WIRELESS WORLD
RESEARCH FORUM

OUTLOOK

Visions and research directions for the Wireless World

Mai 2009, No 3

User Profiles, Personalization and Privacy

WIRELESS WORLD RESEARCH FORUM

User Profiles, Personalization and Privacy

WWRF Outlook

Jointly prepared by WG1, WG2 and WG7

Editors:

Henning Olesen[1], Josef Noll[2], Mario Hoffmann[3]

Contributors:

Allan Hammershøj[1], Antonio Sapuppo[1], Zahid Iqbal[2], Najeeb Elahi[2], Mohammad M. R. Chowdhury[2], Seppo Heikkinen[4], Michael Sutterer[5], Gerrit Hornung[5], Christoph Schnabel[5], Olaf Drögehorn[5], Henrik Thuvesson[6], Christoph Sorge[7]

[1] CMI, Copenhagen Institute of Technology (AAU), Ballerup, Denmark

[2] University Graduate Center, UniK, Kjeller, Norway

[3] Fraunhofer-Institute SIT, Garching, Germany

[4] Tampere University of Technology, Finland

[5] University of Kassel, Germany

[6] TeliaSonera, Malmö, Sweden

[7] NEC Laboratories Europe, Heidelberg, Germany

29 May 2009

Keywords: service, service adaptation, personalization, web, user, user profile, user-centric, I-centric, context, preferences, virtual identity, policies, semantic, ontology, Semantic Web Services, profile management, mobile applications, language, identity management, privacy, environment

Table of Contents

List of figures

Executive summary

User profiles and personalization have been promoted as key enablers of future ambient environments. Based on ubiquitous and pervasive computing context awareness and services specifically tailored to the users' current needs promise much higher comfort and user support in the "Internet of the Real World". The most promising application areas besides cyberspace are currently mobility, healthcare, intelligent buildings, and automotive. The major technical challenges are distributed identity management, managing complexity, as well as seamless and semantic interoperability. At the same time "user profiling" has been identified as one of the three major concerns besides "loss of control" and "increasing probability of surveillance" in such intelligent and smart environments. So, security requirements, privacy concerns and data protection frameworks have to be analysed and taken into account seriously whenever designing such environments in the future.

This WWRF Outlook, jointly compiled by the working groups WG1, WG2, and WG7, describes and discusses the different aspects of the applicability, the structure and the lifecycle of user profiles in future service environments as well as the difficulties with realising privacy-preserving personalization. The work is mainly based on the analysis of the results of several EU projects from FP6 and FP7 as well as the monitoring of relevant standardization bodies referenced throughout the Outlook.

Current and future research as we see it has no more, no less to answer the questions: (1) to what extent users have to disclose personal information in order to enjoy personalized and context-aware services in a user-controlled, privacy-preserving and trusted way, as well as (2) to find a reasonable balance between user-centric requirements and natural business interests of service providers and authorities, who offer and regulate such services.

Chapter Overview

The Outlook starts with recent work based on WWRF's reference scenarios. As an example, Chapter 2 describes several aspects of service delivery supported by a user profile. The example scenario analysed is called "coming home scenario" and identifies useful examples of functionalities possibly based on user profiles, such as "finding by chance a friend travelling on the same train" or "initializing the personal preference profile when approaching home".

The applicability of user profiles is the main topic of Chapter 3. Concepts used to define role-based and virtual identities are discussed and analysed as well as how these identities can be used for service prioritization and service selection. The most important fact is that a so-called virtual identity, which covers only a well-defined part of the user's real identity, is a way for the user to be presented in future ambient environments from a security point of view. This is called the I-centric (or user-centric) perspective, which focuses on user empowerment and control. In addition, user profile ontologies – on a higher abstraction level – are discussed in order to address the interoperability challenge.

Chapter 4 then puts the user explicitly in the centre of the service provisioning process and illustrates in detail how both profile management as well as profile adaptation can be supported. Three aspects are pointed out: The first important aspect is the introduction of specific semantic technologies in order to achieve reasonable representations of user profiles and to enable a learning process. A second important cornerstone is the establishment of policy enforcement mechanisms that handle all requests and interactions with the user profile taking into account security and privacy requirements. Thirdly, a dedicated "Service Logic" takes care of acquisition and management of profile and context information, as well as the negotiation with 3rd party service providers and the adaptation of content and services.

Based on the service provisioning process the difference between passive and active personalization and the implications of user-empowerment are discussed in Chapter 5. Referencing the results of several European research projects and activities in standardization bodies monitored during the last years, e.g. ETSI, 3GPP, Liberty Alliance, the recent Kantara Initiative, and W3C, this chapter introduces the conceptual structure and components of user profiles. Here, user profiles are composed of basic profiles (with predominately static personal information), extended profiles (with more dynamic individual information such as context-specific preferences, service histories, and security & privacy policies) and other subcomponents. Major input refers to the project MAGNET Beyond.

Towards a unified profile management framework the Outlook then discusses the distribution and interoperability of federated user profiles and mechanisms of user representations, if the user is actually offline. A so-called "Digital Butler" is proposed who acts as a personalization and identity provider on the user's behalf.

Technologies and mechanisms for how user profiles can be continuously updated and enhanced is the focus of Chapter 6. Most promising approaches are (1) assisted learning and observation of user behaviour facilitated for example by a "Digital Butler", (2) peer- or community-assisted development of user profiles, and (3) recommender systems based for example on user groups.

Personalized information has become a very valuable trading good for a specialized identity industry and is at the same time already subject to attacks such as identity theft and surveillance. Therefore, Chapters 7 and 8 cover aspects of privacy-preserving personalization and legal frameworks, respectively. We think that especially user-centric approaches in identity management have to be strengthened against more service- and network-centric approaches in order to balance security requirements of the latter ones with privacy concerns of the former ones. Consequently, WWRF suggests that the user owns his personal data including his profile and context data and has full control over the lifecycle of his virtual identities.

Finally the Outlook recommends in Chapter 9 a roadmap of future research trends clustered in user, business, and technology-driven aspects. User aspects from our point of view will continue to address privacy preserving and enhancing research areas. Theory says: The more dynamic context can be analysed and aggregated the more personalized and accurate services can be tailored to users' needs. Important to us is the secured and privacy preserving analysis and exchange of groups' and users' profile and context data. In more business-driven areas a lot of questions around 'who owns and hosts profiles in a trusted manner' are still unsolved and – after the most recent data scandals – became even harder to answer. On the part of technology we expect an increasing trend to semantic technologies, e.g. aging ontologies, reasoning and rule execution engines, as well as security implications in terms of access control to different parts of user profiles combined with dedicated policy enforcement. Also context awareness, identity management and learning algorithms will be important cornerstones in future research activities.

1 Introduction

Machine-understandable descriptions of user context, devices, preferences and service capabilities are the key for an automated service adaptation. Semantic technologies support the machine readability of content and became part of the service-oriented architecture.

This WWRF Outlook focuses on the challenges of describing user preferences, memberships in groups, device settings profiles in a user profile along with context-related information. Also related security, privacy and legal aspects are analysed.

Historically a service-centric architecture was introduced to let services communicate with each other. WWRF's user- or I-centric approach is based on the transition from access delivery to service delivery [Kellerer2002]. Current rule-based algorithms become too complex when handling user context and preferences, thus asking for new mechanisms that can allow dynamic adaptability of services.

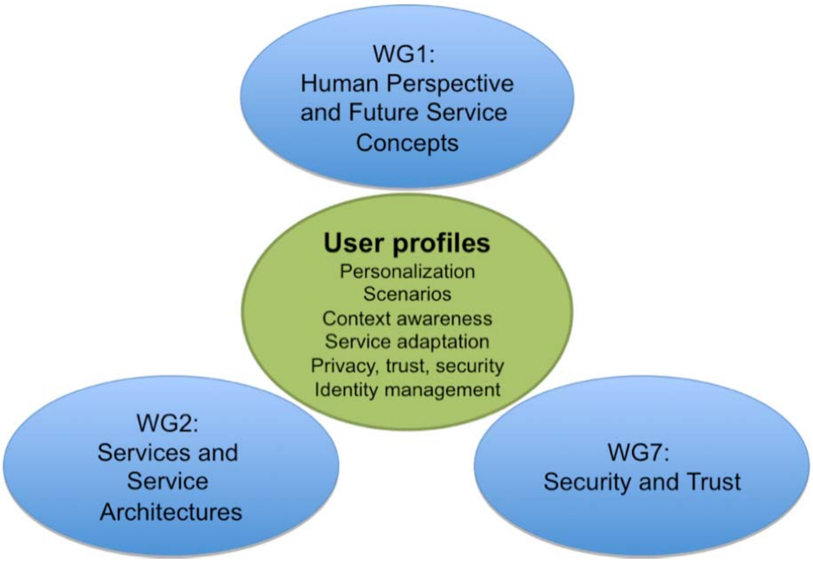


Figure 1: WWRF Working Groups contributing to this Outlook.

Putting the user into the centre of service delivery means adapting services towards the user's profile and context. The challenges of such a user-centric approach are beyond a pure service architecture discussion and address human perspectives, including security and trust. WWRF thus invited the relative working groups WG1, WG2 and WG7 to focus on these interdisciplinary aspects. Figure 1 indicates how this Outlook on user profiles, personalization and privacy relates to other areas such as context awareness, service adaptation, trust and security, which are covered in the WWRF working groups.

Historically, the service-centric world was based on interaction between services. With ambient intelligence, ubiquitous computing and the inclusion of devices and sensors into the "Internet of the Real World" [Zimmermann 2008], the two worlds of service delivery and mobile computing come together. WWRF addressed these topics in the WWRF #21 meeting "Sustainability and the Future Internet", where Håkan Eriksson, the CTO of Ericsson, estimated 6.5 billion mobile subscribers by 2013, with each user interfacing to 30-50 digital devices at any time.

Dozens of EU and national projects such as ePerSpace, MobiLife, SPICE, E2R II, MAGNET Beyond, SIMPLICITY, WellCom, DAIDALOS, SWIFT, PRIME, and PrimeLife have dealt with the topic of personalization. This Outlook collects views of WWRF-related projects and provides a common view for aspects related to user profiles. Standardization of the user profile is also the objective of the ETSI Special Task Force STF342[1], with which the authors have had an ongoing information exchange.

1.1 The mobile service environment

The starting point for this Outlook is Semantic Service Provisioning, as indicated in the WWRF Book of Visions [BoV 2008, Chap. 4]. Semantic technologies are expected to provide solutions for handling the complexity of personalized service provisioning to the mobile user. To represent a dynamic service environment we need to take into account the user and her preferences, the context of the user, as well as the capabilities of the services and communication devices.

1.2 Approach

Based on the current developments in semantic service delivery, this Outlook proposes a semantic user profile description as a potential way to establish a dynamic service offer to the end-user, adjusted to the needs and the context of the user (see Figure 2).

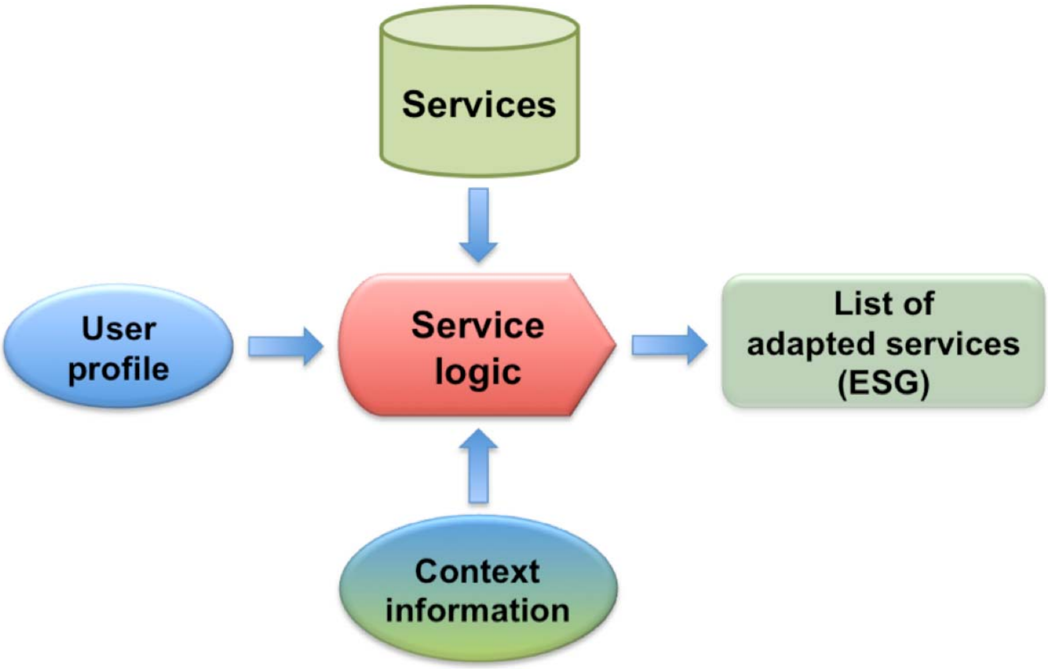


Figure 2: Service adaptation based on user profiles and context information.

User profiles and context information represent different types of information, which can be utilized to perform service adaptation. Useful definitions are the following:

- **User Profiles**: 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 2005]
- **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]

[1] ETSI STF 342, http://portal.etsi.org/stfs/STF_HomePages/STF342/STF342.asp, last accessed 02-05-2009.

A user represented through his or her user profile will experience a service offering at any time and in every situation. Adapting this service offer to the context information and the preferences of the user is the key challenge of the I-Centric service logic, where privacy of user information is taken into consideration. Service adaptation thus means identifying the relevant parts of a user profile and the context information that can be applied for service adaptation. The actual adaptation is then performed by the service logic module, providing the user with a list of adapted services, e.g. in the form of an electronic service guide (ESG). This is well in line with current trends in standardization, e.g. OMA BCAST [OMA BCAST]. Protecting the user's privacy will always be a trade-off between the optimum service offer, knowing each and every detail of the user, and a service offer which is "good-enough", ensuring the privacy of the user data. We suggest policies and their enforcement for ensuring a "good-enough" service offer.

2 Service scenarios

During the past couple of years WWRF has developed a number of **reference scenarios** [WWRF scenarios], which can support the long-term vision of WWRF, more specifically trying to envision, what daily life could be like in the year 2020, when wireless technologies have come a lot further.

In this Chapter we will concentrate on just one scenario describing several aspects of service delivery supported by a user profile. The scenario is called the "coming home scenario", and the full scenario can be found in [WWRF scenarios]. In the following we will quote selected parts of this story and comment on them in order to highlight, where user profiles are a prerequisite or may come into play.

2.1 Social networking

> *"Sabine runs onto the train in Karlsruhe and as soon as she enters, the door closes! That was close! She packs the dripping umbrella, and takes out her mobile personal device, which has automatically detected that she has entered the train*[2] *and therefore asks whether she would like to find a free seat – and what the criteria for this seat should be. Normally, Sabine would ask for a seat next to a friend – if any friends were travelling on the train and if such a seat were available."*

This option has been set as the default option in her profile. So each time she gets into the train, the train service receives her preferences and checks upon the existing list of Sabine's friends.

> *"Then she would automatically make a reservation for such a seat and this would be indicated at the seat so others were unable to take it."*

In case she wants to finish some work before getting to the job, she can modify her preferences for this particular travel: find a seat alone in the working section of the train. She will interact with her mobile device and chooses the new preference. The train service will receive the request of Sabine and will reserve a seat in the working section of the train.

2.2 Privacy policy

> *"However today, Sabine chooses to find a seat alone in the working section of the*

[2] Context awareness

> *train. There are still some things she needs to finish from work before she can call it a day."*

The train service will detect that Sabine is working, whether she will receive a call the service will filter only important calls that she has defined previously. She has defined to receive calls only concerning something really important from one of her family members. In fact, if the other people that are not member of her family will try to call her, they will be told that she is not reachable at the moment.

> *"Carl, Sabine's husband, is on the phone; He will be late and will, therefore not be able to pick up their two daughters Anna (8 years old) and Lea (4 years old) – he is currently in Würzburg on business and knows that Sabine will be too late to pick-up the girls since she has another engagement on her way home from the train. Quickly, Sabine decides to order a pick-up service from the school (a trusted person from the school who will pick up the children and take them home). The service is expensive but in this situation it is necessary and it can all be taken care of electronically with short notice. Her "order" is accepted after she has been authorized as the mother of the two girls, and Sabine can now send (voice) messages to Anna and Lea about the pick-up. At the same time she checks on Lukas, their 15-year-old son – is he home from school or?"*

Lukas does not want all people looking for him to know what he is doing at the moment. Thus, only members of his family will receive the message that he is playing an interactive game at home. All the other people will be told that Lukas could not be reached.

> *"Sabine receives a text message from Lukas' mobile that he does not wish to be disturbed unless it is very important since he is playing an interactive game at home.*
>
> *She is fine with this message and immediately gets back to her work in order to finish before her train stop in Heidelberg."*

2.3 Reservation service

> *"Sabine gets to the centre of Heidelberg relatively easily in spite of the beginning rush hour. One km before the address where the she is to pick up the costumes, the car system comes up with suggestions for where she can park."*

Specifically, Sabine has been inserted the destination address, so the service makes a reservation for the closest place to the destination address. In case she has not inserted the destination address, the system will discover that she is in a parking zone and request to Sabine if she would like to reserve a place. In case of an affirmative answer, the car system checks whether there are some free spaces for Sabine and suggest several parking places.

> *"She is lucky: Just as she enters the street where the shop is located, another car pulls out from a parking space near the shop. Sabine immediately accepts the invitation to reserve the space."*

The service will assign her a special code matching available parking place.

> *"If another car was approaching this place, …"*

The system will check if the special code assigned to the car and the available place will match.

> *"Perhaps it just parks there without a reservation – a loud alarm would go off and the parking personnel would approach the car to resolve the situation."*

> *"Leaving the car – this time with her umbrella – she really appreciates this service that spares her from endless trips to the centre of the city looking for a parking space."*

2.4 Conflict scenario

> *"Just before she arrives home (500 m), the car communication system asks Sabine about her personal preferences for entering the house. She selects her personal preference profile in terms of housing temperature, lighting and music. Today, she wants to listen to a band that one of her colleagues plays in. She received the music on her smart phone earlier and now transfers the music to her personal information base so that she can listen to it when she gets in. She gives the instructions for this using both the eye-tracking device and her voice – depending on the traffic and the task she is to carry out."*

When the system receives the preferences from Sabine, it will discover a conflict between her preferences and the one of Lukas. In fact, Lukas is still playing in the game room and her personal preferences contradict with Lukas preferences for this room.

Then the house service will ask Sabine whether she would like to keep her preferences or cancel them.

> *"She quickly rethinks her preferences and allows for Lukas' set-up of the games room to remain valid."*

2.5 Alert service

> *"Sabine sits down again on the sofa and closes her eyes – it has been a long day. Suddenly she is warned by a loud message from her personal mobile device. The message is that her daughters are almost at home and that she can expect them to be there in a few minutes. It is by own choice that Sabine is being alerted in this way in spite of her resting. The arrival of her children has been set to as important by Sabine herself.*
>
> *Sabine opens the door and immediately hears Lea shouting and yelling and showing something she has made at school. When Anna and Lea enter the house, …"*

The house service stops the music and

> *"she can now listen to all the things her daughters want to tell her about their day. Sabine closes the door – the girls are already on their way to the kitchen to get something to eat and drink while shouting and talking about their day. Sabine follows and smiles – dinner, school meeting and more work – all that will have to wait till she has spent some time with her children."*

2.6 Common user profile and context requirements

The short pieces from the WWRF reference scenario above highlight that:

- users need profile sharing to enhance social networking (user-to-user profile interworking);
- users need to control communication services (privacy policy);
- users need profile sharing to enhance value-added services (user to third party profile interworking);

- users need to solve conflicts between different users´ preferences or policies (conflict resolution);
- users need context sharing to enhance communication services (user-to-user context sharing); and
- in all the scenarios the user's context information serves as important triggers to select which user sub-profile should be active, such as a travelling or a home profile that matches the same context (user's context information is needed to trig and enhance user profiles and related services).

The WWRF reference scenarios reveal a lot of daily-life situations, where user profiles together with context information can support personalization and facilitate tasks for the users. Equally important, the access to profile and context information is a prerequisite for other stakeholders (in particular service providers) to accomplish their business objectives and realize the scenarios. How to realize them – or whether they can be realized – is another issue. Nevertheless, the scenarios in this Outlook provide useful inspiration for the description of user profiles and profile management.

3 Applicability of user profiles

Ubiquitous access and pervasive computing enable the service access in every situation. However, limited capabilities of devices and access networks and poor usability in identity management make the ubiquitous service access quite challenging. In a world of information overflow, users or systems need to filter information to satisfy these challenges and user demands. It is absolutely necessary to select the right services among the plethora of services, and the user preferences serve as inputs to prioritize services for such a selection.

While a user in the physical world will always be represented through various aspects, e.g. his voice, face, dress-code, environment in addition to the identifiers such as driver's license or passport, a user in the digital world typically gains access just through one identifier. He may need to use his username and password for gaining access, or provide his credit card information for payment. However, digital systems carry the capability to store and relate information. Thus histories of user behaviour, purchases and other information usually follow the single identifier.

The challenge, as indicated in Chapter 1, is to provide a "good-enough" service to the user without compromising his privacy. This may be achieved through roles or virtual identities representing the user. Since identities in virtual communities were discussed by sociologists, see [Donath1999], an ongoing discussion on how to differentiate between a role and a virtual identity has taken place. This Outlook uses both synonyms, taking into consideration the different schools of the contributors.

The following sections will provide an introduction to concepts used for roles and virtual identities, and addresses how these identities can be used for service prioritization and service selection. The follow-on chapters will then provide details of the service logic for providing the service offer, as well as elements of the user profile.

3.1 Virtual or role-based identities

Depending on the situation and the current task, the user may desire to appear anonymous, partly anonymous ("pseudonymous") or with his/her real identity revealed. Naturally, services involving payment or authentication may impose mandatory personal information to be revealed. If the user is not willing to meet such requirements the service will not be available to the user. But many other tasks or services will have less strict requirements, thereby allowing the user to act with a virtual identity.

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. It was defined and described in the project DAIDALOS and continued in SWIFT, and it was adopted and further developed in MAGNET Beyond [DAIDALOS], [MBD4.3.2], [MBD4.3.3].

Basically, the VID consists of

- an identifier that the user selects (a sort of nickname)
- references to relevant parts of the user profile, and
- a set of policies, which determine what information or services may be disclosed during the usage of a VID.

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.

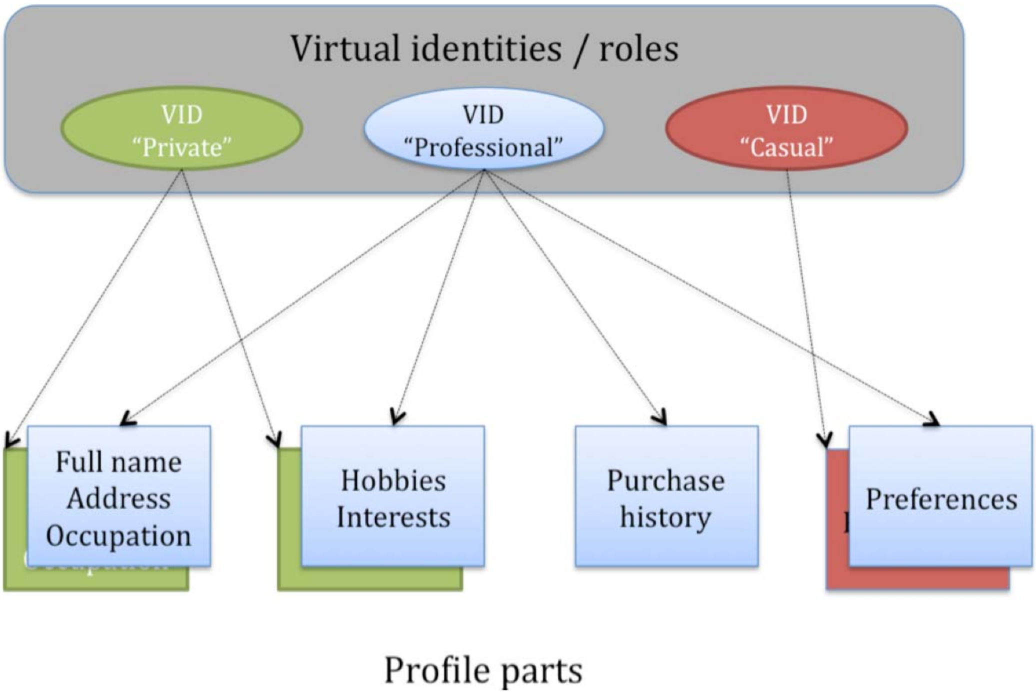


Figure 3: Examples of virtual identities based on different parts of the user profile [MBD1.2.3].

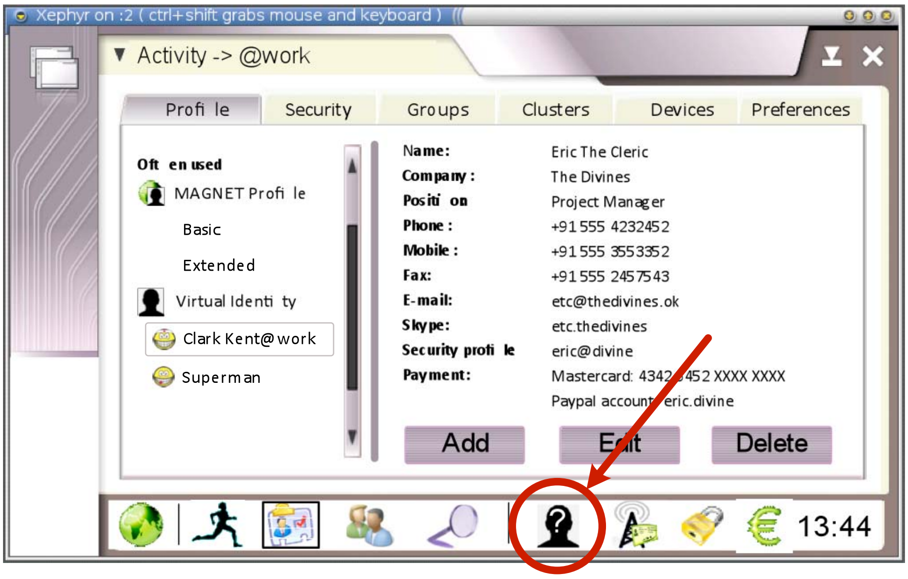
However, it is possible for a user to have multiple instantiations of each profile part (see Figure 3), and fill it with different values if wanted. In this example, the VID is divided into three main categories (depending on the use of the VID), which cannot be linked (unlinkable). These categories are:

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

As shown in Figure 3 they consist of different subsets 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. More details and security aspects of VIDs can be found in [MBD4.3.3]. VIDs can further be combined with the concept of **activities** [MBD1.4.1]. Activities represent all kinds of short- or long-lasting tasks or projects that a user is engaged in, involving devices, communities, foreign services, the user's own files, shared files etc. An example of an activity could be a user visiting a conference, where the 'activity' includes all that relates to the conference: travel planning, tickets, hotel, program, collaboration with participants, presentations, devices, services etc. An activity gathers devices, communities, services and files under one heading; making it easy to access the devices, services and files that are associated with a certain activity. Activities are the user's representation of what is on her/his mind in terms of activities, social relationships and devices and their settings.

The process of defining activities and representing them in an intuitive way to the user (e.g. as customized user interfaces) can be seen as part of the service logic in Figure 2. Activities may also be triggered by context information. The activity concept is related to the "situation-dependent profiles" proposed by ETSI [ETSI 2009a].

In order for the concept to be really useful we need to consider how the user can be assisted in this process, possibly building on simple templates, as most users will not have the knowledge, skills or awareness to define and manage VIDs.



Name:	Eric The Cleric
Company:	The Divines
Position	Project Manager
Phone:	+91 555 4232452
Mobile:	+91 555 3553352
Fax:	+91 555 2457543
E-mail:	etc@thedivines.ok
Skype:	etc.thedivines
Security profile	eric@divine
Payment:	Mastercard: 4342 452 XXXX XXXX Paypal account eric.divine

Figure 4: Conceptual MAGNET GUI design where the red circle marks the VID icon of the user [MBD1.2.3].

The VID of a user literally has many faces and as an example of how a VID can be presented to the user, a GUI design from MAGNET Beyond is shown in Figure 4. The red circle and arrow indicates the actual VID of the user corresponding to the activity the user is currently engaged 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 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 other VIDs. The silhouette could be an example of one of these cases. The fact that VIDs cannot be linked is essential for providing (partial) anonymity and safeguarding user privacy.

Every VID has its own picture to indicate the one that is currently selected and to distinguish between the different ones in a visual way. The user can freely shift between VIDs 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.

This example serves to illustrate that VIDs and activities can be used to adapt user interfaces in a dynamic fashion. More generally, we are looking for ways to filter, adapt and optimize services for the users based on user profiles and context. This will be further discussed in Chap. 4.

3.2 Identity-based service selection

Every human being plays many roles that associate with a certain VID, also at the same time, while accessing services. As a researcher or engineer, we are working in an organization; as a student, we are attending an education institute; as a consumer, we are buying things with cash or credits; we are maintaining social relationships with family, friends, relatives, neighbours and colleagues. The VID associated with a role plays an important parameter in service interaction. Each VID has preferences that will imply services parameters and define, either which services to select, or how to use services. For example, a business person travelling might have the preference to select a specific communication channel and device. Whereas the same person while at home in a social life needs different means for communication. Therefore, the professional and social VIDs associated with the corresponding role of a person are responsible for selecting the distinct type for communications services.

Users in multiple device scenarios also need a flexibility to use the same VID and preferences on all devices such as mobile phone, laptop and PC or to use different VID on different devices at the same time such as work, travelling and work roles. Users might also need different VID on the same device such as chat as private and professional in parallel sessions at the same time. Multiple device scenarios imply a higher level of complexity to support synchronized or parallel service tailoring and to avoid conflicts etc.

3.3 User profile ontologies

A personalized service delivery framework usually contains a software module that selects the services tailored to the user preferences defined in the user profile. One way to formalize the application-specific user profile and preferences is to use ontologies. User profiles (and context information) can be described in ontologies, which can form the basis for reasoning and service adaptation in the Service Logic module.

One of the most comprehensive user profile ontologies has been developed in the European IST-FP6 project SPICE[3]. The user profile ontology[4] is based on Ontology Web Language (OWL) and is a sub-ontology of the Mobile Ontology, which is a higher-level comprehensive ontology for the mobile communication domain. The user profile ontology describes the basic concepts and properties for a user and user group profile structure. User and user group profiles can consist of several service-specific and situation-specific profile subsets. The ontology enables the use of well-known existing user profile vocabularies such as vCard and FOAF (from “friend of a friend”).

[3] http://ontology.ist-spice.org/

[4] http://ontology.ist-spice.org/mobile-ontology/0/10/profile/0/profile.owl

The following example shows the basic concepts of the user profile developed in Ontology Web Language (OWL):

```
<owl:Class rdf:ID=”Profile”>
      <rdfs:subClassOf rdf:resource=”http://ontology.ist-
      spice.org/mobile-ontology/0/10/core/0/core.owl#VirtualEntity”/>
</owl:Class>
<owl:Class rdf:ID=”UserGroupProfile”>
      <rdfs:subClassOf rdf:resource=”#Profile”/>
</owl:Class>
<owl:Class rdf:ID=”Service”>
</owl:Class>
<owl:Class rdf:about=”http://nwalsh.com/rdf/vCard#VCard”>
      <rdfs:subClassOf>
            <owl:Class rdf:ID=”PersonModel”/>
      </rdfs:subClassOf>
</owl:Class>
```

To exemplify, let us consider a user Alice, who has a VID Alice (name is used as VID for the sake of simplicity) and has some preferences such as music, Formula One game, etc. This can be represented as:

```
<Users rdf:ID=”Alice”>
      <hasPreference rdf:resource=”#FormulaOne”/>
      <hasPreference rdf:resource=”#HardRockSong”/>
      <hasPreference rdf:resource=”#PlayOnlineGame”/>
      <hasPreference rdf:resource=”#PlayVideoGame”/>
</Users>
```

Such formal representations can be fed to a reasoner to derive selected services for a user based on preferences associated with the VID of the user. A reasoner is a piece of software, which is able to infer logical consequences from a set of asserted facts. Therefore, preferences of a user play a vital role in service selection.

3.4 Service prioritization

Nowadays high-speed Internet connections are increasingly available to users. Networks also become the conduit for interactive gaming, IPTV, video on demand (VoD), multimedia collaboration, music and data download, secure network storage, and a long list of services. Users are now in need of controlling the traffic to meet their increasingly busy daily life. They have developed sophisticated expectations for high quality services that include many more service options, faster service activation, the flexibility to modify their services, and competitive pricing. Empowered users demand mobility of data, services and personalization. Service providers also need to adapt to this new situation. Growing competitive challenges and changing consumer demands requires a swift and definitive response from them. The traditional competition boundaries among the cable, wireline and wireless network operators are disappearing as many of these operators begin offering triple-play service bundles and tiered service options.

Service prioritization is a tool to personalize service flow towards the users. The result may appear e.g. as the list of adapted services (ESG) described in Chapter 1, and such personalization is a strong requirement now, as users now have less time to select right services from wide range of services. Moreover, many sophisticated services can trigger sensing of the context of users. This can make the right services available at the right time. Service prioritization can also give resources priority to certain traffic types. It is a good means to avoid purchasing additional communication bandwidth while properly managing the current available resources.

3.5 Business considerations

The traditional focus of service providers is to collect as much input as possible from the user in order to provide adapted and personalized services and address their own business needs. Examples of such service provisioning are Amazon, Google and Facebook. Google is doing extensive profiling of its users in order to make its advertisement-based business model successful. Many people are concerned about what Google does and feel out-of-control on which data exist about them, and even that privacy is de-facto not existing. Recent developments, such as the Google Latitude providing context information of users, raised concern that the application could be abused by suspicious partners and paedophiles[5]. Even so, Google still has to comply with public law and regulations, e.g. European Privacy law[6].

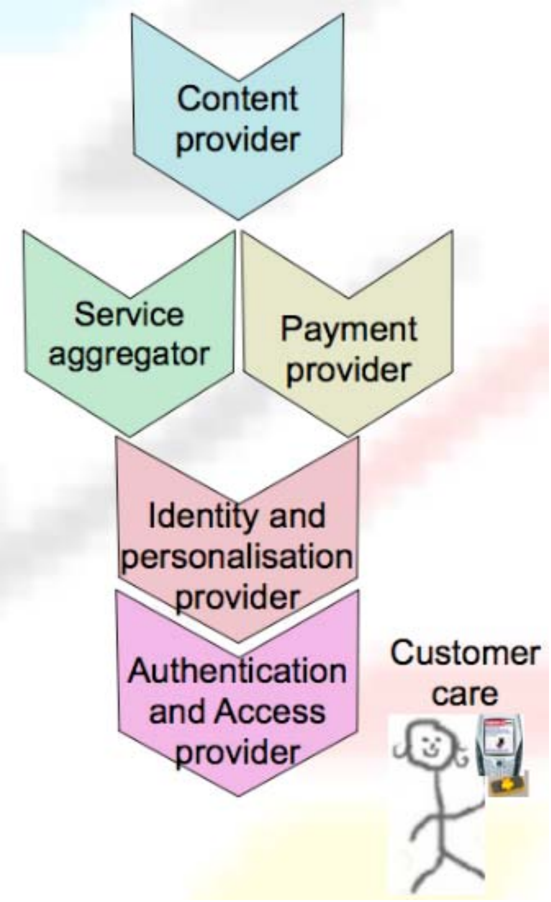

Content provider
Service aggregator
Payment provider
Identity and personalisation provider
Authentication and Access provider
Customer care

Figure 5: Components of future service provisioning.

[5] http://www.brandrepublic.com/News/878765/Googles-mobile-phone-tracking-service-fire-privacy-critics/

[6] See e.g. http://www.google.com/privacy.html and http://www.google.com/privacy_faq.html#serverlogs.

In a digital environment with connectivity of multiple devices and sensors at each moment the handling of roles and identities, user information and related context has to be considered in a new way. Discussions are ongoing about

1. Who provides an identity?
2. Where is identity information stored?
3. Where are user profile and context information stored?
4. Who has access to this information?

While a traditional service provisioning was about packaging content and providing this content to the user, the business model of the future is more complex. Figure 5 displays conventional business entities such as content provider, service aggregator, and payment provider, but also new entities such as an authentication and access provider and an identity and personalization provider, with the latter having the focus on providing trust, privacy and personalization [MBD4.3.2], [Noll 2007]. Such an open business model requires application interfaces between the different partners in a service provisioning process.

WWRF has postulated the I-centric approach, where the user is in control of his preferences, context and related information. This postulation is reflected in the service provisioning logic, which is explained in the following Chapter.

4 I-Centric profile management and service adaptation

Analyses of the communication behaviour and communication space of users show that human beings interact habitually with their environment. Following this vision, a new "User-Centric" or "I-centric" approach emerges by putting the user in the centre of service provision. This implies that each individual will receive service offerings according to his or her preferences and the current situation, environment and resources. Figure 6 depicts the main components of user-centric profile management and service adaptation. Each component will be described in the following sections repeating the symbols from the Figure.

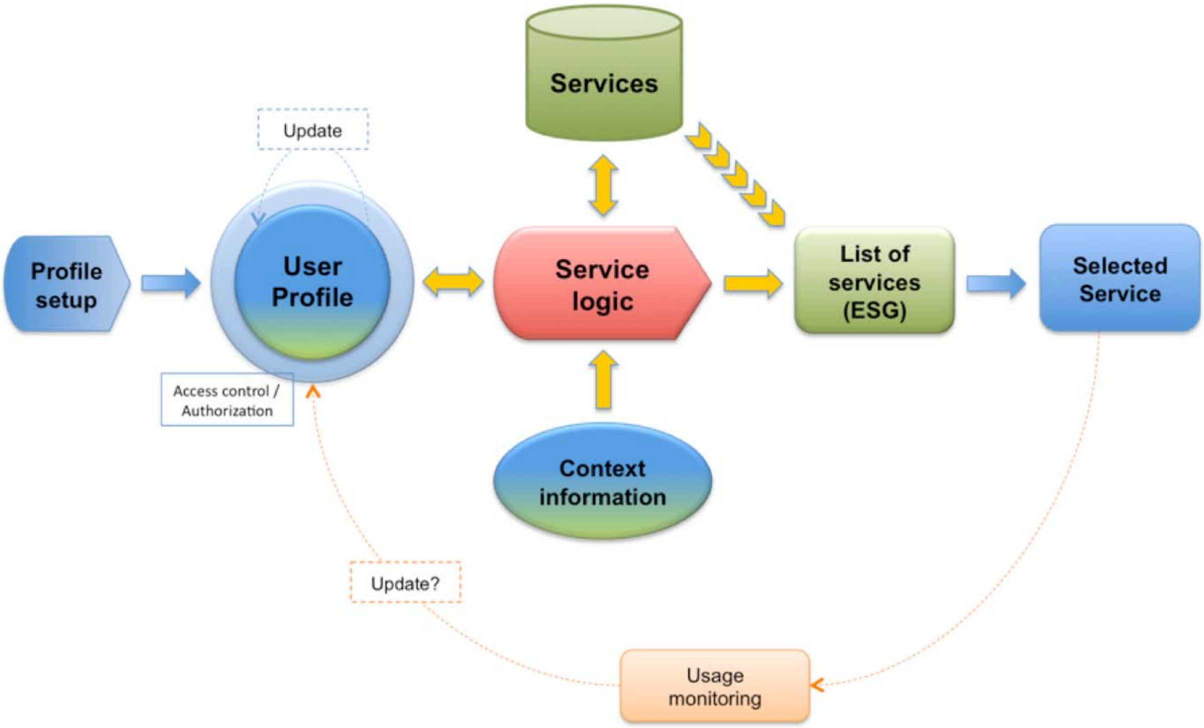


Figure 6: User-centric user profile creation and usage.

The significance of the colours in Figure 6 is that "blue" indicates the parts, which are influenced or controlled by the user, and "green" are the parts controlled by others. The processing module called "Service Logic" and the "Usage monitoring" feedback loop are drawn in red and orange, respectively. Note that some of the arrows are bidirectional, while others are unidirectional.

The user profile is established, maintained and continuously developed through the *profile setup* and *usage monitoring* components, which enable the learning process. Semantic technologies are used to achieve the representations of the user profile. A detailed description of the profile structure and its components is presented in Chapter 5 and approaches for enhancing the user profile are discussed in Chapter 6. The shell surrounding the user profile indicates the protection of the sensitive personal data by policy enforcement, which handles all requests and interactions with the user profile from e.g. service providers and other entities.

Context information is constantly acquired and stored/processed in the "Service logic" module. If a service provider wishes to initiate a service delivery to a user, he will contact the "Service logic" module in order to request specific information from the user profile and possibly store certain 3rd party service provider information in the user profile (see Sect. 5.2.4), the green part of the user profile in Figure 6. Certain context information may also be required by the service provider, but similar to profile information this could as well be sensitive information, which the user does not wish to disclose (e.g. location).

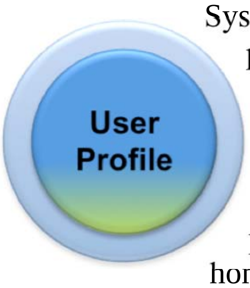
The service logic and the policies set by the user determine whether the requested information can be provided or not. If granted, this will enable the service provider to perform some amount of service adaptation and tailor the service offers to the user and the context. The result is then presented to the user, e.g. as a list of services, and the user can make a selection of the service. If not granted, a conflict may occur between the service provider policy and the user's release policy, in the worst case meaning that the service cannot be delivered.

From the user's point of view this represents the first step of personalization, which already adds value for the user. Making use of the entire user profile, the user may choose to perform further personalization to optimize the user experience, e.g. by customizing device settings. This can be done without involving the service provider or be hidden for the service provider, but will add further value for the user.

4.1 Profile setup

Nowadays, social networks are one of the most widely used platforms of online communities. According to a report from ComScore [ComScore2007], social network sites like MySpace, Facebook, LinkedIn etc. had about 65 million daily visitors in June 2007, and the growth rate was between 50% and 300% per year. People joining several sites declare their friends and publish their contents on every site they register. The profile setup not only facilitates the primary profile setup but also allow an improved setup based on retrieval of information from the user's social networks. Hence, the profile setup includes a mechanism to get membership IDs of online communities based on community tags (meaning who you are in LinkedIn or Facebook) and make use of that information when setting up the user profile. The user profile may contain pointers to or combine several pieces of user information distributed at several online sites (communities, subscribed services, etc.) and organize them in a suitable template. This is further discussed in Sect. 5.5.2.

4.2 User profile



Systems in a pervasive computing environment often need to access the profiles of a user in order to provide services and information that are tailored to the user. A typical user profile may contain the user’s personal details (name, birth date, gender, contact details, etc.) and several types of user preferences. The user might also have different sub-profiles based on different roles on different devices, such as a profile for my job device, my private device, my car device, and my home device etc., as described in Chapter 3.

The reason for separating profile set-up and user profile is to allow applications and services to automatically suggest updates to the profile including default settings to ease the handling of a complex profile.

The following example illustrates how this update process could work:

- You select a new topic, and then a process starts, which will enhance and update your profile. Example: “fishing” is added to interest areas. Then an applet on your mobile phone may start informing you about user groups on the Internet, clubs in your vicinity, or virtual clubs on the Internet. Next step might be further detailing of the interest, e.g. if you have joined any club or want to join a club, for more specific interests “sea water fishing” versus “fly fishing”.

The final goal would be to update the profile according to these specifications.

4.3 Context information

The context information represents the user’s physical and environmental surroundings and is collected from multiple context sources (by “context watchers”). Context information may include the user’s location, time, current activities, available devices and networks, device capabilities etc. High-level context information (like what is the user doing?) is usually deduced from the environmental context.

Delivering information and services to personnel at work premises based on their context has tremendous potential to improve working practices, particularly with respect to productivity and safety. In case of service delivery to mobile devices, context awareness is crucial because of limited bandwidth resources and higher cost of resources.

4.4 Service logic

The Service Logic component brings together user preferences from the user profile, context information from context watchers, and service offers from the service providers. Based on these inputs a matching algorithm will provide the best match, resulting in a personalized list of services.

A simple matching can be provided in terms of “hard-coded” conditions such as “when delivering a certain service to me, please provide it in a certain format and quality”, “if I have access to both a 3G network and a free WLAN hotspot, please deliver the service over the WLAN”.

The following examples describe two real-life scenarios, where the service logic makes use of context information to adapt services.

- Example 1:

  Sabine runs to the train to catch it. She does not want to receive any advertisements but would like to have a ring tone, if train is delayed. Here, context can be “on the way to the train station, running”, and the service can be train operating information.

- Example 2:

  Sabine walks to the train station, and there are still 45 minutes before the departure of her train. She wants some advertisement services such as relevant offers for shopping, coffee, sightseeing, short news, etc. Here, context can be “slow walking” or “on the way to the train station”, and the service can be proximity and Internet services.

More sophisticated algorithms based on e.g. artificial intelligence and semantic web technologies (ontologies, reasoning) can be applied to identify the relevant parts of the profile and context information that are most suited for performing service adaptation in any given situation. This can potentially lead to very advanced, dynamic and (semi-)automatic service adaptation and is an important area for future research.

4.5 List of services (ESG)

The “List of services (ESG)” displays all the available services, which are filtered out from the service logic. Alternatively, the common situation today, service providers may directly present a list of services to the user, as indicated by the yellow dashed arrow in Figure 6, bypassing the Service Logic module.

4.6 Service selection process

The user will select more specific services from the list of services, and these services will be captured by Selected Service component. The service selection process is controlled by the user and based on the user’s profile, needs and interests. As a result of the service logic “pre-processing” the user will always have access to a filtered, relevant and valuable list of services, thereby providing a better user experience.

4.7 Usage monitoring

These selected services are monitored by the Usage monitoring component. This component gathers monitoring data (such as service usage or service execution history, trusted 3rd party services) and presents this information to user profile, which further helps the individual to choose the best available services for a particular task. One may think of “Usage monitoring” as a huge log-file, which records the user’s actions and service usage over time. The main objective behind the monitoring component is to ensure the automatic learning of the user profile concerning the user’s interest domains, service usage and content consumption trend (cf. Chapter 6).

In principle, this would mimic how the user develops his or her personal experience over time, remembering what was good and bad, and using this record to learn from mistakes and improve future behaviour. This falls well in line with current trends of users, who tend to more and more carry along their life history with them in the form of photos, mails, calendars, music, etc. However, although this may become technically feasible, users may not always like this to happen, or they may want to be able to “switch off” this option.

Usage monitoring may consist of three actions:

a) Direct monitoring of service usage, to establish history and way of usage

b) The Service execution history stores and maintains the history of service usage so that all the parties involved have a greater degree of confidence that service usage progresses satisfactorily and, in the case of failure, makes it possible to avoid such services in future.

c) Feedback on service execution in order to establish quality parameters about service providers, e.g. history over "successful services", trusted providers, failures of delivery.

Naturally, from a service provider perspective, this is also extremely valuable information, which can help them to map out the usage of their service and tailor their marketing and service offers. The risk of violating the user's privacy is high. Also, in a society perspective, fears of a "Big Brother" watching are becoming very real, and this raises a lot of ethical and legal issues about surveillance and privacy protection. These issues are further discussed in Chaps. 7 and 8.

4.8 Access control and authorization

User profile
Access control / Authorization

The core functionality of the "Access control/Authorization" component allows the system (service logic) or other users to access the user profile with recommendations and suggestions in order to update it. This would typically result in improvements and additions of new user preferences, but all of these must of course be authorized by the user.

We envisage a federated user profile in combination with policies that manage the access to various parts of federated user profile. The details of the federated user profile are discussed in Chapter 5. For instance, the social part of the user's profile can only be accessed by his online social community friends, and the business part of user's profile can only be accessed by user's colleagues or work friends. Mechanisms must be developed, which on the one hand are simple but still meaningful and effective for the user, and on the other hand can work with different privacy settings in open user communities.

Example:

- Sabine travels to Norway for a business trip. One of her social communities friends John will see from Sabine's profile that she is in Oslo. John already visited Oslo. Being a friend John knows that Sabine likes pizza. John wants to update Sabine's profile to inform her about the best pizza restaurant in Oslo. John will send an update message to Sabine's profile. The system will evaluate the access policy for John. If he is authorized to update Sabine's profile then update is performed. The notification of the update will be sent to Sabine.

5 User profile structure and profile management

Users are familiar with profiles from web-based services such as Amazon.com, Google, news sites and social networking sites, where they are typically requested to fill out a web form to give a set of personal information, when they register, in order for the service provider to tailor the service to the user's identity and preferences.

The problem from the user's perspective is that the user is not in control of the profile information collected and stored by 3rd party service providers. Even though "well-behaved" service providers may clearly state their **terms and conditions** and **privacy policy**, they still have the ability to record usage history to extract patterns and habits, and by collecting and correlating such data from a large number of users they can apply **collaborative filtering** techniques to generate suggestions to the user. Amazon.com is a well-known example of such **recommender systems**: "Customers who bought this book also bought …".

Actually, in the field of media personalization, it is often assumed that users are not willing to or interested in actively contributing to building up their user profiles, and hence personalization is purely based on "passive personalization", i.e. on profiles generated by the provider as described above. Most users are "laymen" and do not possess the skills or awareness to constantly manage their profiles and privacy. Much of the research effort on personalization therefore aims at empowering the users to gain control over their user profile.

Most of the situations encountered by a user, where personalization is relevant, can be considered as either

- interaction with a "system" or a device, or
- interaction with other users (peer-to-peer, communities, etc.),
- interaction with an external service provider offering services to the user.

In either case the user profile (or selected parts of it) serve to optimize the interaction and make it user-friendlier. It is therefore important that the user profile is well structured and managed.

5.1 Previous work

Work on user profiles and context is still very much at the research stage, and several major research projects, e.g. under the European Union FP6 and FP7 programmes, have developed and are developing concepts and tools for personalization. Notable and important projects are MAGNET Beyond, ePerSpace[7], E2R and E2R II[8], SIMPLICITY[9], DAIDALOS[10], SWIFT[11], SPICE[12], SMS[13], PRIME[14] and PrimeLife[15].

In 2004, the ePerSpace project[16] has produced a nice overview of the key concepts, which define personalization, mapping them to available technologies, see Table I. Although some organizations have been merged and new ones should be added, the Table still serves to show the complexity of personalization and user profile management.

Today, even more international standardization bodies and industry forums are working on issues related to user profiles and personalization. These include – besides WWRF – ETSI (European Telecommunication Standards Institute), 3GPP (Third Generation Partnership Project) [3GPP GUP], Liberty Alliance [Liberty], W3C (Worldwide Web Consortium), and social networking initiatives, such as Google's OpenSocial[17]. In particular, there is a lot of

[7] Towards the era of personal services at home and everywhere.
[8] End-to-End Reconfigurability
[9] Secure, Internet-able, Mobile Platforms LeadIng CItizens Towards simplicitY.
[10] Designing Advanced network Interfaces for the Delivery and Administration of Location independent, Optimised personal Services
[11] Secure Widespread Identities for Federated Telecommunications
[12] Service Platform for B3G Innovative Communication Environment
[13] Simple Mobile Services
[14] Privacy and Identity Management for Europe
[15] Privacy and Identity Management in Europe for Life
[16] http://www.ist-eperspace.org
[17] http://code.google.com/apis/opensocial/

work on identity management, which addresses important parts of user profile and privacy issues. Some of most important initiatives are briefly discussed in Sect. 5.4. In 2008, the PrimeLife project has produced a comprehensive survey of ongoing work and initiatives in the field of identity management and privacy control, see [PrimeLife report].

		Profiles	Profile Management	Service Discovery	Service Adaptation	Context	Presence & Availability	Rules & Rule engine	Security & privacy
3GPP	GUP	X	X			X			
	LCS					X			
	Presence						X		
W3C	CC/PP	X							
ISO	MPEG-7	X	X		X				
	MPEG-21	X				X			X
Liberty All.	Federated Network Identity	X	X						
	Single Sign On								X
OMA	UAProf	X							
	Mobile Web Services			X		X	X		X
	PAM						X	X	
	W-Village					X	X		
IETF	Rich Presence					X	X		

Table I. Key organizations and important technologies for personalization (adapted from [ePerSpace]).

5.1.1 European Telecommunications Standards Institute (ETSI)

ETSI has published a comprehensive user profile guide [ETSI 2005] and suggests that details of the user and their personal requirements are included in a user profile, in such 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. The goal has been to create a well-founded guide for service and device developers to solve the common issues of user profile management in both personal and business applications.

The document provides guidelines relevant to users' need to manage their profiles for personalization of services and terminals. It defines a common content of a user profile. It also describes how to set up and maintain the user profile, e.g. creation of profiles from templates, profile updating and data storage. Interesting elements are the profile inheriting data model and the live template.

The work continues in new task forces

- Specialist Task Force STF 342, "Personalization and User Profile Management

Standardization"[18],

- Specialist Task Force STF 352: "Personalization of eHealth systems"[19], and
- Specialist Task Force STF 287: "User-oriented handling of multicultural issues in multimedia communications"[20].

STF 342 is currently working on two deliverables, an ETSI standard on standardized objects of the user profile [ETSI 2009a] and a technical specification of the architectural framework [ETSI 2009b]. The work is focused on user profile structure and management from a telecoms perspective with less focus on identity management and the open Internet, and it does not so far include the aspects of service adaptation. A liaison agreement has been set up between WWRF and ETSI STF 342, and the ETSI proposal is well in line with the work presented in this Outlook.

5.2 Conceptual structure and components

In the following we present the user profile structure, which was developed in the FP6 project MAGNET Beyond. MAGNET Beyond focused on the concept of Personal Networks (PNs), in which the user centricity implies that the user becomes an entire communication cluster made by the user himself with his personal resources (devices, personal clusters and personal federations). The user profile should therefore be able to accommodate:

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

The conceptual user profile structure from MAGNET Beyond is shown in Figure 7. Instead of defining a new user profile concept, the approach has been to extend existing architectures defined by other projects or standardization bodies and adapt them to match the PN scenarios. The proposed structure can thus be seen as an evolution of previous scientific or industrial approaches in defining user profiles towards a global profile including personalization and federation concepts. As indicated in the Figure, the various parts of the MAGNET user profile are linked with existing standardization approaches, which are presented in Section 5.3.

As described in [MBD4.3.2, Chap. 4] the user profile can be structured in a tree, and it consists of several subcomponents, which are accessed through the "User profile" subcomponent. Policies are retrieved and used, when the user browses through content, either on the Internet as web pages or in 3rd party services. Most of the user profile subcomponents are placed locally on the user's devices and synchronized with a network repository (see Sect. 5.5). Some crucial parts of the user profiles may, however, need to be protected as secure elements and stored by the user, who only makes them available when needed.

[18] http://portal.etsi.org/stfs/STF_HomePages/STF342/STF342.asp, last accessed 23-05-2009.
[19] http://portal.etsi.org/stfs/STF_HomePages/STF352/STF352.asp, last accessed 23-05-2009.
[20] http://portal.etsi.org/stfs/STF_HomePages/STF287/STF287.asp, last accessed 23-05-2009.

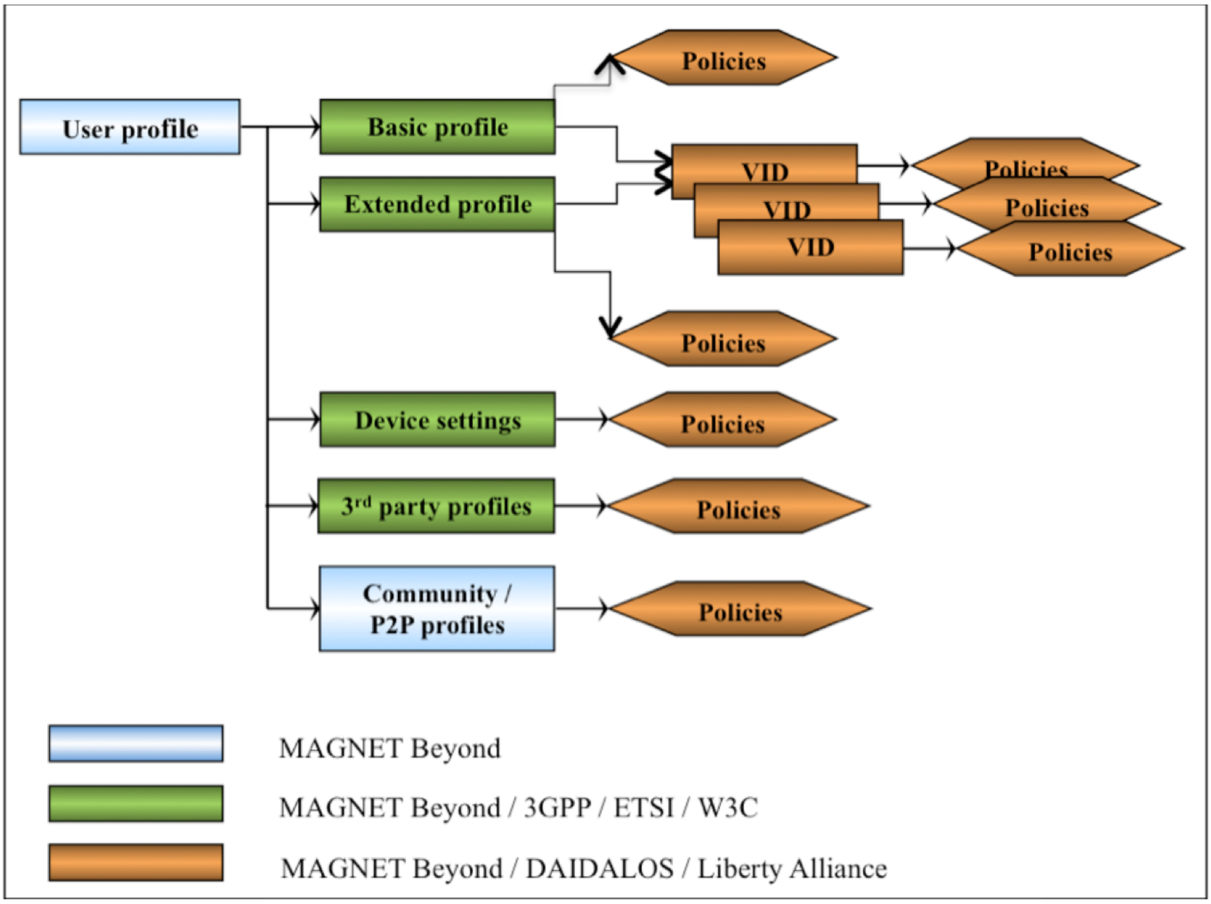


Figure 7: MAGNET user profile in a conceptual representation displaying the different categories and dependencies compared to state-of-the-art (adapted from [MBD4.3.2]).

The top level of the user profile contains the user profile ID, obtained security clearances etc. In MAGNET Beyond, having a certain identity implies a certain level of clearance in different systems with which one interacts. Because the profile contains identity information the user profile plays an important role in storing security clearances and authentication information for accessing accounts and services. *Identity management should therefore be viewed as an integral part of user profile management.*

The user profile consists of

- The basic profile
- The extended profile
- Virtual IDs
- Device settings
- 3rd party profiles
- Community or peer-to-peer (P2P) profiles
- Policies

which are explained in the following.

5.2.1 Basic profile

The basic profile component of the user profile contains the basic personal information about the user, such as name, address, gender, phone numbers, e-mail address or addresses, etc. It is a – predominantly static – set of information, which is defined, when the profile is created. The information may be considered permanent in the sense that it does not change so often, and its attributes are not affected by external factors.

5.2.2 Extended profile

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, mood and needs. The extended user profile mostly contains information that is generated over time; that is, the entries are not present upon profile creation. Thus, the extended profile is dynamic and highly generic, allowing for the introduction of new entries later on. It also contains a reference to the user history log. This is where usage patterns can be used to help adapting the user profile. The information in the extended user profile can be placed on a GUP repository [MBD1.2.1, Chap. 2], if the user has subscribed to this, see Sect. 5.4.6.

We should distinguish between preferences, which seldom change ("habits") and those, which change more often due to personal dislikes and new interests ("current interests"). The last group – current interests – contains "emotion-driven" preferences that may expire due to experiences in the user's life: You get enthusiastic e.g. about a new type of music, but after a while (weeks, months) your enthusiasm fades away, and you get annoyed, if you e.g. signed up to a newsletter or ended up in a consumer database. A simple way of handling this problem is to monitor how often the user actually interacts with files / data concerning this interest, and if inactive for a while, the preference is altered. This is e.g. implemented in the podcast subscription of iTunes.

The preferences, which are in the extended profile, can be further sub-divided into several types as described in the following [MBD1.2.1]:

Generic user preferences

The user may have several common preferences, which are not specific for any context or application/service/device. These would always need to be considered to satisfy the user. They may include:

- General interests
    - Food preferences (food restriction, vegetarian, …)
    - Movie preferences
    - Music preferences
- Service format preferences (text, audio, video, html)
    - Text preferences (e.g. large text or small text)
    - Audio preferences (e.g. very loud)
    - Video preferences (e.g. high resolution)
- Likes and dislikes
- Health-related preferences (e.g. substances that can cause allergy)
- Religion-related preferences (holidays, food restrictions)
- Price preferences (if several connections are available, the user may prefer low price, medium price or high price connection)
- Payment preferences

Application- or service-specific preferences

An experienced user might frequently be using the same applications or services and could have preferences or settings for the use of these services, e.g. a customized user interface.

Context-specific preferences

Many user preferences will refer to a specific context. In a certain context the user would like to receive certain services and prefers to have the services delivered in a specific way. E.g. a user does not want to be disturbed by shopping advertisement during working time, but he/she may want to receive shopping advertisement in the weekend. In a role-based user profile system, a specific profile will be activated according to the current context. This specific profile includes context-specific preferences, specific identity, specific device properties and specific policies[21].

User roles and presence

The extended user profile also contains information about the social roles of the user. This information describes the specific preferences for each profile; does the user want to receive offers from the grocery store, does the user want to receive messages from co-workers etc. The roles may block calls and messages from certain people and/or services, and on top of that the user may assume a presence status that blocks communication all together if he or she is, for instance, on an aeroplane.

The user's culinary preferences, hobbies etc. serve as an intelligent filter for incoming calls, messages, notifications and push services. So even if user preferences are generic, users can define several sets of user preferences on a per-context basis (e.g. at office, at home, at travel), on a per-device basis (laptop A for all emails with large attachments, mobile phone B for work email, mobile phone C for private email), or on an address basis (e.g. store messages from address A for business in network storage A and store messages from address B for private in network storage B).

Users then need to indicate, which profile out of the several profiles user may have created (or default) that should be active, cf. ETSI's situation-dependent profiles [ETSI 2009a].

In multi-device scenarios users may also prefer to use the same active profile in all devices to receive the "same" consistent services at all devices or to have different active profiles on business and privately owned devices for example. Users should also be able to change the contents of each profile at any time from different devices. So profiles belong to the user and are independent of the device from which it was created, and devices need to be synchronized.

User history

The user may choose to record his or her behaviour in order to help adapting the user profile. This information is naturally highly confidential in nature, and the user cannot modify this data, but if he/she wishes, some parts can be deleted.

The history log file is not directly a part of the user profile, but is associated with it. It mimics the user's memory and experience (in principle life-long), and it can serve as a starting point for doing data mining, identifying usage patterns and deducing user preferences, cf. Sect. 4.7. Whether the user wants to be subjected to this analysis or have it done depends on his or her attitude. Again, it is essential that the user is kept on control of personal information, and the user must give permission, at least once, before the start of data mining.

[21] Referred to as situation-dependent profiles by ETSI [ETSI 2009a]

If the analysis is carried out (more or less continuously) the system may propose updates to the user profile, which then must be authorized by the user. If carefully designed, it will add value for the user and improve the service offerings and usage over time, cf. Figure 6.

5.2.3 Device settings

The user will often want to apply personal preferences and settings for each of his or her devices. The settings naturally depend on the device capabilities, which are commonly expressed as **device profiles**. Device profiles are – strictly speaking – not personal, but rather express in a standardized manner the capabilities of a device: Communication interfaces and other connectivity; display resolution; sound, image and video capabilities; operating system and installed software (if applicable); etc.

The user profile should contain information about the **specific** personal devices of the user and personal settings, e.g. tailored user interface, colour themes, language setting, and preferred dictionary. Hence, the combination of settings and the device profile could be stored in the user profile – or the user profile might contain a pointer to another location from where the device profile may be retrieved.

Some of the common standards for device profiles are the Composite Capabilities / Preference Profile (CC/PP) from W3C [W3C CC/PP] and the User Agent Profile, UAProf, which is defined by OMA and is part of the WAP 2.0 specification [OMA UAProf]. More recent work by OMA, the Device Profile Evolution (DPE)[22], takes into account dynamic variation in device capabilities over time.

5.2.4 3rd party profiles

The **3rd-party** components of the user profile contain preferences and information that a 3rd party service provider needs to store in the user profile in order to deliver services to the user. This is a special kind of information, as it must be stored in the user profile, but the user cannot modify it. The user may reject having it or choose to delete it, but then the service can no longer be delivered. Examples of this might be billing information, UID, voice profile, triple play service profile, WiFi-specific parameters, GPRS-specific parameters, etc. [MBD4.3.2].

In addition, whenever the user interacts with a 3rd party service provider, the service provider will collect and maintain subscriber information and a log of the usage history. The latter can be analysed – in conjunction with that of other users – to extract usage patterns and preferences and subsequently tailor advertising, offers and recommendations to the user. A “well-behaved” service provider will clearly state the privacy policy (which the user is asked to accept when signing up), but even so the user cannot know in detail, what his or her data will be used for.

5.2.5 Community or peer-to-peer (P2P) profiles

In general, these profiles govern the user’s interaction with other users in a community or peer-to-peer situation, where the user may make certain personal resources available to others in order to carry out some common task.

In MAGNET Beyond they are referred to as PN Federation (PN-F) and PN Federation participation profiles [MBD4.3.2]. The **PN-F profile** contains all the information about the user’s PN-Fs. The PN-F profile is a data structure that is created, stored and maintained by

[22] http://www.openmobilealliance.org/technical/release_program/docs/rd/oma-rd-dpe-v1_0-20070209-c.pdf, last accessed 16-02-2009.

the federation creator and describes the entire PN-F, while the **PN-F participation profile** contains information and preferences about each specific member. The PN-F participation profile includes the participant's (i.e. the user's) security settings, administrative rights, other preferences etc. The creator or administrator of a PN-F has a copy of all participation profiles and administer each other participant's rights. Strictly speaking, only the PN-F participation profile is part of the user profile.

Web-based social communities are one of the most widely used applications nowadays. These web sites help people to connect with others who share their interests, build online profiles and share contents. In [Chowdhury2008] the author suggested the community platform scenario, where personal profiles are not centrally maintained within the community platform. They are distributed and owners have full control on which information or content will be disclosed to the community. In our envisaged profile we are extending the same idea from a user perspective so that user can supply his membership information of different communities such as LinkedIn, Facebook etc. One way to formalize community membership information is to use the semantic web technology.

To exemplify, let's consider Sabine example as described in Sect. 2.1. Upon receiving a query from Sabine, her personal mobile device will contact the ticket service and ticket service will check her community membership information from her profile to get the information of Sabine's friend from her community profile. The ticket service will try to find out if any friend of her is travelling on the train and if such a seat is available. If so, she will reserve the seat automatically.

5.2.6 Virtual identities

Several instances of the personal information and preferences constitute Virtual Identities (VIDs), which the user may take on and use for specific purposes, cf. Sect. 3.1. Upon creation of a VID, the user selects, which of the already obtained levels of clearance should be active, when using the relevant identity. The information collected over time is thus used to determine the user's preferences with respect to the user's VIDs; each VID has an individual history. The approach is similar to the personal cards proposed by the Higgins framework[23], the Bandit DigitalMe project[24] and Microsoft CardSpace[25].

5.2.7 Policies

Policies are all the settings and rules related to the security and privacy of a user. Which data can be transferred, does the user want his/her real identity revealed, and revealed to whom? Policies include generic policies, service-specific policies and context-specific policies. For example, a user does not allow his/her location to be revealed, when he/she is doing a confidential task. Users will have different policies for different services. A user may want to hide his/her real identity for one service but reveal it for another.

Since the extended user profile contains a vast number of preferences, but also rules as well as social roles, a need for sophisticated policy handling arises. Thus, each entry in the extended user profile needs to have specified to whom it might be disclosed. This could include groups, such as "Friends", "Family", "All my buddies", or specific 3rd party service providers.

A policy framework must deal with different "reasoning" situations from access control,

[23] http://www.eclipse.org/higgins/, last accessed 21-02-2009.
[24] http://code.bandit-project.org/trac/wiki/DigitalMe, last accessed 21-02-2009.
[25] http://msdn.microsoft.com/en-us/library/aa480189.aspx, last accessed 21-02-2009.

protection of profile and context data, to federation formation and mobility decisions required by the service platform. This will consist of a policy engine (reasoner) and a system of semantic policies. Service policies based on W3C's Platform for Privacy Preferences (P3P)[26] should be accommodated. P3P enables web sites to express their privacy practices in a standard format that can be automatically retrieved and easily interpreted by user agents.

5.2.8 User security preferences

When it comes to security, user preferences form a delicate subject to deal with. Users in general tend to care more for functionalities, nice GUIs and usability than their own security. Thus, they usually are willing too easily to give away some of their personal data, lose some of their privacy and in general sacrifice to an extent the security of the applications, services and devices they use.

Alan Westin was the first to divide people to three categories according to their concerns about privacy [Westin 2003]:

- **The privacy fundamentalists**: Fundamentalists are generally distrustful of organizations that ask for their personal information, worried about the accuracy of computerized information and additional uses made of it, and are in favour of new laws and regulatory actions to spell out privacy rights and provide enforceable remedies. They generally choose privacy controls over consumer-service benefits when these compete with each other.
- **The privacy pragmatists**: They weigh the benefits to them of various consumer opportunities and services, protections of public safety or enforcement of personal morality against the degree of intrusiveness of personal information sought and the increase in government power involved. They look to see what practical procedures for accuracy, challenge and correction of errors the business organization or government agency follows when consumer or citizen evaluations are involved. They believe that business organizations or government should "earn" the public's trust rather than assume automatically that they have it. And, where consumer matters are involved, they want the opportunity to decide whether to opt out of even non-evaluative uses of their personal information as in compilations of mailing lists.
- **The privacy unconcerned**: The Unconcerned are generally trustful of organizations collecting their personal information, comfortable with existing organizational procedures and uses, are ready to forego privacy claims to secure consumer-service benefits or public-order values, and not in favour of the enactment of new privacy laws or regulations.

Security experts often say that security in your system forms a chain, and your system is therefore only secure as your weakest link. The system must therefore be protected from naive behaviour of unconcerned users. User security preferences might include:

- Custom personal data filtering: The user can learn at all times what kind of data she is sharing and with which entities. She can set the security clearance needed for someone to be eligible to use certain data, as well as appropriate privacy filters. In case of anonymity, filters cut off any data directly or indirectly leading to the user's physical identity. Of course filters work the other way around, thus blocking out harassment, spam and unwanted disturbance through the context management framework.

[26] http://www.w3.org/P3P/, last accessed 16-02-2009.

- User’s access to personal data: The user may access personal data shared previously with other entities and remotely delete all or part of this data. In case foreign security policies don’t allow this functionality the user will be warned for this at the time of sharing and prompted not to share the data.
- Changing Security Policies: as a more general functionality than the previous ones, all security strategy can be re-defined by the user by using security policy management tools. These changes are appropriately stored inside the security part of profiles.

Chapter 7 will later reflect security and privacy implications of user-centric personalization in ambient and ubiquitous environments in more detail. There, also sociological aspects and user behaviour will be taken into account.

5.3 Context and communication environment

Figure 2 in Chap. 1 has introduced the context as one of the key input parameters to the service logic. Section 4.3 provided some examples of context such as position, speed of movement, target of movement. This information is sensitive information and publishing it might conflict with the privacy expectations of the user. However, the example of Section 4.6 also showed that service provision needs to know this context information in order to prioritize the information like “you don’t need to run, the train is delayed”.

While traditional context information talks about the surroundings of the user, this paper also addresses devices, sensors, communication networks and application-related information as part of the context. Examples of network and device related context identifiers are information stored in device profiles and protocols like CC/PP, UAprof, and UPnP-AV. Context descriptors might even have information about “the user is reading web pages” or “participating in a phone conference”.

There are different ways to organize these types of data. WWRF suggests that the user owns his personal data including his profile and context data. These data are stored in containers and the service logic needs to have some indication about the combination of user profile and context information.

A potential approach is to have a part of the user profile storing “context-related profiles and policies” (or “situation-dependent profiles” [ETSI 2009a]), which would ensure privacy better as compared to providing all information to the service logic. An alternative approach is to split up the service logic in a private part controlled by the user and his equipment and a public part providing the service offers. While the first approach does not require a service logic engine in the user profile, it might be too limited for real context-aware services. We expect this topic to be a study item in future work.

5.4 Identity and subscriber data management

Profile management is closely related to identity management and – from the operators’ perspective – to subscriber data management. Many of the ideas and concepts already developed can be extended to cover user profiles in general rather than just identities or subscriber data.

For the end user, it is desirable to be able to access personal information and services from a single point of entry with a single sign-on function, instead of having to memorize a large number of user-IDs and passwords. If a user has to create separate profiles at each service provider, the entire concept of service discovery based on personalized user data would fall apart. Many projects address the problem of a single sign-on function and different solutions have been presented with various security aspects.

In this Section we briefly describe some of the main international forums, which are working on profile management frameworks.

5.4.1 Liberty Alliance Project (LA)

Liberty Alliance has been a prime exponent for **identity management** and single sign-on (SSO) frameworks. A user can have several identities including the “real” identity and virtual identities, which are a key part of the user profile.

The Liberty Alliance Project (LA) is a global organisation working to define and drive open technology standards, privacy and business guidelines for federated identity management [Liberty]. Liberty Alliance provides technology, knowledge and certifications to build identity into the foundation of mobile and web-based communications and transactions. There are over 150 diverse member companies and organizations in Liberty Alliance, including government organizations, end-user companies, system integrators, and software and hardware vendors.

Groups in Liberty Alliance develop mechanisms to handle identities enabling interoperability and seamless user experiences as well as business relationships between different entities in a distributed environment. The specifications build on existing standards like SAML, SOAP, WS-Security, XML, etc.

The Liberty Alliance key concepts are:

- **Federation –** The act of establishing a relationship between two entities, an association comprising any number of Providers and Identity Providers
- **Principal –** a person or “user”, a system entity whose identity can be authenticated
- **Identity Provider** (IdP) – a service which authenticates and asserts a Principal’s identity
- **Single Sign-On** (SSO) – the Principal’s ability to authenticate with one system entity (Identity Provider) and have that authentication honoured by other system entities, often Service Providers.

An identity provider (IdP) is defined as a computer system that issues credentials to a user and verifies that the issued credentials are valid. Identity providers (IdPs) are since long mainstream. Sometimes they carry other names, like payment service, credit card company, bank, e-government, and even communication service providers are already a kind of IdP, e.g. for providing a SIM card to billions of subscribers. An IdP may operate one or more credential services, each of which issues end user credentials based on standards for identity verification and operations defined by the National Institute of Standards and Technology (NIST). A user can hold credentials from multiple IdPs and a "Federation" of IdPs is also possible.

The concept of personalizing services and making them value-added is not new. It has been described thoroughly in many projects and one project worth mentioning is TV-Anytime [TVA]. In 2004 they joined forces with the Liberty Alliance (cf. Sect. 5.4.1) bringing the concept of IdPs into the project of TV-Anytime and by using metadata to make a standard for digital video recording and thereby open the opportunities for video-on-demand services. The TV-Anytime project introduces the concept of a personalization provider that helps the user find and present his or her wanted media.

A user logs on to authenticate himself to an IdP, and in doing so he or she is automatically authenticated to all service providers or other IdPs that have been trusted by this IdP (a **“circle of trust”**). The different service providers, however, are not allowed to communicate any information about the user between each other.

5.4.2 Identity Commons (IC)

Identity Commons is a community of groups working together on the creation of an open identity and relationship layer for the Internet covering the whole range of social, legal and technical issues. ID commons counts notable members like Google, IBM, Microsoft, VeriSign and Yahoo to mention a few.

The community has working groups considering all serious ongoing initiatives and ended projects to make recommendations for further deployment and lead trends towards an open common identity deployment for all IP based services and therefore also available for mobile terminals. The most prominent working groups on technologies and initiatives cover OpenID, OSIS (Open Source Identity Systems), the Higgins Project, SAML Commons, XDI Commons and the Pamela Project.

5.4.3 OpenID

OpenID is an open source decentralized, lightweight protocol for single sign-on and portable identity with more than 25,000 web sites accepting OpenID. An OpenID is basically a URL and can be a domain name or the URL of an OpenID Identity Provider. This could be a URL like “littleimp.myopenid.com”, and when asked to sign in to an OpenID-enabled site “littleimp.myopenid.com” is written as the user name. When you log in with an OpenID the system logs in to the IdP for validation. This means that on OpenID-enabled sites, web users do not need to remember traditional items of identity such as username and password, but instead simply register with any OpenID IdP.

Since OpenID is decentralized, any website can use OpenID and OpenID does not require a centralized authority to confirm a user’s digital identity and just like email addresses, the user can have more than one OpenID for work, at home or for any other use. However, unlike email, the web sites cannot send spam or access the user’s data unless the user allows it.

OpenID operates with the following terms:

- **End-user –** The person who wants to assert his or her identity to a site.
- **Identifier –** The URL or XRI chosen by the end-user as their OpenID identifier.
- **OpenID Identity Provider –** A service provider offering the service of registering OpenID URLs or XRIs and providing OpenID authentication.
- **Relying party –** The site that wishes to verify the end-user’s identifier referred in Liberty Alliance as a Service Provider (SP).
- **Server or server-agent –** The server that verifies the end-user’s identifier. This may be the end-user’s own server (such as their blog), or a server operated by an IdP.
- **User-agent –** The program (such as a browser) that the end-user is using to access an identity provider or a relying party.
- **Consumer –** an obsolete term for the relying party.

OpenID does not provide its own form of authentication, but if an IdP uses strong authentication, OpenID can be used for secure transactions such as banking and e-commerce.

An example of a bigger OpenID provider is the company Verisign, who is one of world’s biggest providers of secure digital infrastructure. Among other roles Verisign is acting as a Personal Identity Provider (PIP), and it has also adapted and enabled the OpenID technology. Verisign does not release software, as most of the software is fully proprietary, but a PIP portal which also enables OpenID is available online [Verisign], along with a list of OpenID enabled sites [OpenID sites]. However, in many cases the PIP is acting passively depending solely on the user interaction and not proactively predicting the user's needs.

5.4.4 The Kantara Initiative

A recent undertaking is the Kantara Initiative[27], which aims to "shape the future of digital identity" with a mission of "Bridging and harmonizing the identity community with actions that will help ensure secure, identity-based, online interactions while preventing misuse of personal information so that networks will become privacy protecting and more natively trustworthy environments."

5.4.5 OpenSocial Foundation (OpenSocial)

The OpenSocial [OpenSocial API, 2008] community is a non-profit foundation jointly proposed by Yahoo, MySpace, and Google to advance 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 provides a common way for web sites to expose their social graph and more, by taking into account the user preferences when setting up user interface controls for gadgets.

5.4.6 3rd Generation Partnership Project (3GPP)

3GPP (3rd Generation Partnership Project)[28] is a major standardization body dealing with future 3G networks and services. Important activities include the specification of a flexible service architecture based on IP Multimedia Subsystem (IMS) and the Generic User Profile (GUP) framework. The GUP framework addresses **subscriber data management** and is included in the standardization work of ETSI STF 342.

The GUP specification is aimed at managing subscriber data within the operators' domain. It addresses all user-related subscriber data (user description, user services, user devices, etc) with the main objective of providing a single access point to the user-related information originating from different entities and locations. In order to manage their subscribers the operators need to keep track of subscriber data such as [3GPP GUP], [MBD1.2.1]:

- Authorized and subscribed services information
- General user information
- PLMN specific user information
- Privacy control data of the user
- Service-specific information of the user
- Terminal-related data
- Charging and billing related data

The 3GPP Generic User Profile is the collection of data, which is stored and managed by different entities such as the User Environment, the Home Environment, the Visited Network and Value Added Service Provider. The application does not need to know where the user data is stored.

[27] http://kantarainitiative.org/, last accessed 24-05-2009.
[28] http://www.3gpp.org, last accessed 16-02-2009.

An individual service may make use of a number of **User Profile Components** (subset) from the GUP. The **GUP server** (Figure 8) is the key element in the architecture. It contains the metadata that holds the knowledge of the location of the data components and of the different **GUP data repositories**. It also acts as a gatekeeper by authorizing or denying access to profile data. The GUP server either operates in **proxy mode** (collects the requested data and provides it to the requestor), or in **redirect mode** (provides the addresses of the data repositories to the requestor).

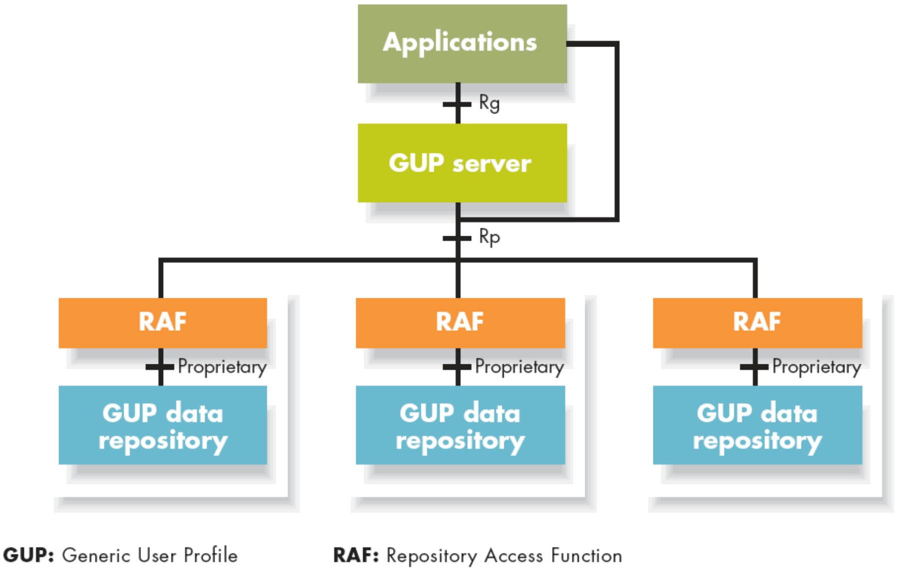


Figure 8: The basic GUP architecture [ucentric], [MBD1.2.1].

The GUP reference points are:

- Reference point R_g: This reference point allows applications to create, read, modify and delete any user profile data using the harmonised access interface.
- Reference point R_p: This reference point allows the GUP Server or applications, excluding external applications to create, read, modify and delete user profile data using the harmonised access interface.

External applications and third party GUP data repositories can be connected to the GUP server by using the R_g reference point only.

3GPP has also done a comprehensive technical study (TR) [3GPP TR32.808] for analysis of a common user model and of the basic structure of a Common Profile Storage (CPS) framework. The study focuses on 3GPP-based networks (IMS-based). In addition, they have started to develop Personal Network Management [(TS 22.259, TS 23.259, and TS 24.259).

A natural extension of the GUP framework would be to enable user profile data to be shared between different stakeholders in order to facilitate:

- **User preference management**
  Enable applications to read and utilize a limited set of user preference information
- **User service customization**
  Enable applications to read and utilize personalized service information, i.e., individual settings for a particular service
- **Terminal capability management**
  Enable applications to access terminal-related capabilities

- **User information sharing**
  Enable applications to read and utilize application level information, e.g. address book information
- **Profile key access**
  Enable applications to use a unique identity as a key to access profile information, e.g. any public user identity or an alias.

e.g. based on an IMS (IP Multimedia Subsystem) approach [3GPP GUP].

5.4.7 Open Mobile Alliance (OMA)

As already mentioned (cf. Sect. 5.2.3), the Open Mobile Alliance (OMA) specifies service enablers and service environments for mobile services.

OMA has also started new related works including Services User Profile Management (ServUserProf) in autumn 2008. The objective is to determine the requirements for the common access data model for "user service-related data", and the access and management of such data in a unified way (also by other OMA service enabler). ServUserProf should support and promote new personalization and contextualization of services and content. It will probably reside in the Service Provider environment. This work is related to 3GPP's Generic User Profile (GUP) and User Data Convergence (UDC) and might reuse mechanisms etc. But in general device user profile settings are out of GUP scope. Also, OMA General Service Subscription Management (GSSM) has relations (that are under discussions) with ServUserProf, but it is more focused on service subscription data and profile.

All OMA specifications must be agnostic to the underlying network in wireline and wireless implementations to support the Internet Protocol family (not only IMS framework).

5.5 Towards a unified profile management framework

5.5.1 Offline and federated user profile

Considering the trade-off between utility and privacy and how to keep the user in control, it is obvious that

- On the one hand the user must always have access to his or her profile data in order to manage and update them as desired, but
- On the other hand user profile data must be revealed to others in order to be useful. An isolated user profile kept on the user's own device(s) would only facilitate the second type of interaction above, where no other persons are involved.

Policies therefore play an important role and a profile management system must ensure that only as much information as needed is revealed (e.g. to a service provider) in order to have a value-added and personalized service delivered to the user. Further, these considerations imply that we need to operate both an "offline" and a "federated" user profile.

MAGNET Beyond has proposed the concept of 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. This is referred to as a "Digital Butler" and it contains parts of the user profile (federated user profile) needed for finding and adapting services to a user's needs. It is obviously a trusted and secure partner for the end user, similar to a bank or credit card provider.

As most of the service discovering requires connectivity (i.e. most of the 3rd party service providers will be online), the most logical idea is to keep it online. That would also help on two other aspects. One is the aspect of power consumption on handheld devices, as this entity would require a lot of processing. The other aspect is that keeping the entity online would make it a more 24/7 value-adding service discoverer adapting relevant services to suit the user.

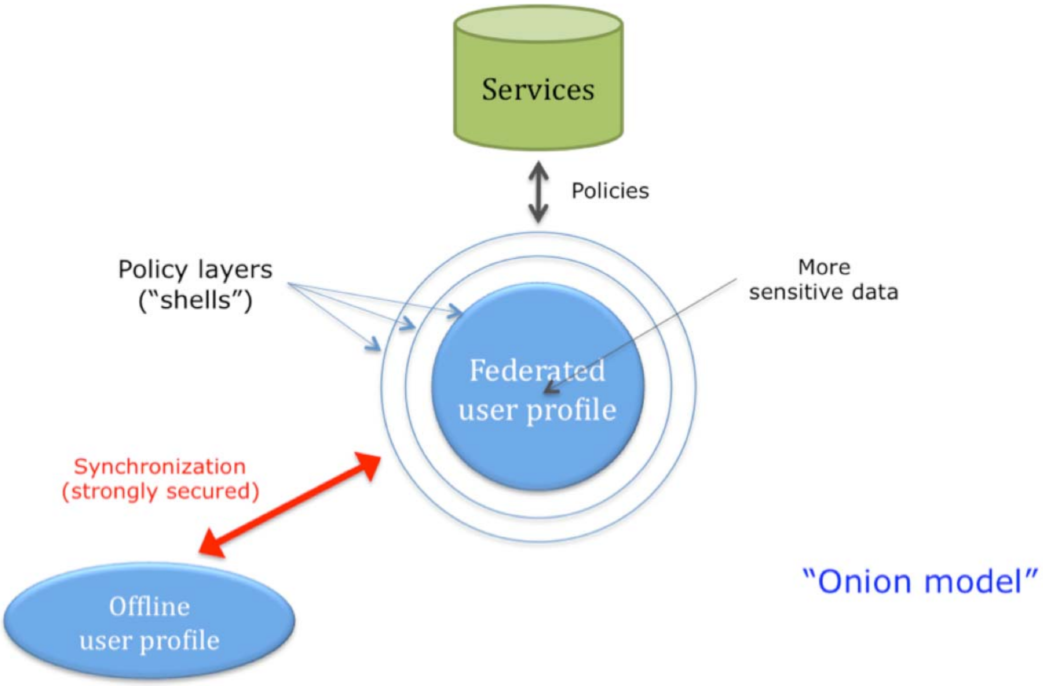


Figure 9: Conceptual view of the offline and federated user profile [MBD4.3.2].

Figure 9 illustrates the concept of the "Digital Butler". It displays the different policy layers of the federated user profile, relating to the fact that a user could have different levels of trust towards different service providers (the "Onion Model"). The shells of the "onion" are meant to illustrate different levels of importance or sensitivity of the personal information contained in the federated profile. The outer layers are least sensitive, meaning limited loss of privacy, whereas getting closer to the core means more sensitive data and stronger policy enforcement.

The offline user profile is synchronized with the online federated profile, which is managed by the "Digital Butler". The "Digital Butler" could be a part of a user's Personal Network (PN) but it is not a requirement. It could also be a 3rd party service provider acting as a **personalization provider (PeP)** working in collaboration with the relevant IdPs, cf. Sect. 5.4. It could actually be one of the IdPs making it more like an autonomous PIP.

The concept of trust is the main issue as the "butler" is actually keeping parts of a user's profile, and it is important only to provide the information to a 3rd party service provider that is in the interest of the user. It is defined in the policy parts of the user profile and enforced in the policy engine. The views of security in the sense of policies are sketched in the following high-level architecture model.

5.5.2 System overview

Taking the concept of the "Digital Butler" further, a high-level overview can be drawn. Figure 10 illustrates how two of the types of user interaction mentioned in the beginning of Section 5.5, interaction with other users and interaction with 3rd party service providers, could be realized. First of all, we distinguish between an "offline" mode, where the user has limited or no connectivity (only short range communication, such as Bluetooth or NFC), and an "online" mode with full connectivity and much more advanced options for personalization and identity management.

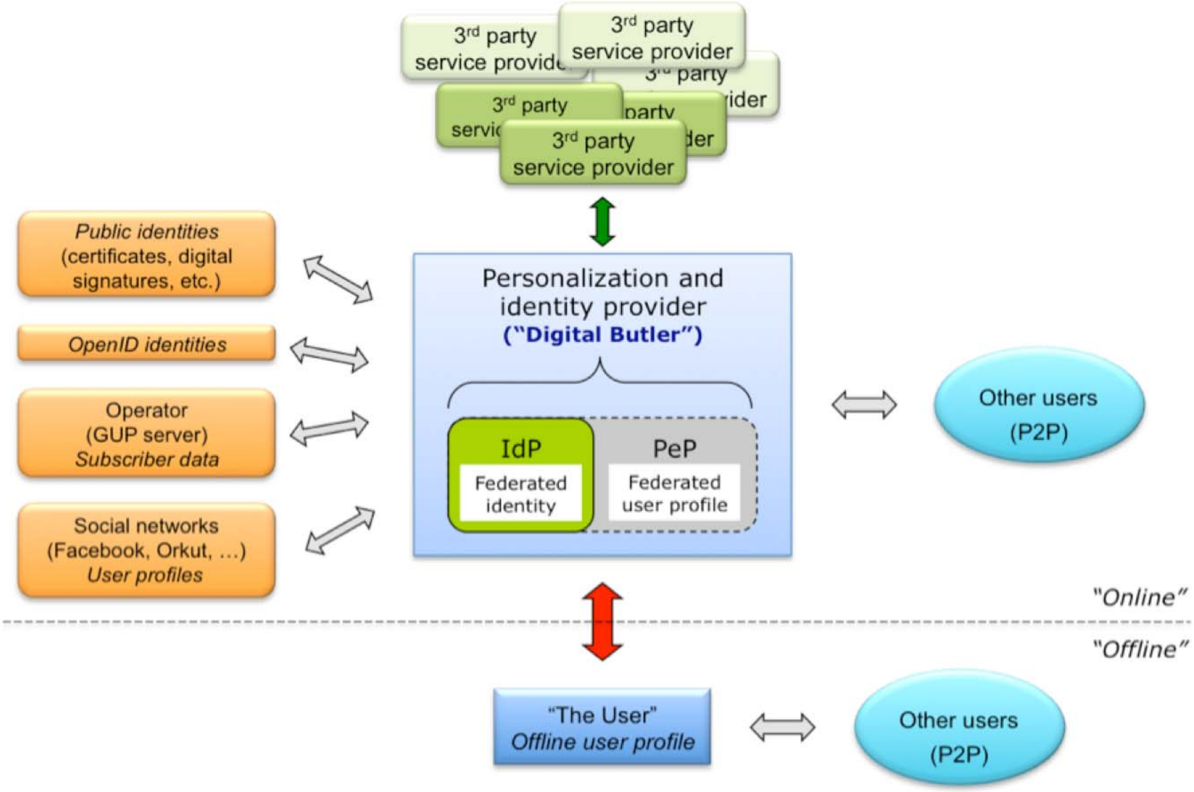

3rd party service provider
3rd party service provider
3rd party service provider
3rd party service provider
3rd party service provider
3rd party service provider
Public identities (certificates, digital signatures, etc.)
OpenID identities
Operator (GUP server) Subscriber data
Social networks (Facebook, Orkut, …) User profiles
Personalization and identity provider ("Digital Butler")
IdP
Federated identity
PeP
Federated user profile
Other users (P2P)
"Online"
"Offline"
"The User" Offline user profile
Other users (P2P)

Figure 10: System overview of user profile and identity management.

In the "offline" mode only the offline user profile with a limited functionality is available for the user. A limited amount of personalization can still be performed when interacting with other users over a short range – or when the user interacts with a device or a system (not shown in the figure).

In the "online" mode the user can fully benefit from having a federated identity and user profile, managed by the "Digital Butler". The offline and federated user profiles are synchronized over a strongly secured and trusted link (red arrow). The "Digital Butler" manages not only the federated identity, but also the federated user profile, interacting with several identities and user profiles belonging to the user, and controlling the interaction with service providers and other users.

The user can have single sign-on functionality to a "circle of trust", including selected 3rd party service providers (darker green) or other users (in MAGNET Beyond: Users in a PN Federation).

The left side of the figure illustrates that the user may already have created several identities, user profiles, and subscriber data (orange boxes), which can be highly distributed. Some of these may be managed by public authorities (citizen IDs, certificates, digital signatures); these are typically used for accessing citizen information (e.g. birth certificate, tax, health data), and other applications involving secure personal access (home banking, transactions). OpenID is developing rapidly (as described in Section 5.4.3), and it will facilitate single sign-on and creation of VIDs (cf. Sect. 3.1). When users subscribe to services from an operator, the operator will manage subscriber data, e.g. based on 3GPP GUP (cf. Section 5.4.6), and as already mentioned the framework of GUP could be extended to handle controlled access to user profiles in general. Finally, social networking sites, such as Facebook, are becoming extremely popular, and many users will already have user profiles to express their interests and preferences.

The profile management system could potentially acquire information from all these sources and build up a user profile in a standardized way, mimicking the conceptual structure discussed in Section 5.2. If (when) user profiles become standardized, service providers would know the general structure on beforehand, if they wish to target a user with their service, and they would be able to query for specific types of information in the user profile, which they might need to adapt and personalize their service to this user. However, they may not be able to access this information, if the policies set by the user forbid it. If so, they can choose to refuse offering their service, or they may deliver a more basic version of the service without the added value of personalization.

As the initial contact and negotiation from the 3rd party service provider to a given user takes place through this user's "Digital Butler", the user is not disturbed unduly. The butler acts as an intelligent spam filter personalizing services according to its owner's needs.

5.5.3 Trust and profile management

While security and privacy requirements suggest bringing the user into the control of his profile and context information, the typical user will not bother to manage his profile. Depending on his personal preferences, he might want to explicitly control access to parts of his profile, e.g. he wants to confirm that someone can read his medical record. A user might also have a preference of carrying parts of his profile with him all the time, examples of which are electronic representations of credit or admittance cards. Thus, access to this information will need access to the user and potentially an explicit action from the user.

Thus we suggest establishing a distributed user profile, where parts of the information are stored in a secure element, e.g. a SIM card, parts in personal devices and other parts in the network. To manage such a distributed profile exceeds the capabilities of a typical user, asking for a new business entity as a trust and profile provider (see also Figure 5 in Sect. 3.5). It should be up to the user to select such a provider, and interfaces between profile components should be based on standardized APIs. Providers might be communities like Mobile Monday[29], OpenID[30], public authorities or business entities like banks or telecommunication providers.

6 Enhancing the user profile

After the initial profile creation, the user profile may be enhanced over time by the user and the surroundings to make it more precise. There are at least 4 different mechanisms to be considered:

- Continuous (manual) update by the user (left side of Figure 6)
- Assisted learning ability and intelligence, e.g. by a "digital butler", based on observation of user behaviour and usage history (bottom feedback loop of Figure 6)
- Peer- or community-assisted development of the user profile (mutual)

[29] Mobile Monday, the world's largest community in mobile service provisioning. http://mobilemonday.org
[30] Open ID, http://openid.org

- Recommender systems, based on user groups

6.1 Update by the user

The set-up and updating of the user profile is illustrated in the left part of Figure 6.

6.1.1 Profile templates

Profile templates and wizards are very important in order to obtain ready-to-use profiles as easily as possible. First-time users, ordinary users and administrators will all benefit from the reduced and hidden complexity and be relieved from the boring work to enter new preferences, settings, rules, etc.

A procedure to initialize and construct user profiles is described in the ETSI guide [ETSI 2005, Chap. 9]. The user initially sets up his or her profile using a wizard and template. The wizard guides the user by explaining and proposing a set of templates that suit different types of users, roles and situations. Information is already filled in as suggested or default values in templates as a starting point. The user can choose to accept the default value or select an alternative value.

There are two types of templates, **creation templates** and **live templates**. The creation template is used for easy creation of user profiles by end-users, service providers, software developers, administrators, etc. Modifications made to creation templates will not affect any rules, settings or user profiles created by them. A live template is a dynamic template associated with user profile, which means modifications made by users to live templates will affect the content of their associated user profiles.

A user profile may or may not associate to a live template, as decided by the user. A live template could be beneficial for a group of users, who have similar characteristics, e.g. all colleagues working in the same company or all members in the same club. It will be convenient to make changes to all of their user profiles by only changing the live template. Inherited information defines inheritance relations between different user profiles owned by the same user.

In constructing the user profiles we must consider existing templates and wizards and ensure the dynamic and flexible nature of the user information. Reuse of existing user profile data as initial values for new services and devices is important, so the same user’s profile data only need to be defined once. In particular, social networking profiles, which are extremely popular, could be reused and merged.

6.1.2 Building profile during usage

After initialization by means of a wizard or template, some information may be missing for new services and devices. Also, the user profile will be further developed and improved during the process of use. When a service or entity needs specific user information, the system will prompt the user for that information and update the result in the user profile. This updating process can be based on roles and common situations (including activities/places such as driving, in a meeting, at the office, or at home). A question may pop up to the user to inquire about his/her preference; a later question will be “is this preference based on the current role?” The answer could be:

- Yes, this preference will be updated based on this specific role.
- No, it is a generic preference to all roles.
- No, it is based on another role.

Thereby, it gives the user the sense of expanding the profile, as he/she explores the supporting framework for personalization. An interesting add-on is that users may benefit from their social network contacts in sharing and developing their profile information.

6.1.3 Profile version control

Some mistakes might occur when handling the user profile because of wrong operation of the user or errors generated by automatic update of the user profile. If the user detects a strange behaviour in the usage of his service, he is able to trace the changes and reverse his user profile to a previous version. Users can choose whether they want their user profile be backed up after a certain time or triggered by a special condition. Users will also be able to choose how many versions of their profile should exist, since too many backups will occupy a large storage space.

6.2 Assisted learning ability and intelligence

As already discussed in Sect. 5.2, the framework incorporates a continuous logging of the user's activities, so that the usage history is recorded. This will lead to "learning ability" and "intelligence" and potentially an improved user experience over time, helping the user to avoid repetition of mistakes or bad experiences from the past.

6.2.1 Learning profiles

There are different forms for profile updates through learning from the behaviour of the user. All these methods have in common that they observe what the user is doing. Different strategies are then used to relate the observations to "habits" and update the profile accordingly. We will shortly present some of the approaches, but remind the reader, that "systems which seam to be more intelligent than the user are neglected from the user" [Nyseth 2003].

Association Rule Learning is a special kind of learning by observation. First, different types of user-related data are captured, such as user behaviour, user preferences, and different types of other user-related contexts. These observations are gathered as snapshots, in which the captured data is linked to each other. Afterwards, a mining algorithm evaluates the snapshots and represents found associations by means of association rules. An association rule of the form X => Y could for example say that whenever the sun was shining on a Sunday, the user went playing golf. The most interesting parameter is the confidence of an association rule, which shows how often the association rule X => Y is supported in case the item X is supported in a snapshot. Based on predefined values for the minimum confidence, the mining algorithm decides whether association rules are or are not selected for the user's profile and for personalization purposes [Menzies 2003].

This learner could be used for learning user interests concerning content, services, preferred input and output modalities with end-user devices, and others. In the example of modality learning, multiple data items could be used such as information on end-user devices, used modality, renderer and network. Examples for modality values could be text, audio and video.

Decision Tree Learning is another approach that is often used in the area of knowledge retrieval and machine learning. A tree structure is used for the classification of data into features, and can be converted to a set of rules. However, this approach only supports the learning of rules for one target item, whereas it is often envisioned to support several target items, as mentioned in the above section on association rules [Menzies 2003].

Another learning approach is based on tree-augmented naive Bayesian classifiers [Friedman

1997]. This is for example used by a system for context-dependent user modelling [Nurmi 2006]. In this system, context-dependent user models are learned and applied for the personalization of applications in mobile environment. The user models attempt to include the user's interests and these interests are linked to the situation of the user. Afterwards, the models can be used for making recommendations on what the user might be interested in her current situation. Yet another approach uses the Ripper rule-learning algorithm [Cohan 1995]. This algorithm is also used for learning context-dependent user models, as explained in [Lau 2007].

6.2.2 Analysis of user history

Analysing the user history for advanced service provision is a common technology very similar to the ones presented in Section 6.2.1. The difference is in the usage of historical data instead of actual observations.

A different time of observation is currently hard to capture by semantic systems. While these systems are good on structuring information and relating information to each other, they are less usable for providing time-related descriptions. If a user interest was stated today, yesterday or five years ago is not captured. A potential approach to overcome this lack is to use the learning profile to "decrease or increase" interest flags, e.g. times for TV watching is recorded and adjusts the interests flags. However, this measure has difficulties to take into considerations cyclic events, like "interests in winter sports only if there is snow". We regard these areas as subject for future research.

6.2.3 Data mining and intelligence

In a vast universe of information and services the user will benefit tremendously from having a system, which can sort and filter the information, and it is also necessary to develop systems that can perform intelligent searches in these services. In order for push services to become a success, users should be protected against irrelevant (push) service offers from 3rd party service providers. Many search engines have been made to solve this problem, and the most common search method simply matches a range of criteria.

Instead of statistically based service presentation, services should be presented in an intelligent manner, according to the individual user's behaviour. The system should be able to learn, what the user normally requires in different situations. "*Fuzzy logic*" could allow a system to adapt to user behaviour and allow for exceptions – just because a person one day stays home because of illness, the system should not stop giving a wake-up call in the morning.

In other words, the system has basic default settings, and user behaviour in a number of chosen categories should be **mined** for data in a manner, where the computer prompts the user to answer questions, upon which the computer system changes both its behaviour and the way these changes are made (double-loop learning).

Some users prefer a very superficial interface with service providers, while others prefer a deep and intelligent interface. The system must be able to determine the depth of this vertical differentiation and integration of information. No matter the depth of interface, the system needs to determine normal behaviour in each type of situation in the horizontal differentiation and integration of information. Some users enjoy receiving free advertising when shopping in their leisure time, while they reject any advertisement when working.

System requirements regarding desirable depth of data mining and degree of precision in each case must be determined.

6.3 Peer- or community-assisted development of the user profile

A major challenge in user profiling is the process of establishing and maintaining valuable profile information. Recent developments in communities and community software suggest using the relations of users to provide them with profile updates. Ling and Yttri suggested the term of micro-coordination for describing the community interaction of mobile users back in 2002 [Ling 2002]. While they focused on SMS as a technology for keeping contact on a minute-to-minute basis, mobile community sites like Twitter[31], Jaiku[32] and mFacebook[33] allow users to report any detailed action from their mobile phone to the whole community.

Communities might be the arena for profile development and profile updating. Friends can help each other to develop profiles, or communities might suggest structures for profiles. Actual interests might be fed through the contributions or behaviour of other community members, e.g. "your close friend recommends reading this book" or "five of your friends have watched this film".

Collaborative filtering recommends user interests based on what other similar users have liked. It could also be described as making automatic predictions (filtering) about the interests of a user by collecting and evaluating information from many users (collaborating). These filtering methods can be divided into two groups. The first group uses all available data when making recommendations. The quality of this group of algorithms typically increases with the size of the user population. However, the diversity of the recommendations decreases as the size of the population grows. The second group, on the other hand, learns a statistical model from the available data at some point, and uses that model in the future.

Methods are also distinguished into active and passive as well as into explicit and implicit collaborative filtering. With active filtering, it is meant that people with similar interests rate items, e.g. products, and share this information. An example of this is the Web, in which people want to share consumer information with other people. Passive filtering, on the other hand, collects information implicitly. This could e.g. be done by a Web browser that records the actions of users when purchasing items or downloading items. Furthermore, explicit filtering requires the user to rate the learned content, whereas implicit filtering does not involve the direct feedback by the user.

Collaborative filtering could for example be used for recommending points of interest to users based on the interest of users with similar profiles. This could be done in letting the user specify some input parameters, e.g. point of interest of category restaurant, and the collaborative filtering algorithm evaluates a ranked list of recommended restaurants based on the interests of other users in the past.

6.4 Recommender systems

An alternative approach is to establish the user likes or dislikes simply by monitoring his behaviour in service consumption. The WellCom project[34] uses the mobile phone as context indicator "watching channel xy on TV" and relates user interests to information provided by the electronic service guide. From this, an alternative user profile can be generated (without active participation by the user), and the service logic of Figure 2 (Chap. 1) is then a recommender system, as displayed in Figure 11.

[31] Twitter "What are you doing right now?" http://twitter.com

[32] Jaiku "Create your activity stream", http://jaiku.com

[33] mobile Facebook, http://m.facebook.com

[34] ITEA WellCom project on interactive TV, http://www.itea-wellcom.org.

The WellCom recommender system uses

- Context information as “who is in front of the TV” and “what channel is consumed”,
- User profile information as “which preferences does the user have”, and
- Media content through an electronic service guide.

The recommender provides a list of prioritized services/content based on the interests of all users being in the vicinity of the TV, allowing the user to select from both private and broadcast content. The recommender system can also be used for monitoring the user interest in content.

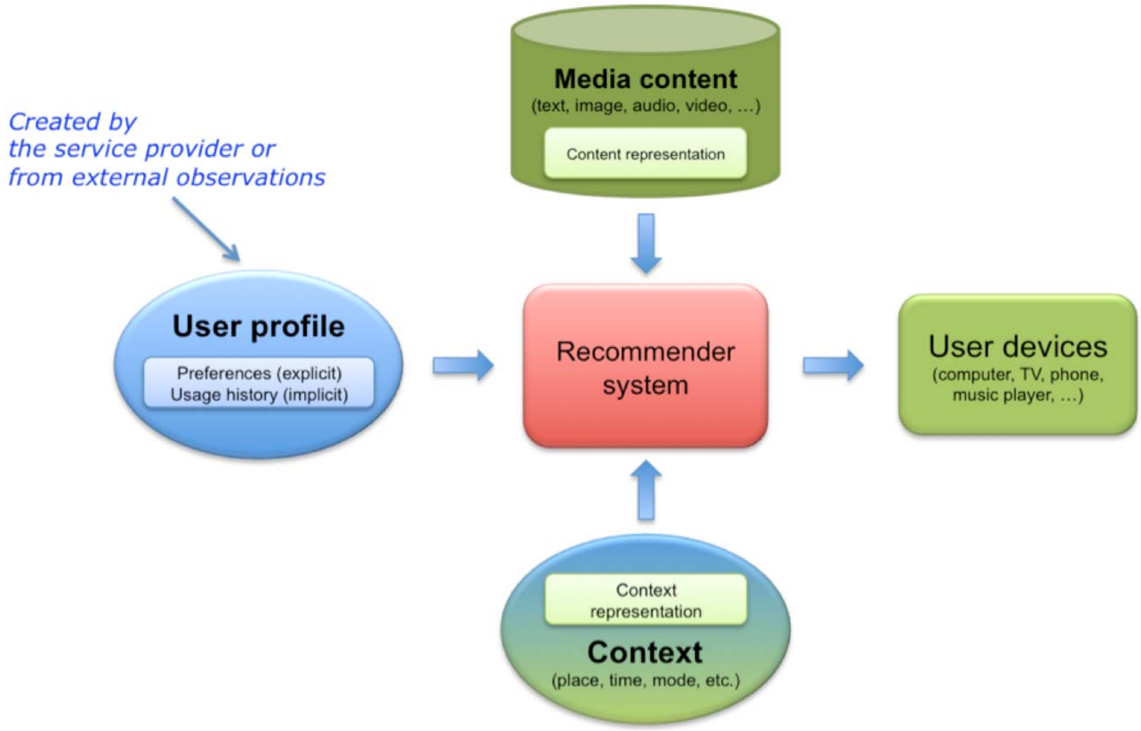


Figure 11: Personalized media consumption (inspired by [Butkus 2009]).

Studies performed in related research show that 15 dedicated recordings will satisfy 95 % of viewing time [Brajal 2008], meaning that very little user interaction is required to establish a user profile, which triggers content selection.

All these approaches suggest to remove as much as possible hurdle from the user, thus defining systems, which will automatically establish and update user profiles based on some limited user input.

7 Analysing privacy-enhanced personalization

The previous chapters have pointed out how to structure, manage and enhance the structure of user profiles discussing different scenarios, use cases and specific aspects. The kind of service personalization introduced, however, has implications to security requirements that might be identified by service providers and network operators, as well as privacy concerns end users might raise. The following chapter is dedicated to the analysis of those security and privacy implications.

User profiles and personalization in the WWRF scenarios such as the “coming home scenario” described in Chapter 2 or more generally in ambient environments have specific implications to security requirements and – even more – to privacy concerns and data protection. On the one hand these ambient environments are characterized by pervasive and ubiquitous computer infrastructures that are supposed to make the user's life easier and more comfortable. On the other hand personalization is based on individual information that is analysed, aggregated, linked, compared and stored in backend systems, which obviously raise serious questions such as "Which information is stored and where?", "Who and what has access to such information?" and "For how long is this information available?".

The Wireless World Research Forum states at its website "7 trillion wireless devices serving 7 billion people in 2020". This vision reflects the increasing trend of introducing micro- and nano-sized computers to everyday devices and tools (Ubiquitous Computing, Internet of Things). However, in ambient environments not only computer systems become transparent and ubiquitous to users but also the users and their contexts become transparent and ubiquitous to the systems running in the background. And the more computers become transparent and ubiquitous the more the user's privacy and control is at stake.

Therefore, this Chapter discusses different perspectives on how the increasing amount of information in future ambient environments, which is either personal or can be personalized, can be used and misused. A detailed privacy analysis gives an overview of how individuals perceive and benefit from the right to privacy and how future scenarios can be analysed. Finally, three categories of privacy enhancing technologies will be introduced.

7.1 Use of personal information

The use of personal information can be analysed from different perspectives. A user-centric view focuses on the mechanisms and features that enable users to manage and control the life cycle of their personal information, e.g. his virtual identities, and how they can benefit from personalized services. A service provider-centric view highlights business opportunities based on user profile and context information, and how this information can be securely stored. Whereas a network operator-centric perspective mainly deals with issues on how operators may enable and support service providers with identity management, accounting and billing.

7.1.1 User-centric view

In the ambient setting the benefit of personalization to the user comes from the adaptability of the environment. Thus, in theory, when the user discloses information, better services suited for that particular user can be provided. This could be related for automatically selecting connectivity services based on certain pricing, for instance, but it could be something on the higher level as well, like usability enhancements. Services free of charge are of course also a key argument for users to share personal information to advertisers and sponsors. This can be further complemented with a requirement to agree to receive such targeted marketing, e.g. in the form of SMSs.

However, what sort of information the users might be willing to disclose and how long time they expect information to be stored, is another matter. Generally, users seem more comfortable with releasing demographic information than specific contact or financial information [Metzger 2004]. Additionally, many users lie about their profile data, so the accuracy of personalization suffers from this.

7.1.2 Service provider-centric view

The service providers naturally are interested in receiving usage data from their customers in order to keep up with the current trends and maximise the cost efficiency of their offerings, i.e. the marketing efforts can be concentrated on the correct focus group. In terms of free services this can even lead to new business models for certain service providers.

The providers also need enough identification information to know who will be paying the bills or enough information to be able to do efficient advertisements for the free services. This kind of personalization information can also become a commodity between the service providers. While the marketing people might be content with less identifiable individuals, more sinister examples are the lists of email addresses and credit card numbers sold to spammers and fraudsters.

Naturally, they can also increase customer satisfaction by providing consistent view on the services and increase interactivity based on personalization and context, but still taking into account the possible limitations and adaptations which might result from using multiple devices and networks.

7.1.3 Network operator-centric view

The availability of context information connected to customer contacts allows the network operators to provide better service to the customers as they are able to provide “correct” kind of connectivity and operability, i.e. it is possible to better optimise the available bandwidth and resource usage. The customers experience better quality of the service when the networks adapt to their needs in a pro-active manner, thus increasing their satisfaction with the current operator. This allows better possibilities to hold on to these customers, as the competition in access provisioning will be much fiercer in the highly dynamic ambient environment.

7.2 Security and privacy analysis

7.2.1 Threats to privacy – state of the art

In the ambient setting the threats to user privacy come from many sources and it is less controllable than the traditional people-to-people communication, as information is mediated and can also be recorded. Thus, the lifespan of the information availability is vastly different. Through their actions the users might reveal more information than they intended in such communication. On top of that, the intelligent ambient environment has the possibility to collect data, which the user might have little control over afterwards. Also, the technology could contain glitches and shortcomings that allowed unauthorized access to sensitive data.

7.2.1.1 User aspects

Perhaps the biggest contributors to the unauthorized information disclosure are the users themselves. There is not much a specific control mechanism can do if the user is asked to provide information and the user wishes to do so, even though he might not realize what is about to happen. Even though it can be claimed that the users are privacy-conscious and wary about giving out their personal information, studies have shown that their actual actions might be contrary to this [Spiekermann et al. 2001]. While this can be done with innocent looking questions, it can be a more large-scale social engineering attack, which lures the user in giving out more information than intended by employing different kind of psychological “gimmicks” [Heikkinen 2006]. Naturally, social engineering techniques can almost always be used in various creative ways to gain access to personal profile information or resources. When it comes to privacy, the user may not always be very logical, but instead seek immediate gratification for their actions [Acquisti 2004]. Also, when people have already revealed some information in a certain context, they feel more committed to their actions and can reveal additional information more easily [Workman 2008].

7.2.1.2 Service-related threats

As the technology gives people more chances for interaction, the potential for sensitive information disclosure also increases. A good example of this nowadays is the emergence of social networking sites. People can give out quite personal information about themselves as they might think that they are just linked to their friends. Among a peer group some might even feel that they are giving a vote of distrust, if they do not share sensitive data [WeirichSasse 2001]. However, it might not be quite transparent, what sort of default setting the service is using and it might require additional user actions to tune the privacy settings. The users are not generally interested in configuration and even less in security-related configurations, which might be too complex for them anyway [WhittenTygar 1999]. Another point is that these sites are also evolving into application platforms, which makes it possible for people to suggest applications to their friends. When this kind of suggestion comes from a friend, the user may not think twice about giving the application access to private information and let their curiosity get the best of them. Like Peter Guttman has noted, “people just want to see the dancing bunnies” [Guttman 2008].

The services might have some privacy policies, but this does not guarantee that they are understandable to users or that users even read them. For instance, how many have realized that when signing into Facebook, they give the site the right to collect information about the user from various other sources as well [Facebook 2008]? Or do they realize what sort of data handling policies they conduct and how it is controlled and audited within the company who is authorized to see the private data?

7.2.1.3 Shortcomings of technological environment

Another thing is that while these sites contain enormous amounts of information about the users, they make attractive targets for attacks. The same applies to any other future service that might be hosting profile information, like attribute providers envisaged in Liberty Alliance model [Hodges 2007]. Often the user has little control or knowledge how his information is protected on such sites. There have been quite many records about incidents, where user passwords or credit card numbers have been stolen from a poorly protected site. This is actually even more severe considering the fact that the people have the tendency to reuse their passwords on different sites. With regard to the user data, it is another question what happens to it when the user leaves the service, i.e. are there guarantees that the available information is removed? With the existence of caches and archiving services, it might be hard to make certain that data is no longer available [NolanLevesque 2005].

One emerging threat is the context information. As future systems are envisaged to take advantage of context information, this gives additional possibilities for information leakage. So, someone else’s “sphere of influence” might contain the nearby user and use that information in a way, which is uncontrollable by the user. For instance, if some security surveillance system like Remote Personnel Assessment (RPA) collects records of people’s blood pressures or some other bodily function in order to find nervous people, can people really control this? Or one could combine little pieces of information from several sources and violate the privacy that way. This has already happened in case of cleverly combining data of anonymous movie reviews from different sites and figuring out who is who [Narayanan 2008]. In a similar sense, lot of other behaviour can be used to infer the identity of the users, such as queries they make [Barbaro 2006] or content they access [Carey et al. 2003]. Of course, sometimes it might be possible that one makes a mistake of interpreting the context information, which might lead to awkward situations in social awareness systems [Lehikoinen 2008]. For some, it is also a cause of worry, if the data is not kept with the context [AdamsSasse 1999]. The similar concerns can also be applied to cases, where there is no certainty and common understanding of the semantic interpretation of the data, i.e. the authentic source data could get a different kind of meaning when the semantic interpretation is distorted.

7.2.2 Privacy requirements engineering

In order to develop a structured approach to identifying future challenges of ambient environments this section illustrates a general privacy requirements engineering process (Figure 12). The aim is to be able to identify appropriate approaches, technologies and mechanisms that lead to an adequate balance between stakeholders' interests and user-centric constraints.

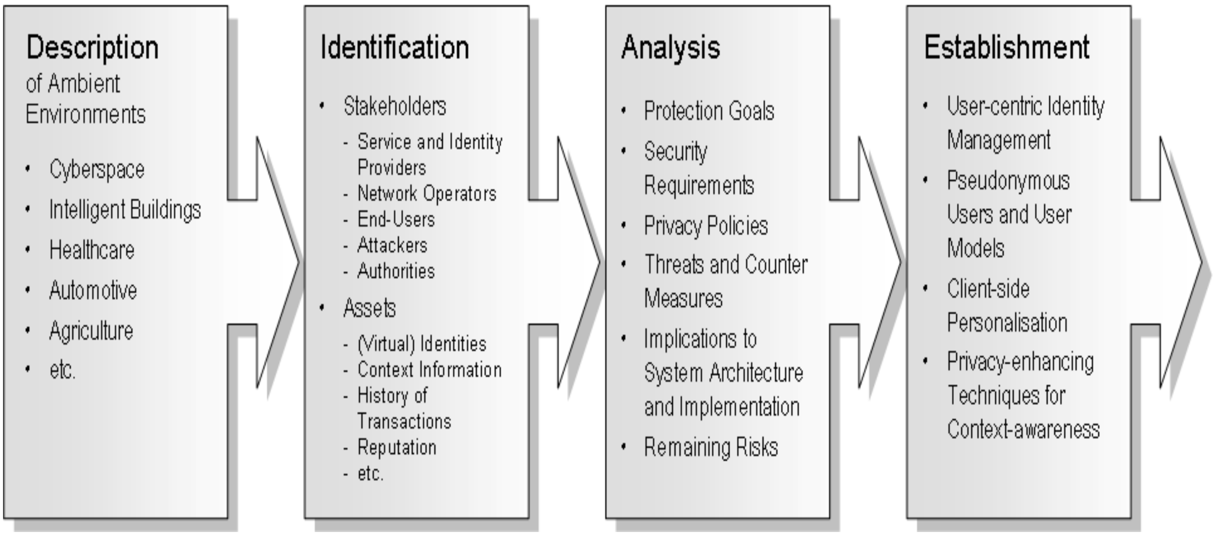


Figure 12: Privacy requirements engineering process.

The process [Robertson 2006] is divided into four parts that will be briefly introduced in the following subsections.

7.2.2.1 Description of ambient environments

Detailed descriptions of future ambient environments at the beginning of the requirements process aim at getting an in-depth understanding of cooperating processes and technologies in a specific scenario. This serves in the following to enrich a more *technical* description with first derived implications to security as well as privacy. Comprehensive examples of scenarios, use cases and technical descriptions can be found in [WWRF scenarios] and the projects referenced in Sect. 5.1. Figure 12 lists other the high-level application areas cyberspace, intelligent buildings, healthcare, automotive, and agriculture.

In order to illustrate here the engineering process let's consider a simple example from future healthcare: Technically speaking in a couple of years intelligent healthcare will be characterized by bio-sensors, mobile devices, wireless smartcards and (central) databases. Biosensors will monitor vital functions and send them for aggregation to a mobile device probably integrated in wearable computing systems. The smartcards will be typically used at the doctor, in hospitals, and pharmacies for personalized access to the patient's medical record.

7.2.2.2 Identification of stakeholders and assets

In a second step the stakeholders of such scenarios as well as their roles and assets will be identified. Stakeholders, however, may not be easily derived from the technical scenario. In the healthcare example above some are obvious, such as the patient, the doctor, nurses, the family and the pharmacist. Other parties who might be interested in health records are not so obvious such as insurances, employers, researchers, and authorities.

Emphasizing the privacy interests of patients for example typical assets comprise at least the patient’s identity, the smartcard, the bio-sensors, any intelligent device connected to these sensors and his personal health record. However, a detailed analysis of the assets of all stakeholders is out of the scope of this paper.

7.2.2.3 Analysis of threats and risks

The third step of the requirements process continues with a detailed security analysis taking all interests and roles of all stakeholders into account including considering everyone in a sub-step as a potential attacker in order to identify so-called dark scenarios. Based on this analysis one can define what “intended” and “non-intended” usage in a specific scenario particularly means and analyse the threats and risks each stakeholder has to face with respect to his assets. A good starting point for this analysis are the well known – depending on the literature – five to seven high-level protection go7als comprising authenticity, confidentiality, integrity, availability, and non-repudiation [Müller et al. 1999]. In addition sub-goals for privacy enhancing scenarios are taken into account such as user empowerment, data minimisation, and minimal disclosure of information. The result of step three is then a comprehensive list of particular privacy requirements and policies.

7.2.2.4 Establishment of privacy-enhancing technologies

The fourth and final step is dedicated to mechanisms and technologies that help to meet and balance security requirements and privacy constraints as well as to address and tackle certain challenges and risks. As high-level technique Figure 12 highlights user-centric identity management, pseudonyms, client-side personalization and privacy-enhanced context awareness [Kobsa 2007]. Three basic categories of privacy-enhancing technologies will be introduced in the next section.

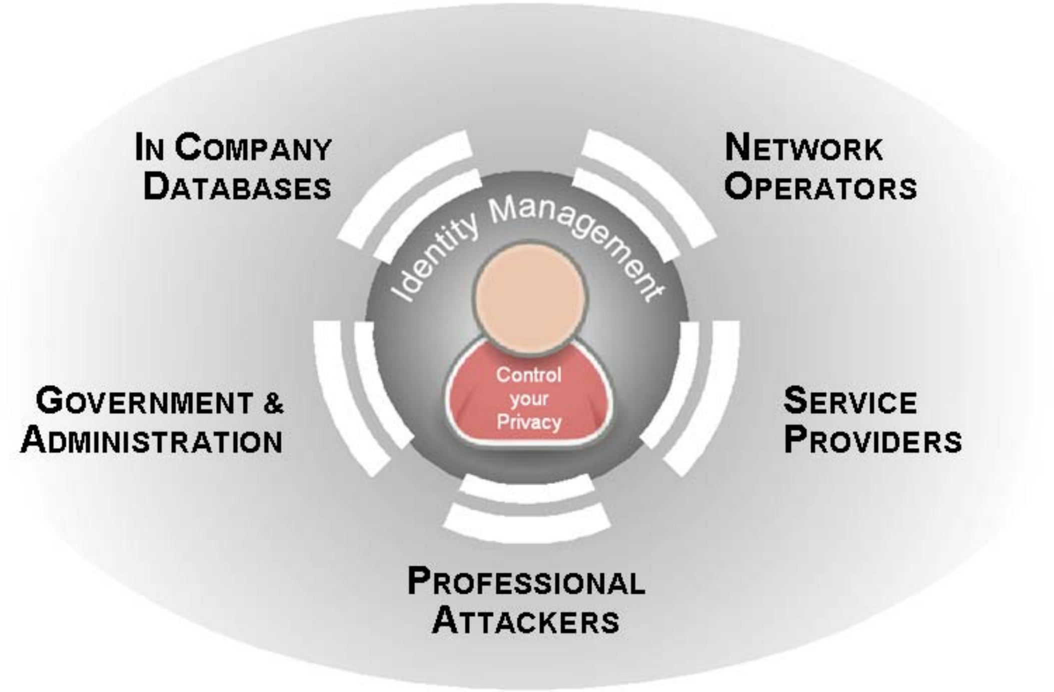
7.3 Privacy-enhancing technologies

7.3.1 User-centric identity management

User centricity in identity management, here, means that the user is not only in the centre of all considerations but also the one who is in control (user empowerment) with the right to administer his (virtual, partial) identities in order to minimise information disclosure. This is in contrast to approaches where the user is in the centre but for example service and identity providers or network operators are in control of personalized information (see Figure 13).

In the future this becomes even more important as the vision of ambient environments aims at ubiquitous and context-aware support by always-available computer systems working transparently in the background. Many supporting tasks, however, will be inherently based on detailed context information that can be personalized, and on information about profiles and preferences of certain identities interacting with these intelligent environments. The more personal digital information is available, thus, the higher the risk of non-intended usage. Omni-presence must not lead to omni-persistence.

Figure 13: User-centric identity management.



Therefore, besides the "Digital Butler" approach of MAGNET Beyond that has been introduced in detail in Chapter 5 and general approaches to identity management driven by industry and academic, such as MS CardSpace, Liberty Alliance, OpenID, Shibboleth and Higgins, three perspectives of user-centric identity management are worth adding and distinguishing here:

- PrimeLife (http://www.primelife.eu, the successor of PRIME) started in March 2008 aims at making tools for privacy-enhancing identity management widely available;
- SWIFT (http://www.ist-swift.org, the successor of DAIDALOS) started in Jan 2008 covers user-centric identity management from the perspective of mobile operators;
- HYDRA (http://www.hydramiddleware.eu) started in Jul 2006 develops a middleware for ambient environments including support for user-centric identity management.

ETSI has also published a comprehensive report on identity management in Next Generation Networks [ETSI NGN, 2008].

Future research projects, in addition, have to take the trend of interoperability and convergence of "fixed-mobile-ambient" more into account. The more this trend supports that real and virtual identities from different domains will converge, the more user-centric identity management will gain attention.

7.3.2 Anonymizers

There are already some simple ways for the users to enhance their privacy by applying different kind of anonymizing services. The similar techniques could be used in the ambient environment as well, even though the mobility and the possibility to have several points of access to the network pose extra challenges, as the user no longer is so clearly within a single controlled domain. Naturally, there might be some regulative requirements, such as lawful interception that need to be taken into account, at least from the telecom operator perspective.

Basically, the anonymizing services take advantage of an intermediary, who is responsible for hiding the true identity of the user. This could be done by just one gateway or it could be even a complete overlay network to obfuscate the whole routing of information. Common thing, however, for these anonymizers is that there ought to be suitably large population using them. In other words, the anonymity is provided by hiding the individuals inside the mass. The smaller the crowd, the easier it is to pick out individuals.

7.3.3 Policy tools

In order to ensure interoperability, there is a need to have common mechanisms to convey policy information, which can automate the information exchange processes. In other words, standards such as Platform for Privacy Preferences (P3P) can be used to automatically compare the policy of the service and the privacy preferences of the user and decide whether the relevant transaction should proceed. Other mechanisms, such as eXtensible Access Control Markup Language (XACML) can also be used to exchange policy information to control the access to sensitive resources.

8 Legal frameworks and requirements

Having analysed the privacy issues of ubiquitous computing and ambient environments in Chapter 7, there are legal issues to discuss. First, the question arises of whether the current legal frameworks and requirements apply to the new technologies and modes of data processing. Second, it is of utmost interest whether the existing legal solutions are suitable to solve the arising problems.

8.1 Current legal framework

The provisions of the European legal data protection framework (particularly the European Data Protection Directive) are generally drafted without references to specific technologies. There are some national laws on data protection, which comprise regulations on technologies such as chip cards or video surveillance (e.g. sections 6b and 6c of the German Bundesdatenschutzgesetz), but even those laws do not address the specific privacy challenges of ambient environments.

Hence the general data protection rules apply to every process within those environments, as long as this process implies the processing of **personal data** in the meaning of Article 2 (a) of the Data Protection Directive, i.e.

- “any information relating to an identified or identifiable natural person
(‘data subject’)”

According to the directive, an **identifiable person** is

- “one who can be identified, directly or indirectly, in particular by reference to an identification number or to one or more factors specific to his physical, physiological, mental, economic, cultural or social identity”.

The prevailing opinion in doctrine is that the question whether data is related to such an identifiable natural person has to be answered as regards each particular data controller, taking into account the resources he has access to. Thus, the concept of personal data is “relative”, as the same data may be personal data for some data controllers, and anonymous data for others [GolaSchomerus] [RoßnagelScholz].

Although this may sound like a simple definition, the issue is far more complicated than it may seem at first glance. A good example for the problems that can occur, when the question of linkability arises, is the discussion of **whether IP addresses are personal data** under Art. 2 (a) of the Data Protection Directive. There can be no doubt that this is the case from the Access Provider`s point of view, since he has access to the files that link each dynamic IP address with the customer [Schnabel 2009]. But it is unclear whether the same holds true for other Internet Service Providers. This question has been the topic of a long discussion between Google [Fleischer 2007] and European data protection supervisors [Schaar 2008]. Some data protection supervisors call for an objective view on personal data [Pahlen-Brandt 2008], but the ICT industry is reluctant when it comes to that issue [Meyerdierks 2009]. The courts are also undecided. Some stick to concept of "relative linkability" [AG München], others consider IP addresses to be personal data even if they are not being processed by Access Providers [AG Berlin-Mitte]. The Article 29 Working Group has issued a whole working paper dedicated to the concept of "personal data" [Art. 29 Group 2007] and still there is no end of the discussion in sight.

The question of whether a natural person is identifiable will most likely pose major technological and legal questions within the context of ambient environments [FIDIS 7.9]. Even today, there are huge debates around the issue of "linkability" of digital identities in different circumstances, particularly in the context of the Internet [ULD]. Even though every case has to be analysed in detail, there is a general presumption that the more data processed, the higher the probability that a person will be identifiable [FIDIS 7.3].

Whenever a person is identified or identifiable, the general data protection requirements apply. These include, inter alia, the need of a legal basis for the processing of the data (i.e. either legislation or an effective consent of the data subject), the principles of proportionality, purpose binding, data minimization and transparency, the specific rights of the data subject, special safeguards for sensitive data, and the implementation of proper organizational and technical security measures [Kuner 2008].

8.2 A need for changes in the legal framework?

It is apparent however that the future implementation of ambient environments will call the aforementioned principles of data protection law into question. A very obvious example is provided by the customary role of the effective consent of the data subject [Roßnagel 2007]. While there are already serious doubts regarding the effectiveness of the "informed" consent in some of today's applications, it is apparent that in a world of ubiquitous data processing, such a consent will be neither possible nor desirable, as it would simply lead to a burdensome and time-consuming life of reading consent forms.

Recent scientific research has shown that ubiquitous computing comes into conflict with other principles of data protection law as well [Roßnagel 2007]. The development of ad-hoc networks, consisting of continuously changing IT systems of various (mostly private) persons, will seriously dilute the meaning and the role of the "controller" of the data processing in the meaning of Article 2 (d) of the European Data Protection Directive. Data subjects become controllers, controllers become data subjects, and natural persons may even be both at the same time. The same holds true for data processing in P2P networks [Sorge 2007].

Furthermore, the strict enforcement of the principle of transparency could lead to such enormous amounts of information about the processing of the personal data of a natural person that he/she would be incapable of handling it – thus leading to even less transparency. Some argue the purpose-binding principle may be incompatible with the idea of collecting personal data for the unnoticeable and spontaneous assistance of the data subject in future, but yet unknown, situations [Roßnagel 2007], although there are ideas to uphold the principle of purpose-binding in a world of ambient intelligence, e.g. through constructs such as "spaces of accountability" [TAUCIS].

Hence, even though there is no doubt that the principles of data protection law apply to ambient environments, there is the need to re-think their shape and enforceability. The works on the legal data protection issues of RFID [Art. 29 Group 2005], chip cards [Hornung 2005] and context awareness [Roßnagel 2006] can be seen as a first step in this direction, but the difficulties described above go beyond the problems posed by these new technologies. To protect privacy and informational self-determination in an age of ambient intelligence, the law itself needs to adopt.

There have been some proposals put forward in this respect [Roßnagel 2007]: Legal principles have to be implemented in the technology itself through requirements for researchers, developers and integrators. There is a strong need for economic instruments such as privacy seals and audits. Basic architectures need to be designed in accordance with privacy principles instead of security interests (that comes into direct conflict with current developments such as the retention of traffic data). In contrast to most of today's data protection laws, individual persons have to be included as data controllers at least into some parts of the data protection legislation. If the individual is not capable of seeing through the structures of the data processing processes, then supervisory authorities need to be given more and effective competences. Last but not least, it is essential to develop precautionary rules for the processing of data, which cannot (yet) be deemed as relating to an "identifiable person".

It is apparent from this list that there is no need for the law of data protection to surrender to the technological developments. However, the debate on the future of the legal frameworks and requirements of data protection law as regards ambient environments has just begun.

8.3 Recent and future developments regarding fundamental rights

The framework of data protection law consists of two layers. While the statutes and case law may be more relevant for the daily data processing of the controllers, further developments on the fundamental rights level could also contribute to changes in the legal requirements.

On Feb. 27, 2008, the German Bundesverfassungsgericht (federal constitutional court) delivered its decision in a case concerning an act on secret online searching of computers, enacted by the state of Nordrhein-Westfalen. In this ruling, it established a new "fundamental right to confidentiality and integrity of information technology systems" as a sub-group of the general right of personality [BverfG].

It is currently unclear whether other national or European courts will adopt this approach. If they do, then this new right could have a major impact on the future design of the information society [Hornung 2008], [HornungSchnabel 2009]. Picking up the new ideas of the German court would be particularly desirable in view of ambient environments. The new concept has a clear focus on technology. As regards the notion of "integrity", there is no need for "personal data" to apply the fundamental right. Even though the development of ambient networks could pose new questions (e.g. the attribution of systems to specific persons), there appears to be an opportunity to develop appropriate privacy models on this basis.

8.4 Legal considerations for identity management systems[35]

As discussed above, data protection legislation applies to "information relating to an identified or identifiable natural person". The question whether a person is identified or identifiable creates a clear link to identity management systems. Following the definition by Pfitzmann and Hansen [PfitzmannHansen 2008], "managing various partial identities (usually denoted by pseudonyms) of an individual, i.e., administration of identity attributes

[35] Parts of this section are based on [SorgeGirao09].

including the development and choice of the partial identity and pseudonym to be (re-)used in a specific context or role."

Identity management can be seen as a great chance to improve user's privacy, allowing a user to control the kind and amount of identity information that is communicated to others. But how does the technology relate to the above-mentioned legal situation in data protection legislation?

In a typical identity management scenario, identity providers are introduced as additional players. They store comprehensive information about their users' identities – a superset of all attributes that are required by the service providers they use. This may include names and addresses, phone numbers, birthdays, and preferences (e.g. font sizes to be used on web pages). The attributes are obviously personal data for the identity provider. When a user wants to use a service, he authenticates towards his identity provider who confirms this authentication to the service provider. The identity provider will also transmit the attributes needed by the service provider, but not allow linking of other attributes or pseudonyms used in other context. As a consequence, service providers have limited information about their users. They do, however, have comprehensive information about how their services are used. A link between service usage behaviour and users' identities could be established either by the identity provider or the user's Internet Service Provider (ISP). Therefore, the question whether the service provider has *personal* data about his users is equivalent to the question whether IP addresses are considered as personal data (see Sect. 8.1).

8.4.1 Data transfers

What about transfers of data between the three main players (service provider, identity provider, and user)? Restrictions may arise from the already mentioned purpose binding principle, as stated in article 6, section 1b of the European data protection directive:

- Personal data has to be "collected for specified, explicit and legitimate purposes and not further processed in a way incompatible with those purposes".

Despite identity management efforts, personal data are likely to be transferred *from the user to the service provider* – at least if following the opinion that IP addresses are personal data.

Since the purpose of data collection by the service provider is typically only to provide the service itself, any further processing or transfer is illegal. Identity management does not seem to be to the service provider's advantage: Legally, refraining from a full identification of its users does not help, at least at first glance.

Still, there are two major advantages of using identity providers. Firstly, the authentication function is outsourced (and more comfortable for the users). Secondly, the identity provider can provide (possibly short-lived) partial identities and refrain from retaining a mapping to the user's "real-world" identity. In other words, the identity provider can reduce the amount of personal data collected.

This way, the service provider may retain data longer than necessary for service provisioning and even bind them to the partial identity, as long as a mapping to an actual person remains impossible. In particular, this includes deleting the IP address as soon as possible.

Transfer of personal data *from the user to the identity provider*, too, is worth considering. If the user enters into a contract with the identity provider about identity provisioning, collecting all data necessary to fulfil this contract is allowed. Therefore, this case is not problematic. If, on the other hand, an existing network operator (or a service provider) wants to also act as an identity provider, it has to ask for the user's consent (the network operator can use this chance to also ask for additional attributes it needs for its new role).

Finally, there is the relationship between *identity provider and service provider*. Once again, we differentiate two cases: If the user has concluded an identity provisioning contract with the identity provider, the transfer of personal data to the service provider is typically comprised by this contract. However, we can think of scenarios where there is no such contract. If a network operator chooses to act as an identity provider, it could simply decide to give identity information about its users to all service providers it considers trustworthy, as far as the information is needed by them. Obviously, this would be a comfortable means of authentication for the user. It may even serve the fulfilment of a contract—but this is true only for the contract between user and service provider. Though aiming at a more comfortable user experience, this kind of data transfer requires the user's explicit consent or the existence of a contract about identity provisioning.

There may also be reasons for the service provider to transfer personal data to the identity provider. This may be helpful if the identity provider performs additional tasks: For example, it could store reputation information about the user, or store usage information in order to facilitate personalization across several services or for billing purposes. Once again, it depends on contractual relationships whether this is allowed.

Consider the example of an identity provider that also stores user profiles for service personalization. These user profiles would be transferred from service providers. Though this may be convenient, it is typically not necessary for fulfilling the SP's contract with the user. Therefore, it is necessary to extend this contract or to explicitly ask for the user's consent.

8.4.2 Opinion of the Article 29 data protection working party

In 2003, the Article 29 data protection working party adopted a document on "on-line authentication services" [Art. 29 Group 2003], being a subset of identity management systems. The report was mainly concerned with Microsoft's Passport service. As a result of the Working Party's statements, Microsoft decided to perform a number of changes to this service. However, the results of the report are applicable to a wider range of systems. We list those that we believe to be most relevant:

- A centralized system storing personal data may both lead to security risks and facilitate abuse of that data.
- The users should be in control of which data each service provider receives from the identity provider and vice versa.
- The use of a single unique identifier could enable service providers to build user profiles by exchanging information, using the identifier as a key. Users should also be able to access their own unique identifiers. The working party favours the Liberty Alliance Approach, which does not require a single unique identifier for a user.
- The contractual framework between service providers and identity providers plays an important role; contracts should make each party's obligations concerning the processing of personal data explicit.

Though these concerns go (at least in part) beyond actual legal requirements, taking them into consideration is likely to increase user acceptance and reduce the risk of a large-scale data leak.

9 Identified areas of research

It is obvious from the previous chapters that the development and management of user profiles has great potential for improving future services and the way that users interact with their environment, be it devices, systems, other users or service providers. Advances in technology can lead to user empowerment and new business opportunities, but also give rise to ethical and legal questions regarding the handling of sensitive personal information.

A number of research areas and questions can be derived from this work; in the following these are divided into user-, business- and technology-related issues.

9.1 Areas of research on user aspects

- How much of a user profile can be established without “a-priori knowledge”?
- How to deal with attributes of the user, like mood?
- How to ensure that privacy is taken into consideration?
- What are the privacy protection mechanisms?
- Does knowledge of memberships in social communities significantly increase the accuracy of the profile?
- Is there such a thing as a “group profile”?
- How to handle event-related preferences? This includes analyzing user behaviour when important events are happened.
- Are users interested in – or willing to – actively set up and maintain their user profile?
- Will users accept to let a trusted partner (a personalized identity provider) manage their identity and user profile?
- Is the concept of Virtual Identity useful and how does the user manage having a number of VIDs?

9.2 Areas of research on business aspects

- Who owns the profiles?
- Who will host the profile?
- Where to host the profile?
- IIs there a business in hosting the profile?
- Is there a new business opportunity in the role as “personalized identity provider” or “digital butler”? Will users accept this?
- Is there an allowed business in using profiles? Is there a valid business case for which the user always needs to give you access to the profile?
- Is it feasible and desirable to have a framework for unified profile and identity management?
- Global legislation for ambient data.
- Privacy for user data when crossing legislation boundary.

9.3 Areas of research on technology aspects

- User-modified profile structuring, building on templates?
- Explicit versus implicit learning of behaviour
- Relations of concepts, how to express preferences with respect to content in such a way that they can be matched with different ways to organize content (content taxonomies)? E.g. how does “Norwegian soccer” content on a news site relate to the

“Norwegian soccer” structure of the user profile?

- How can we make it easier for the users to manage a large number of distributed user profiles and identities, such as social network profiles, subscription profiles and digital identities?
- Mechanisms for the “onion” approach: “further away from me means less information to you”, but also “further away from me means less interesting for me”, trust management
- Is it possible to combine passive and active personalization approaches, i.e. recommender systems using passive user profiling and the approach with active user involvement and control?
- Service-oriented peer-to-peer profile federation
- Distinction between context and profile, where to place the service logic for context-aware services?
- ETSI work: Profile can access the context (NGN idea)?
- Secured exchange of context and user profile data (policies and policy enforcement)
- What is in the service logic box, how can service adaptation be provided?
- Limitations of semantic technologies, e.g. reasoning and rule execution
- Security and trust in ontologies. We want to secure the entries in the ontologies, control access to different parts of the profile, policies and policy enforcement on profiles
- Dynamic ontologies: Deleting and adding information, time stamps, taking into consideration the “aging” of information
- How trust can be established to share VIDs?
- How long should VIDs be shared by users?

10 Summary

Our surrounding world is changing. Technological development gives us multitude of new ways to communicate with others and to make the environment adapt to our personalized needs and enhance our lives. Users have identities and preferences and they are always in a context or environment, which can influence the way in which they interact with their devices, with other users and with service providers. Knowledge about the individual user and his or her current context will in principle make it possible to optimize content and service delivery to the user instead of delivering a “one size fits all” to a large group of users. If this is properly implemented and managed it will add value for the end users and make the service offerings more attractive. Hence, it adds to the value proposition and can create new business and revenue opportunities.

From a technical perspective, it is already – to some extent – feasible and realistic to assist the users with personalization, adaptation and enhancement, but are users really prepared to take advantage of these possibilities? Nothing comes for free; both user profile and context information are sensitive data, which can easily be misused, if falling in the wrong hands. Can we empower the users, so that they will get the benefits of personalization without losing their privacy?

In this WWRF Outlook we have focused on the challenges of describing user identities, preferences, and other personal information in a user profile, and we have presented a framework for managing user profiles and context information and adapting services in controlled manner based on this information. Also related security, privacy and legal aspects have been analysed.

Realizing the long-term visions of WWRF towards the year 2020 depends not only on general progress in technology, but to a large extent on personalization and intelligent service adaptation mechanisms. Profile and context sharing (interworking) are needed to enhance social networking, communication services and value-added services (not only in the same domain). In Chapter 2, we used the WWRF service scenario "coming home" to reveal and highlight, where and how user profiles together with context information can support personalization and facilitate tasks for the users.

In a world of information overflow and limited device and access networks capabilities, users or systems need to filter information to satisfy these challenges and user demands. In Chapter 3 we described how virtual and role-based ID could support service selection and service prioritization based on user preferences and profiles.

In Chapter 4 we have presented the overall general and conceptual view of how I-Centric profile management puts the user in the centre of service provisioning according to the context, his resources and preferences. A central element of the proposed framework is a "service logic" module, which negotiates service provider policies and user's release policies and performs an intelligent match of content and services to user profile and context information. This functionality should probably be based on ontologies and semantic reasoning. The service logic could result in a personalized list of services being presented to the user, e.g. in the form of an Electronic Service Guide (ESG), and the actual selection and usage of services could be monitored to support automated user profile learning and assist the user in building up experience over time, remembering successes and failures.

A user profile should serve to optimize different user, system and service interactions and make it user-friendlier. It needs to be well structured to work in a consistent and efficient way. However, most users already today have a large number of identities, profiles and subscriptions, which must be taken into account. An important objective is therefore to facilitate the management and control of all these profiles, possibly in a unified template managed and controlled by the user. In Chapter 5 we have introduced the overall structure of the user profile and discussed the main parts of the profile: Identities and personal information (facts), different types of user preferences, device settings, 3rd party profiles and community or peer-to-peer related profiles. We also discussed how to set up and manage the profile based on templates and taking into account existing profiles, identities and subscriber data. Finally, we have discussed the prospects of realizing a unified profile and identity management framework.

After the initial profile creation, the user profile may be enhanced over time by the user and the surroundings by different mechanisms to make it more precise. In Chapter 6 we have discussed how manual user update, assisted learning, peer- or community-assisted and recommender systems can enhance the user profile with more optimized settings.

Gathering personal information in a user profile, making it available to the outside world and monitoring the user's behaviour inherently leads to the risk of undesirable information disclosure and loss of privacy. Therefore, in Chapter 7 we have discussed privacy issues in this new ubiquitous world from the user and technology points of view and how the emerging privacy requirements can be analysed in the ambient scenarios. One of the key concepts is the user centricity that puts the users in control of their identity information. Naturally, the technology has to support this in a convenient and usable way, as the users might not always be aware of all the privacy consequences of their actions.

An important point to consider and covered in Chapter 8 is also the legislation, which sets the framework for sensitive data handling. It is, however, challenging as the communication tends to take global scale and the laws are enacted on local level. Thus, there is need for international discussion and cooperation in order to ensure that common principles are applied and embedded into the technical solutions.

Finally, in Chapter 9 we have identified several areas for future research within user-, business-, and technology aspects.

Summary of remarks:

- The user profile should be user-centric, and not service-/service provider-centric
- Profile and context sharing (interworking) are needed in the long-term WWRF service scenarios (not only in the same domain)
- Virtual and role-based ID should support service selection and service prioritization based on user preferences and profiles
- Main focus is on "hiding complexity" for the user
- Privacy-critical information, such as profile content, *"my context"* (personalizable), usage monitoring and auditing/authorization should be controlled by the user by privacy policies
- Standardization required for profile/service logic interface (ETSI, Telemanagement forum)
- Semantics are a good tool for describing a user and his environment, thus a good starting point for context-aware and personalized service adaptation
- The result of service logic could be a dynamic user interface
- There are also several opportunities to enhance the user profile over time (after the profile creation) that shouldn't be forgotten

Even though the fields of personalization, service adaptation, identity management and privacy protection are moving and developing rapidly, we believe that this Outlook has managed to capture and present a comprehensive body of research. In particular, we have put focus on the need for user centricity and user friendliness in dealing with a growing number of user profiles and identities, the potential of facilitating and enhancing future service consumption and the important issue of privacy protection. It is therefore our hope that the Outlook will serve as an important and useful reference for future research.

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.

[3GPP TR32.808] *Study of Common Profile Storage (CPS) Framework of User Data for network services and management (Release 8)*, 3GPP Technical Specification Group Services and System Aspects TR32.808, Version 8.0.0, June 2007.

[Acquisti 2004] A. Acquisti, “Privacy in Electronic Commerce and the Economics of Immediate Gratification”, In Proceedings of the ACM Electronic Commerce Conference, May 2004.

[AdamsSasse 1999] A. Adams, and A. Sasse, “Taming the wolf in sheep’s clothing: privacy in multimedia communications”, in Proceedings of the seventh ACM international conference on Multimedia. Oct 1999.

[AG Berlin-Mittte] District Court Berlin-Mitte, 27.3.2007 – 5 C 314/06, Datenschutz und Datensicherheit 2007, pp. 856-858.

[AG München] District Court München, 30.9.2008 – 133 C 5677/08, MultiMedia und Recht 2008, p. 860.

[Arbanowski 2004] S. Arbanowski, P. Ballon, K. David, O. Droegehorn, H. Eertink, W. Kellerer, H. van Kranenburg, K. Raatikainen, and R. Popescu-Zeletin, ”I-centric Communications: Personalization, Ambient Awareness, and Adaptability for Future Mobile Services”, IEEE Comm. Magazine, Sep 2004, pp 63-69.

[Art. 29 Group 2003] Art. 29 Data Protection Working Party, Working Document on on-line authentication services, 10054/03/EN, WP 68, 2003, available at http://ec.europa.eu/justice_home/fsj/privacy/docs/wpdocs/2003/2003-01-30-online-authentif_en.pdf.

[Art. 29 Group 2005] Art. 29 Data Protection Working Party, Working document on data protection issues related to RFID technology, 2005, available at http://ec.europa.eu/justice_home/fsj/privacy/docs/wpdocs/2005/wp105_en.pdf.

[Art. 29 Group 2007] Art. 29 Data Protection Working Party, Opinion 4/2007, on the concept of personal data, 2007, available at http://ec.europa.eu/justice_home/fsj/privacy/docs/wpdocs/2007/wp136_en.pdf.

[Barbaro 2006] M. Barbaro, and T. Zeller, “A Face Is Exposed for AOL Searcher No. 4417749”, New York Times online article, available at http://www.nytimes.com/2006/08/09/technology/09aol.html (accessed 06/2008), Aug 2006.

[BoV 2008] “Technologies for the Wireless Future: Wireless World Research Forum, Volume 3”, Klaus David (Editor), Wiley, 2008.

[Brajal 2008] A. Brajal, “Monitoring TV consumption as input for recommender systems”, private communication, 2008.

[Butkus 2009] A. Butkus, “Enhancing media personalization by extraction of similarity knowledge from metadata”, PhD thesis, Technical University of Denmark, 2009.

[BverfG] Bundesverfassungsgericht, decision of 27 February 2008, 1 BvR 370 and 595/07, available at http://www.bundesverfassungsgericht.de/entscheidungen/rs20080227_1bvr037007.html.

[Carey et al. 2003] M. J. Carey, G. D. Tattersall, H. Lloyd-Thomas, and M. J. Russell, “Inferring identity from user behaviour”, in IEEE Proceedings Vision, Image & Signal Processing, vol 150, issue 6, Dec 2003.

[Chowdhury 2008] M. M. R. Chowdhury, N. Elahi, S. Alam, and J. Noll, “A Framework for Privacy in Social Communities”, Special Issue of International Journal of Web Based Communities (IJWBC), Inderscience Publishers, ISSN (online): 1741-8216, ISSN (print): 1477-8394.

[Cohen1995] Cohen, W. W., “Fast Effective Rule Induction”, Proc. 12th International Conference on Machine Learning (ICML), Morgan Kaufmann, 1995.

[ComScore 2007] Social Networking Goes Global, http://www.comscore.com/press/release.asp?press=1555.

[DAIDALOS] The EU IST DAIDALOS project, http://www.ist-daidalos.org.

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

[Donath 1999] J. S. Donath, “Identity and deception in the virtual community”, in ‘Communities in Cyberspace’ by Marc A. Smith, Peter Kollock, Routledge, 1999.

[ePerSpace] “Report of State of the Art in Personalization. Common Framework”, ePerSpace project deliverable D5.1, Feb. 2004. Available online at: http://www.ist-eperspace.org/deliverables/D5.1.pdf

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

[ETSI NGN, 2008] Telecommunications and Internet converged Services and Protocols for Advanced Networking (TISPAN); NGN Security;
Report on issues related to security in identity management and their resolution in the NGN, ETSI Technical Report TR 187 010 v2.1.1 (2008-07), Retrieved April 28, 2009, from http://pda.etsi.org/exchangefolder/tr_187010v020101p.pdf.

[ETSI 2009a] Human Factors (HF); Personalization and User Profile Management; User Profile Preferences and Information, ETSI draft standard ES 202 746, Retrieved Feb. 4, 2009, from http://portal.etsi.org/stfs/STF_HomePages/STF342/ES-202%20746_V12.doc.

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

[Facebook 2008] Facebook, "Terms of Use, November 15, 2007", available at http://www.facebook.com/terms.php (accessed 06/2008)

[FIDIS 7.3] W. Schreurs, M. Hildebrandt, M. Gasson, and K. Warwick (eds.), "FIDIS Deliverable D7.3: Report on Actual and Possible Profiling Techniques in the Field of Ambient Intelligence", available at http://www.fidis.net/fileadmin/fidis/deliverables/fidis-wp7-del7.3.ami_profiling.pdf.

[FIDIS 7.9] M. Hildebrandt, and B.-J. Koops (eds.), "FIDIS Deliverable D7.9: A Vision of Ambient Law", available at http://www.fidis.net/fileadmin/fidis/deliverables/fidis-wp7-d7.9_A_Vision_of_Ambient_Law.pdf.

[Fleischer 2007] P. Fleischer, "Are IP addresses "Personal Data"?", 2007, via http://peterfleischer.blogspot.com/2007/02/are-ip-addresses-personal-data.html.

[Friedman 1997] N. Friedman, D. Geiger, and M. Goldszmidt, "Bayesian Network Classifiers", Machine Learning 29, 1997.

[GolaSchomerus] P. Gola, and R. Schomerus, "Bundesdatenschutzgesetz", 9th edition, 2008.

[Guttman 2008] P. Guttman, "Security Usability Fundamentals,", available at http://www.cs.auckland.ac.nz/~pgut001/pubs/usability.pdf (online article, accessed 06/2008)

[Heikkinen 2006] S. Heikkinen, "Social engineering in the world of emerging communication technologies", in the Proceedings of Wireless World Research Forum meeting #17, Nov 2006.

[Hodges 2007] J. Hodges (ed.), "Liberty Technical Glossary v2.0", Liberty Alliance project specification, Dec 2007.

[Hornung 2005] G. Hornung, Die digitale Identität. Rechtsprobleme von Chipkartenausweisen: digitaler Personalausweis, elektronische Gesundheitskarte, JobCard-Verfahren, 2005 (available at http://kobra.bibliothek.uni-kassel.de/handle/urn:nbn:de:hebis:34-2007113019808).

[Hornung 2008] G. Hornung, Ein neues Grundrecht. Der verfassungsrechtliche Schutz der „Vertraulichkeit und Integrität informationstechnischer Systeme“, Computer und Recht 2008, pp. 209-306.

[HornungSchnabel 2009] G. Hornung, and C. Schnabel, “Data Protection in Germany II: Recent Decisions on Online-Searching of Computers, Automatic Number Plate Recognition and Data Retention”, Computer Law and Security Review 2009, forthcoming.

[Kellerer 2002] W. Kellerer, M. Wagner, R. Hirschfeld, J. Noll, S. Svaet, J. Ferreira, O. Karasti, T. Hudginson, R. Giaffreda, S. Fallis, J. C. Francis, and C. Fischer, “Systems beyond 3G – Operators’ vision”, Eurescom Project P1203, Dec. 2002

[Kobsa 2007] A. Kobsa, “Privacy-Enhanced Personalization,” in Communications of the ACM, vol. 50, no. 8, Aug 2007, pp. 24-33.

[Konstruktors] Konstruktors home page, http://konstruktors.com/blog/understanding-web/259-how-to-be-your-own-openid-provider-and-use-your-blogs-url-for-identification/.

[Kuner 2008] C. Kuner, European Data Protection Law: Corporate Compliance and Regulation, 2nd edition, Oxford University Press, 2008.

[Lau 2007] S. L. Lau, J. Millerat, M. Sutterer, N. Brgulja, O. Coutand, and O. Droegehorn, “Integrating Expert Knowledge into Context Reasoning in Context-Aware Environment”, In Proceedings ASWN 2007, Santander, Spain, May 24-25, 2007.

[Lehikoinen 2008] J. T. Lehikoinen, “Theory and application of the privacy regulation model”, in Handbook of Research on User Interface Design and Evaluation for Mobile Technology, Information Science Reference, Feb 2008.

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

[Ling 2002] R. Ling, and B. Yttri, “Nobody sits at home and waits for the telephone to ring:” Micro and hyper-coordination through the use of the mobile telephone, in Katz, J. and Aakhus, M. (eds.) Perpetual contact: Mobile communication, private talk, public performance. Cambridge University Press, Cambridge, 2002.

[MBD1.2.1] H. Olesen (ed.), “The conceptual structure of user profiles”, IST-027396 MAGNET Beyond deliverable, Sept. 2006. Available from Internet: http://www.magnet.aau.dk/public+deliverables.

[MBD1.2.3] H. Olesen (ed.), “The role of user profiles in PN services and context awareness”, IST-027396 MAGNET Beyond Deliverable D1.2.3, June 2008. Available from Internet: http://www.magnet.aau.dk/public+deliverables.

[MBD1.4.1] J. Schou Pedersen et al., “Usability of PN services (low-fi prototyping)”, IST-027396 MAGNET Beyond Deliverable D1.4.1, June 2007. Available from Internet: http://www.magnet.aau.dk/public+deliverables.

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

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

[MBD4.3.3] D. Kyriazanos (ed.), “Solutions for identity management, trust model and privacy for PNs”, IST-027396 MAGNET Beyond Deliverable D4.3.3, June 2008. Available from Internet: http://www.magnet.aau.dk/public+deliverables.

[Menzies 2003] T. Menzies and Y. Hu, “Data Mining for Very Busy People”, IEEE Computer Society, 2003.

[Metzger 2004] M. Metzger, “Privacy, Trust, and Disclosure: Exploring Barriers to Electronic Commerce” in Journal of Computer-Meditated Communication, vol. 9, no. 4, Jul 2004.

[Meyerdierks 2009] P. Meyerdierks, “Sind IP-Adressen personenbezogene Daten?”, MultiMedia und Recht 2009, pp. 8-13.

[Müller et al. 1999] G. Müller, and K. Rannenberg, (Eds.): Multilateral Security in Communications: Technology, Infrastructure, Economy, Addison-Wesley-Longman, 1999

[Narayanan 2008] A. Narayanan, and V. Shmatikov, “Robust De-anonymization of Large Sparse Datasets”, in Proceedings of IEEE Symposium on Security and Privacy, May 2008.

[NolanLevesque 2005] J. Nolan, and M. Levesque, “Hacking Human: Data-Archaeology and Surveillance in Social Networks”, ACM SIGGROUP Bulletin, Vol. 25, Issue 2, Feb 2005.

[Noll2007] J. Noll, “Who owns the SIM card? – The Trusted Third Party Control of the Secure Element”, Near Field Communications Technology and Application Forum, Marcus Evans Conference, Barcelona, Spain, 4.-6. June 2007

[Nurmi2006] P. Nurmi, A. Salden, S.L. Lau, J. Suomela, M. Sutterer, J. Millerat, M. Martin, E. Lagerspetz, and R. Poortinga, “A System for Context-Dependent User Modeling,”, in On the Move to Meaningful Internet Systems 2006: OTM 2006 Workshops, pages 1894-1903, Montpellier, France, Oct. 2006.

[Nyseth 2003] A. Nyseth, “Experiences from usage patterns in Telenor’s house of the future”, private communication, Telenor, 2003

[OASIS] Organization for the Advancement of Structured Information Standards, http://www.oasis-open.org/specs/.

[OMA BCAST] OMA Mobile Broadcast Services V 1.1, Candidate Enabler 24-03-2009. Available online at http://www.openmobilealliance.org/Technical/release_program/bcast_v1_1.aspx.

[OMA UAProf] "OMA User Agent Profile V2.0", OMA Service Enabler release. Available online at: http://www.openmobilealliance.org/Technical/release_program/uap_v2_0.aspx.

[OpenID sites] OpenID enabled sites, http://openiddirectory.com/.

[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.

[Pahlen-Brandt 2008] I. Pahlen-Brandt, "Datenschutz braucht scharfe Instrumente", Datenschutz und Datensicherheit 2008, pp. 34-40.

[PfitzmannHansen 2008] A. Pfitzmann, and M. Hansen, "Anonymity, unlinkability, undetectability, unobservability, pseudonymity, and identity management – a consolidated proposal for terminology". Version 0.31, 2008 (available at http://dud.inf.tu-dresden.de/literatur/Anon_Terminology_v0.31.pdf)

[PrimeLife report] "First Report on Standardization and Interoperability – Overview and Analysis of Open Source Initiatives", PrimeLife Consortium, Deliverable D3.3.1-D3.4.1, May 2008. Available online at: http://www.primelife.eu/images/stories/deliverables/d3.3.1_d3.4.1-public.pdf.

[Robertson 2006] S. Robertson, and J. Robertson: Mastering the Requirements Process, Addison-Wesley Longman, Amsterdam, 2nd ed., March 2006.

[Roßnagel 2006] A. Roßnagel, S. Jandt, J. Müller, A. Gutscher, and J. Heesen, Datenschutzfragen mobiler kontextbezogener Systeme, 2006.

[Roßnagel 2007] A. Roßnagel, Datenschutz in einem informatisierten Alltag, 2007 (available at http://library.fes.de/pdf-files/stabsabteilung/04548.pdf).

[RoßnagelScholz] A. Roßnagel, and P. Scholz, "Datenschutz durch Anonymität und Pseudonymität", MultiMedia und Recht 2000, pp. 721-731.

[Schaar 2008] P. Schaar "IP Addresses Are Personal Data, E.U. Regulator Says", Washington Post, 22 January 2008, via http://www.washingtonpost.com/wp-dyn/content/article/2008/01/21/AR2008012101340.html.

[Schnabel 2009] C. Schnabel, "Privacy and Data Protection in EC Telecommunications Law", in: C. Koenig, A. Bartosch, J.-D. Braun, M. Romes (eds.), EC Competition and Telecommunications Law, Springer 2009, forthcoming.

[Sorge 2007] C. Sorge, “Datenschutz in P2P-basierten Systemen”, Datenschutz und Datensicherheit 2007, pp. 102-106.

[SorgeGirao09] C. Sorge, J. Girao, and A. Sarma, “Privacy-enabled identity management in the Future Internet”, Future of the Internet Conference, Prague 2009.

[Spiekermann et al. 2001] S. Spiekermann, J. Grossklags, and B. Berendt, “E-privacy in 2nd Generation E-Commerce: Privacy Preferences versus actual Behavior”, in the Proceedings of the 3rd ACM conference on Electronic Commerce, Oct 2001.

[TAUCIS] Unabhängiges Landeszentrum für Datenschutz Schleswig-Holstein und Humboldt-Universität zu Berlin (Ed.), TAUCIS – Technikfolgenabschätzung Ubiquitous Computing und Informationelle Selbstbestimmung, Berlin 2006.

[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.

[ULD] Unabhängiges Landeszentrum für Datenschutz, Verkettung digitaler Identitäten, 2007, available at http://www.datenschutzzentrum.de/ projekte/verkettung/2007-uld-tud-verkettung-digitaler-identitaeten-bmbf.pdf.

[Verisign] Personal Identity Portal from Verisign, https://pip.verisignlabs.com/.

[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.

[WeirichSasse 2001] D. Weirich, and A. Sasse, “Pretty Good Persuasion: A First Step towards Effective Password Security in the Real World”, in Proceedings of the 2001 workshop on New security paradigms, Sep 2001.

[Westin 2003] *Social and Political Dimensions of Privacy*, Alan F. Westin, Columbia University, Journal of Social Issues, Vol. 59, No. 2, 2003, pp. 431-453.

[WhittenTygar 1999] A. Whitten, and J. D. Tygar, “Why Johnny Can't Encrypt: A Usability Evaluation of PGP 5.0”. in Proceedings of the 8th conference on USENIX Security Symposium, Aug 1999.

[Workman 2008] M. Workman, “Wisecrackers: A Theory-Grounded Investigation of Phishing and Pretext Social Engineering Threats to Information Security”, in Journal of the American Society for Information Science and Technology, vol 59, no. 4, Feb 2008.

[WWRF scenarios] L. Sørensen and K. E. Skouby (eds.), “User Scenarios 2020”.
To be submitted for the WWRF Outlook series.

[Zimmermann 2008] R. Zimmermann, "FP7 Workplan and activities for 2009 and beyond", eMobility GA4, Stockholm, 16. Oct. 2008.

Imprint

Wireless World Research Forum
Othmarstrasse 8
CH-8024 Zurich
Switzerland

Secretariat:
Vinod Kumar
Alcatel-Lucent France
Centre de Villarceaux
Route de Villejuste
91 620, NOZAY
France
e-Mail: vinod.kumar@alcatel-lucent.fr
Phone : + 33 1 30 77 27 37
Fax : + 33 1 30 77 61 75

The WWRF is a non-profit organisation registered in Switzerland

Chairman of the Forum:
Dr. Nigel Jefferies

Editor-in-Chief: Mr Sudhir Dixit

The WWRF Outlook Visions and research directions for the Wireless World

ISSN 1662-615X is published non-periodically by the Wireless World Research Forum
http://www.wireless-world-research.org

Responsibility for the contents rests with the Steering Board of the Forum.