network, dealing with PN communities[7], would come to exist.

If we take into account the above providers, it is obvious that both will need to administrate subscription of users and preferences. A tailored MUP server could be assigned to each application provider, who would like to follow customized rules for access and authorisation. As for today, if the subscriber data management is done only within the application provider domain, we will face yet again a fragmented user experience (Figure 5-6), which is not user-centric at all. Vice versa, if the overlay PN is globally diffused, there will also be needs for operation and administration of the network and the need to administrate the registered users. A user that will make a subscription for the utilisation of a client to MAGNETize his environments.

Issues related to the security and domain roaming should therefore be considered. These aspects are again possible evolutions in the long run, but have not been addressed within the project plan. However, some of the achievements made on the security aspects and demonstrations of pilot services rep-

[7] PN user communities allowing single users to MAGNETize personal devices and several remote clusters like home, office, gym, personal storage clusters etc. and who have the possibility to create PN-Fs with other users. This overlay PN would be interoperable with the IMS standard.

resent a good starting point for discussing inter-domain and roaming issues for subscribers of PNs, eventually complemented with existing status of 3GPP/IMS standardization efforts towards the specification of future 4G systems.

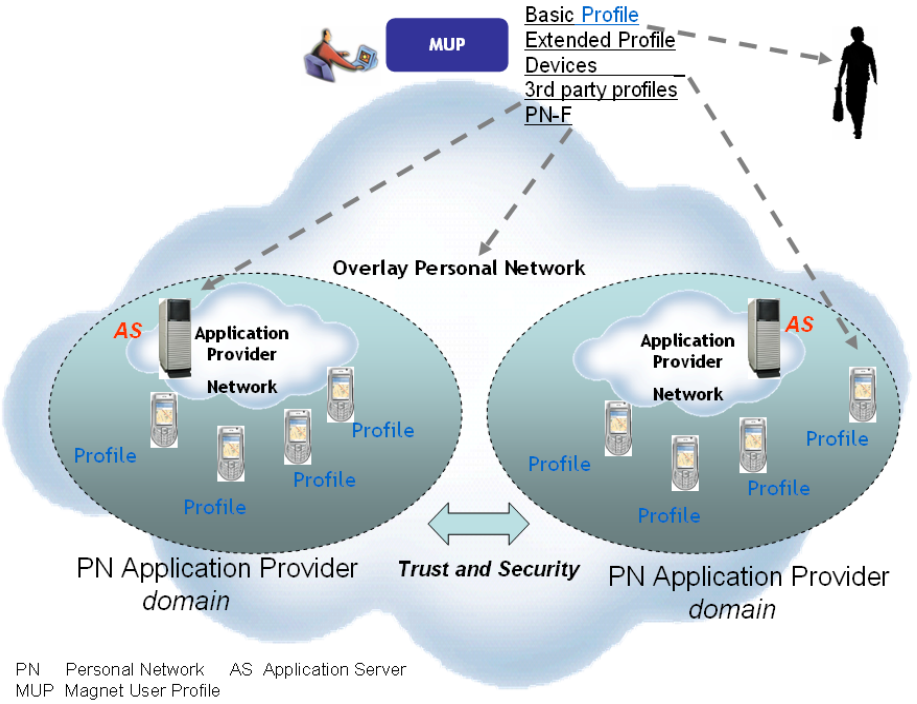


Figure 5-7: Overlay PN domain.

Under the given scenario it will be more appropriate to allocate the administration of subscriber data for a global village of PN community (Figure 5-7) and thus to interoperate with application providers via PN service providers and a user's MUP.

5.3.2 Pilot services

The two pilots of the project are well chosen to illustrate service categories, where the strategic decisions are different in nature. In the Icebreaker case, the number of users of the service is important. When entering a conference, it is important for the value of the service to the users whether all participants are on the system or whether just a few participants have subscribed. There are network effects: the value of the service increases with the number of users of the system. Here, the extrinsic value of the service is important.

In the case of LifeStyle Companion, the value of the service to the individual user is not dependent on how many other users are subscribed. The value of this service is in its intrinsic character, i.e. the measurement of the blood glucose level, etc. There can also be extrinsic value related to the networking of different people using the same service, but the importance of the network effect is far smaller than in the Icebreaker case.

These matters have an influence on the business modelling and strategic options of the companies involved in delivering the services. Although it is possible that different conferences and fairs etc. will use different 'Icebreaker' systems, which means that the network effects are only local at the specific event, it is very likely that a limited number of 'Icebreaker' systems will be used and that the network effects transcend the individual events. This means that it will be important to be among the first providers of such systems, as there is a lock-in effect to the systems once implemented. There will be a 'first mover'-effect, which is part of the strategic concerns of companies.

In the local context – the individual conference, for instance – the network effect also has consequences. If conference participants are offered the Icebreaker service as a specific offer, only some of

the participants will subscribe, and this again will limit the value of the service, as not all will be available via the system. A more obvious strategic choice is to include the payment for the service in the general participation fee, as this will secure that all participants are on the system. In the wider context, it can be a strategic choice to offer the service for free at first in order to get as many users on the system and in that manner profit from the positive network effects.

In the LifeStyle Companion case, pricing is also a central issue. It is important for the take-up of the service that the service is priced rightly in accordance with the value perception that the users have of the service. Furthermore, single sign-on is seen as important for the users. It can be inconvenient for the users if they have to pay for each individual service. For the operators of the services it is an advantage to offer packages or bundles of services, as bundles lock in the users to the service provider. There will be switching cost for the users in changing providers of either single services of the whole package.

5.3.3 IMS Group Management

Personal Networks are a radical new concept that allows users to connect and combine their personal devices at their own command. PN-Fs extend the concept to a full and highly secure service platform for the ubiquitous, always connected world. The combination of wide-area distributed PN with an external service platform such as IMS provide unique features and advantages for user friendly and powerful new services [Kovacs 2008].

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, IETF and 3GPP have specified Group Management functionality using different technologies such as web services, SIP or XCAP [Parlay X], [XCAP].

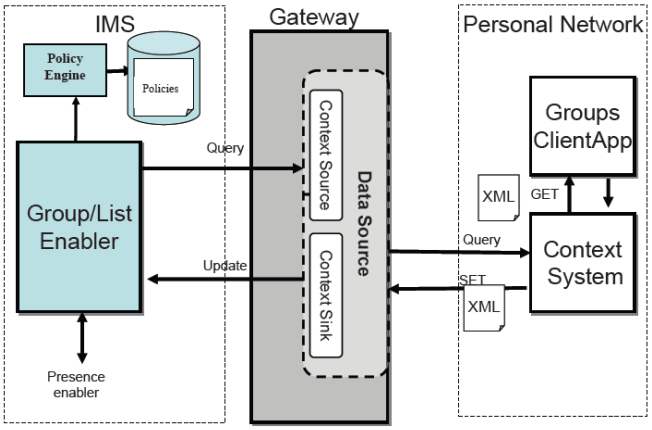


Figure 5-8: PN interactions with the IMS Group/Document Management Enabler.

Concerning the access and usage of centralized groups in IMS from inside of a PN, the benefits arise when the group information is not private to the user but shared by an organization or community. The architecture for inter-working is shown in Figure 5-8. The PN user application (on any device) initiates a query or update 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.

5.3.4 Offering personalized and blended services

As a consequence of network convergence, telcos and service providers are pressured to deliver personalized services to the customers mixing multiple devices, services and more often managing more than one network. For network operators, a general user profile architecture deals with subscription

management and stacks of databases using different formats. Figure 5-9 shows the databases that typically are going to be considered in IMS / NGN.

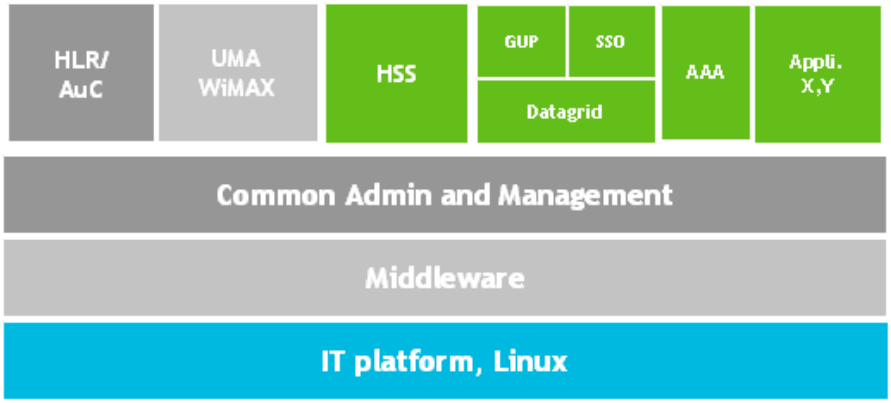


Figure 5-9: IMS databases.

To compete more effectively, capture, and grow market share, all service providers need the ability to go beyond offering bundled services. They must now provide personalized, blended services that span individual types of access methods and devices (Figure 5-10). To do this, service providers need to make their networks more agile. A key element to facilitating network agility and strategically positioning a service operation to have the flexibility to shift business paradigms is to maintain simplification and control of subscriber data. It is also important to outline how these efficiencies allow service providers to transform a cost structure into a revenue structure that offers the opportunity to monetize their network.

The business environment for service providers is changing almost on a daily basis. Service providers who at one time provided services that complemented one another – mobile operators providing voice, cable operators providing video, Internet service providers enabling broadband – are now colliding and competing for the same subscribers.

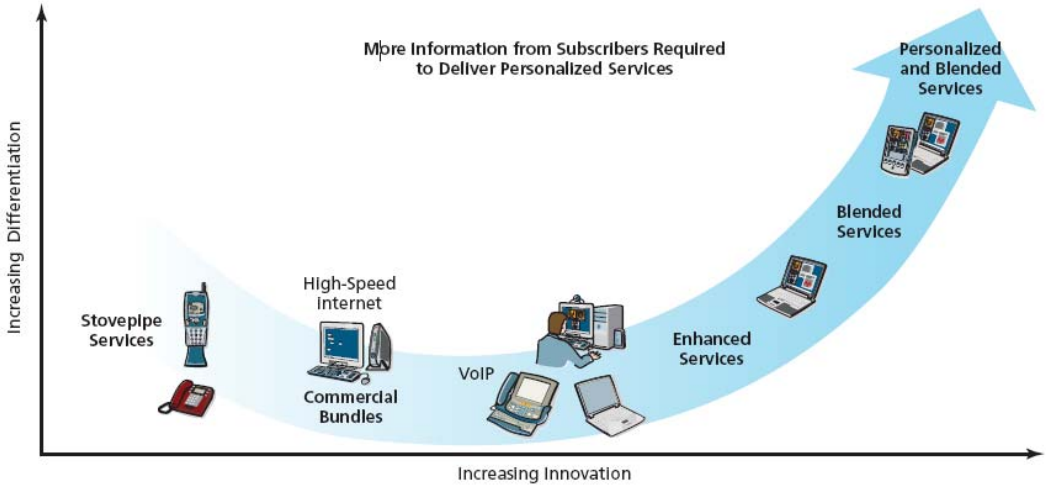


Figure 5-10: Trends for personalisation and blended services.

To do this, service providers need to make their networks more agile. By establishing network agility, service providers have the freedom to offer services that are:

- Access- and connectivity-agnostic
- More convenient for subscribers

- Enhanced by subscriber-relevant information
- Available everywhere
- Facilitators of business transformation

From an operational efficiency standpoint, an agile network environment allows operators to:

- Rapidly create and deploy new services
- Expedite provisioning
- Support flexible rating, charging and billing
- Enable easy-to-manage service level agreements (SLAs) and quality of experience (QoE)

Service providers, who want to transform their business and create new revenue streams by establishing network agility, must deal with several issues before they can begin to offer personalized, blended services. Many service providers today authenticate and authorize services by managing subscriber data through traditional methods, cf. Figure 5-11. Mobile operators may use home location registers (HLRs). Broadband Internet service providers may use authentication, authorization and accounting (AAA) servers, while in IMS networks, subscriber data is encapsulated in a home subscriber server (HSS).

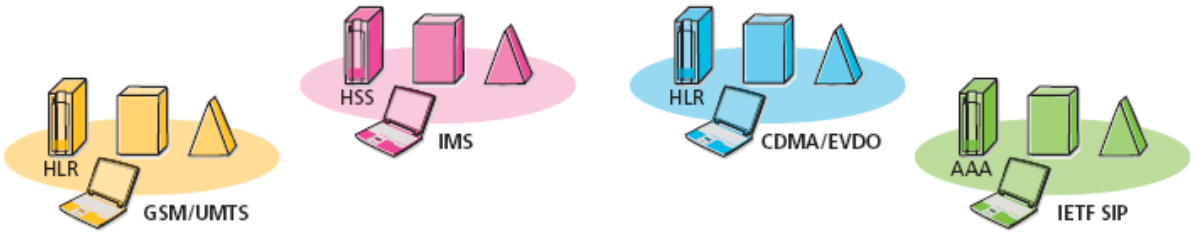


Figure 5-11: Overview of traditional networks [Ballot 2008].

To offer services that are access- and connectivity-agnostic and available everywhere, service providers must ensure services are available to the same subscriber across multiple networks and domains. But using multiple data stores to support individual services, networks and domains, creates independent databases. These databases are often independently managed, administered and uniquely provisioned. As a result, subscriber profile data records are often duplicated, fragmented or out-of-date and out-of-sync. This leaves service providers to deal with:

- Multiple network components with different database schemas, data models and northbound data interfaces
- Multiple applications accessing data from multiple components
- Heterogeneity (NxM connectivity) issues, which create an additional expense for applications
- Data that cannot be directly shared across network components or applications
- Redundant and overlapping data
- Complicated customer care processes created by the need to access multiple databases for customer care issues
- Difficulty personalizing services because profile data is not easily accessible
- Difficulty creating services that span multiple domains

All this leads to “dirty data”. In fact, it is estimated [Yankee Group 2006] that:

- Up to 50% of existing access network records have some level of inaccuracy

- Up to 50% of access network faults are related to inaccurate data
- Dirty data will cost U.S. and European operators USD $6.3 billion per year by 2010

The Subscriber Data Management (SDM) solution [Ballot 2008] is an example of a commercial product that allows service providers to deploy a single, virtual repository of subscriber data on- and off-the-shelf IT- or telco-grade platform that is configurable for high-availability, high-reliability and geographical redundancy.

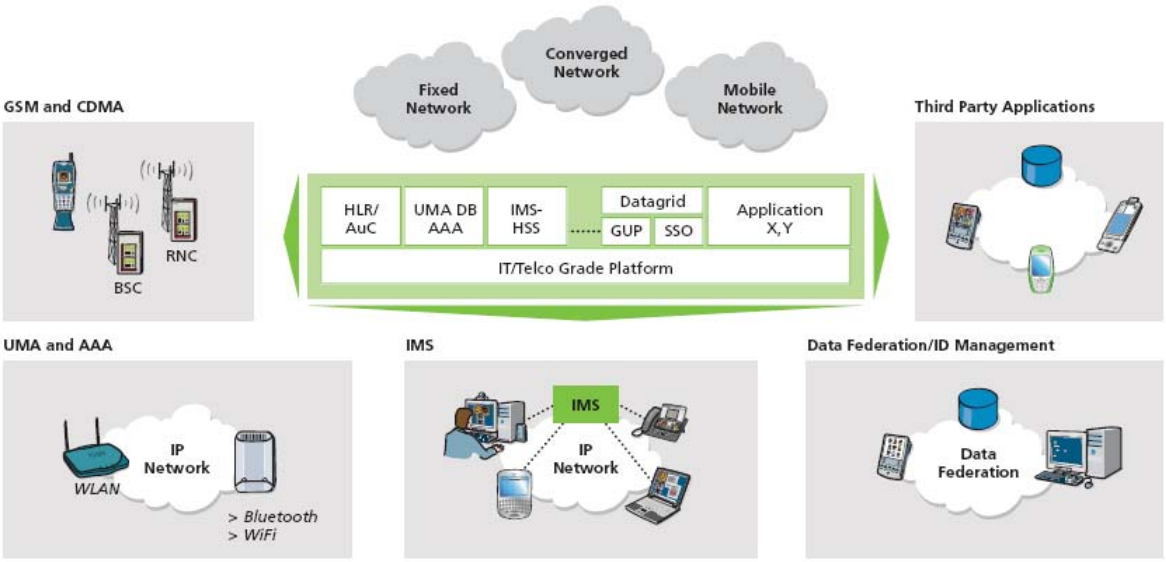


Figure 5-12: Subscriber data management across different networks [Ballot 2008].

This solution eliminates the risk of duplicate data and gives service providers the opportunity to reduce the operational costs of managing subscriber profile information. As a result, service providers can simplify the management and administration of subscriber profile data across multiple networks.

Simplification comes from being able to provide a common subscriber profile combined with the needed HLR, HSS and AAA services. In addition, with its unique architecture, the Alcatel-Lucent SDM solution supports multiple fixed, broadband and wireless networks simultaneously, including:

- CDMA/EV-DO
- GSM/GPRS/UMTS
- IMS/Broadband networks
- WiFi/WLAN and WiMAX
- UMA/FMC

Therefore, it may represent a possible architecture to cope with the subscriber data administration of PN eventually, as extensions or gateways for the IMS are already handled.

6 Conclusions

At the end of the MAGNET Beyond project a comprehensive and versatile framework for user profiles has been developed. The conceptual model has been implemented as an integral part of the PN service architecture, and the difference between user profile and context information has been clarified. Both types of information can be stored and managed in the Secure Context Management Framework, and both are important for adapting and optimizing services, device settings and user interfaces for the end user under a variety of conditions.

The user profile consists of several parts or sub-components: the basic profile, the extended profile, device profiles and settings, the PN-F participation profile and 3rd party profiles. A common ontology for user profile and context information has been developed and implemented. This represents the common representation of the "domain" of use, and the ontology is an important element for the adaptation of services. A limited version of the ontology has been implemented and used in the pilot services, and more sophisticated reasoning and decision-making is enabled for future use.

Even though user profile and context information originate from different sources and are quite different in nature, they can be handled and managed in a similar way, which has been one of the main objectives of the work. Throughout the project there has been a close interaction between the work packages dealing with user aspects, the PN architecture, and security, trust and identity management. This has resulted in a more unified view and better coherence of approaches. The concept of Virtual Identity (VID) is one of the useful results of this collaboration. It was originally developed in the IST DAIDALOS project, but has been incorporated and adapted in the PN framework. Combined with the concept of activities from MAGNET Beyond it enables sophisticated personalization and adaptation of services and GUIs for the end users.

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 provides the framework for the definition of a clear standard towards user profiles that incorporate context-aware information management. Of course, the unification of the existing proposals requires further work in order to present a core standardization proposal for user profile management.

The research on user profiles in MAGNET Beyond adds important contributions to ongoing research and standardization work, and several ideas for future work and creation of new business opportunities have been discussed. Among these is the provisioning of PNs and associated pilot service applications and the enabling of PN-assisted service creation. The results can also be seen as an important extension to the IMS framework and could enable a much better subscriber data management for future personalized and blended service offerings. For the end users protection of privacy is always a major concern, and the framework of MAGNET Beyond could significantly improve personalization and control of resources and personal information compared to existing solutions.

References

[3GPP GUP] *Service requirement for the 3GPP Generic User Profile (GUP); Stage 1, (Release 6),* 3GPP Technical Specification Document TS 22.240, Version 6.5.0, Jan. 2005;

Architecture, Stage 2, (Release 6), 3GPP Technical Specification Group Services and System Aspects TS23.240, Version 6.7.0, March 2005;

Network, Stage 3, (Release 6), 3GPP Technical Specification Group Core Network and Terminals TS29.240; Version 6.1.0, June 2005.

[Ballot 2008] J.-M. Ballot, A. Bultinck, T. Dewitt, and H. Menendez, "Simplifying the User Experience while Enabling the Profitable Evolution to All-IP Mobile Transport", Enriching Communications, Vol. 2, Issue 1, 2008, Alcatel-Lucent, available online at http://www.alcatel-lucent.com/enrich/v2i12008/article_c4a2.html.

[Dey00] A. K. Dey, "Providing Architectural Support for Building Context-Aware Applications", PhD thesis, Georgia Inst. Tech., USA, Nov. 2000.

[ETSI 2005a] ETSI Guide (2005a), Human factors (HF); User profile management, , EG 202 325 v1.1.1, Retrieved May 15, 2007, from http://webapp.etsi.org/action/PU/20051018/eg_202325v010101p.pdf.

[Kovacs 2008] E. Kovacs, D. Kraft, A.Cimmino S. Bessler, M. Ghader and L. Gavrilovska, "Personal Networks as Distributed Clients for IMS", ICT Mobile Summit, Stockholm, June 2008.

[Liberty] The Liberty Alliance Project: http://www.projectliberty.org/.

[MBD1.1.1] IST-027396 MAGNET/B/WP1/Task1/D1.1.1, "MAGNET System and Pilot Service Design Specifications**",** Dec. 2007.

[MBD1.1.2] IST-027396 MAGNET/B/WP1/Task1/D1.1.2, "Pilot service implementation specification**",** June 2007.

[MBD1.2.1] IST-027396 MAGNET/B/WP1.2/DTU/D1.2.1/R/PU/001/02.10.2006, "The conceptual structure of user profiles", September 2006.

[MBD1.4.1] IST-027396 MAGNET Beyond Deliverable D1.4.1, "Usability of PN services (low-fi prototyping)", June 2007.

[MBD1.4.2] IST-027396 MAGNET Beyond Deliverable D1.4.2, "Defining usability of PN services", Dec. 2007.

[MBD1.4.3] IST-027396 MAGNET Beyond Deliverable D1.4.3, "Usability testing of pilot services", June 2008.

[MBD1.5.4] IST-027396 MAGNET Beyond Deliverable D1.5.4, "Analysis of strategy options", May 2008.

[MBD2.3.1] IST-027396 MAGNET/WP2.3/DUT/D2.3.1/PU/001/15.01.2007, "Specification of PN networking and security components", Jan. 2007.

[MBD2.3.2] IST-027396 MAGNET Beyond Deliverable D2.3.2, "MAGNET PN secure networking frameworks, solution and performance", June 2008.

[MBD4.3.2] IST-027396 MAGNET Beyond Deliverable D4.3.2 (D1.2.2), "Specification of user profile, identity and role management for PNs and integration to the PN platform", retrieved May 15, 2007, from Internet http://www.ist-MAGNET.org/public+deliverables.

[MBD4.3.3] IST-027396 MAGNET Beyond Deliverable D4.3.3, "Solutions for identity management, trust model and privacy for PNs", June 2008.

[OMA CPNS] *Converged Personal Network Service*, Open Mobile Alliance BoF (new work study), http://member.openmobilealliance.org/ftp/Public_documents/TP/CPNS/2008/

[OMA Shared XDM] *Shared XML Document Management*, Open Mobile Alliance Technical Specification, OMA-Shared_XDM_Specification-V1_0-20050129-D, approved version 1.0. Jan. 2005.

[OMA UAP] *User agent profile*, Open Mobile Alliance Technical Specification, OMA-TS-UAProf-V2_0-20060206-A, approved version 2.0. Feb. 2006.

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

[Parlay X] http://www.parlay.org/en/specifications/

[ucentric] S. Grégoir and H. Verbandt, "Alcatel's User-Centric Data Repository and provisioning Architecture", Alcatel Telecommunications Review, 4th quarter, 2005. Available online at: http://www.alcatel.com/com/en/appcontent/apl/T0512-User-Centric_DATA-EN_tcm172-521371635.pdf.

[XCAP] *The Extensible Markup Language (XML) Configuration Access protocol (XCAP)*, J. Rosenberg, November 16, 2004, URL: http://www.ietf.org/internet-drafts/draft-ietf-simple-xcap-05.txt.

[Varshneya] A. Varshneya, "Service Creation in Next-Generation Networks", http://www.newtelephony.com/newsvoices/0CFF1022-46DE-448A-9FD6-B55C4D7BDC80.html.

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

[Yankee Group 2006] C. Mendler, "Dirty data threatens next generation broadband", Yankee Group report, 2006, see e.g. http://www.telecomprophet.com/issue1/issue1.pdf (retrieved June 20, 2008).

Abbreviations

3GPP	3rd Generation Partnership Project
BC	Business Card
CA	Context Agent
CALA	Context Access Language
CAM	Context Access Manager
CASM	Context Aware Security Manager
CC/PP	Composite Capabilities/Preferences Profile
CPNS	Converged Personal Network Service
DSA	Data Source Abstraction
ETSI	European Telecommunications Standards Institute
FM	Federation Manager
FMC	Fixed Mobile Convergence
GUI	Graphical User Interface
GUP	Generic User Profile
HTTP	HyperText Transfer Protocol
IdP	Identity Provider
IETF	Internet Engineering Task Force
IP	Internet Protocol
IMS	IP Multimedia Subsystem
MAGNET	My personal Adaptive Global NET
MOD	Modality environment
MUP	MAGNET User Profile
NGN	Next Generation Networks
OMA	Open Mobile Alliance
OSS	Operation Support System
OWL-DL	Ontology Web Language – Description Logics
P-PAN	Private Personal Area Network
P&S	Processing and Storage
PE	Policy Engine
PeP	Personalization Provider
PIP	Personal Identity Provider
PN	Personal Network
PN-F	Personal Network Federation
PNDS	Personal Network Directory Service

PNM	Personal Network management
PU	Processing Unit
RDF	Resource Description Framework
RPC	Remote Procedure Call
SCE	Service Creation Environment
SCMF	Secure Context Management Framework
SDM	Subscriber Data Management
SIM	Subscriber Identity Module
SIP	Session Initiation Protocol
SLEE	Service-Logic Execution Environment
SPN	Service Provider Network
UAProf	User Agent Profile
UMA	Unlicensed Mobile Access
UMTS	Universal Mobile Telecommunication System
USIM	Universal Subscriber Identity Module
VB	Virtual Badge
VID	Virtual Identity
VPN	Virtual Private Network
W3C	The World Wide Web Consortium
WCDMA	Wideband Code Division Multiple Access
WP	Work Package
WPAN	Wireless Personal Area Network
XCAP	XML Configuration Access Protocol (XCAP)
XDM	XML Document Management
XML	Extensible Mark-up Language

List of figures

Figure 2-1: Basic PN-F scenario. 7
Figure 2-2: Access to third party services. a) Basic personalization targeting a standard user. b) Enhanced personalization targeting a MAGNET-enabled user. 8
Figure 2-3: MAGNET user profile in a conceptual representation displaying the different categories and dependencies [MBD4.3.2], compared to state-of-the-art. 1
Figure 2-4: Conceptual structure of the VID in MAGNET relating to both user profile (upper part) and policy data (lower part). 1
Figure 2-5: Conceptual MAGNET GUI design where the red circle marks the VID icon of the user. 12
Figure 2-6: Policy decisions in the PN-F life cycle. 1
Figure 2-7: Public part of the PN-F profile. 14
Figure 2-8: Private part of the PN-F profile. 1
Figure 2-9: Overview of the Integrated SCMF Ontology. 16
Figure 2-10: User profile part of the Integrated SCMF Ontology. 17
Figure 2-11: Properties of the FitnessCenterProfile. 18
Figure 2-12: MUP Extended User Profile. 18
Figure 3-1: Overview of a Context Agent with active components. 19
Figure 3-2: Example configuration of Context Agents in a PN with connection to another PN in a PN-F scenario. 20
Figure 3-3: Security Policy Enforcement Algorithm [MBD4.3.3]. 21
Figure 3-4: Policy decision point for the protection of context. 22
Figure 3-5: Context-based reasoning. 23
Figure 3-6: The basic GUP architecture [ucentric], [MBD1.2.1]. 23
Figure 3-7: PN agents forming the SCMF and communicating with the MUP server through a gateway using CALA. 24
Figure 3-8: Message sequence chart showing the interactions of the SCMF, gateway and MUP server. 24
Figure 3-9: MUP server high-level architecture. 25
Figure 3-10: Overview of a MAGNET-enabled user with an optional "Digital Butler" communicating with a 3rd party service provider. The orange arrows are only meant as the components having connectivity [MBD4.3.2]. 26
Figure 4-1: Icebreaker GUI. 27
Figure 4-2: Basic User Profile. 28
Figure 4-3: Attributes of *DetailedProfessionalProfile.* 29
Figure 4-4: Properties of the TrainingProgramme. 30
Figure 4-5: Properties of the Exercise. 30
Figure 4-6: Interaction model with bicycle and illustration of how the SCMF is being used for storing and distributing user profiles related to the bike settings and training program. 31

Figure 4-7: Overview of how the weight of the user is obtained through a scale retriever and made accessible through the SCMF. 32

Figure 4-8: Illustration of how the distance between objects are obtained and used to trigger events at the application when being near the specified object, here the bicycle and the scale. 33

Figure 4-9: The booking system of the Presentation Service. The phone number is not displayed when the booking is registered, but the booking is stored under this identifier. 34

Figure 4-10: The main screen of the Presentation Service where the user has signed in. The name is automatically fetched from the user profile and the current virtual identity. 34

Figure 4-11: a) The activity menu on the user's device. Last activity was "At work". b) The manager screen. A tool called "Calendar" is selected. This tool is shared with three people and only visible in the activity "At work". 35

Figure 4-12: Screen displays. a) The different MAGNET users available in different groups. The user selected is available in two groups and has a lot of shared tools. b) The manager of the same person where specific information can be edited. c) An example of a MAGNET-enabled device with attributes and tools available. 1

Figure 4-13: User profile editor for personal information about the user. The screens show an example of metadata in the a) "Basic", b) "Extended" and c) "Virtual Identity" entries. 1

Figure 5-1: Examples of MODs based on user profile and context. 42

Figure 5-2: GUI based SCE example. 43

Figure 5-3: Interaction with other environments. 44

Figure 5-4: MUP-based scenario. 47

Figure 5-5: PN Service Provider domain. 47

Figure 5-6: Interaction between PN Service Provider domains. 48

Figure 5-7: Overlay PN domain. 1

Figure 5-8: PN interactions with the IMS Group/Document Management Enabler. 50

Figure 5-9: IMS databases. 51

Figure 5-10: Trends for personalisation and blended services. 51

Figure 5-11: Overview of traditional networks [Ballot 2008]. 52

Figure 5-12: Subscriber data management across different networks [Ballot 2008]. 53