Towards the Future Internet
G. Tselentis et al. (Eds.)
IOS Press, 2010
© 2010 The authors and IOS Press. All rights reserved.
doi:10.3233/978-1-60750-539-6-183

The Human side of the Future Internet

Jose SIMOES [a,1], Peter WEIK [a] and Thomas MAGEDANZ [a]

[a] *Fraunhofer Institute FOKUS, Kaiserin-Augusta-Allee, 31, 10589 Berlin, Germany*
{jose.simoes, peter.weik, thomas.magedanz}@fokus.fraunhofer.de

Abstract. Despite all the uncertainties regarding the architectures, protocols and technologies to be used in an Internet of the future, it is clear that it will be shaped for humans, carrying with it major social and economical impact. In this sense, aiming at improving the user perceived Quality of Experience in the Internet of the Future, our paper presents common ground work for designing a unified generic human profile structure and correspondent architecture capable of seamless interacting with a myriad of things and services, independently from their associated technologies. Moreover, supported by its reality, social and context awareness conception principles, it will enable human behavior to be leveraged to any entity present in every single next generation ecosystem.

Keywords. Future Internet, Generic Human Profile, Quality of Experience, Social-aware, User-centric

1. Introduction

Humans in all cultures, at all times tend to form complex social networks. This happens because they are validated by shared perceptions of worth. Likewise, social networks among individuals who may not be related can be validated and maintained by agreement on objectives, social values, or even by choice of entertainment. Therefore, and mainly due to the growing success and adoption of online social networks, it is easy to foresee that the services of the future will become multi-context and social-aware capable. However, to enable such vision we need a ubiquitous technological platform (the Future Internet) that is prepared to address the associated challenges. In this sense, the Internet of the Future can be seen as a seamless fabric of classic networks and networked objects that will not only co-exist but also be intimately bound up with our human world. It will be an Internet with Things, where the content and services it facilitates will be all around us, always on, everywhere, all the time [1].

Nevertheless, despite all the technological revolutions, for the end user (Humans) it is the perceived Quality of Experience (QoE) that counts, where QoE is a consequence of a user's internal state (e.g., predispositions, expectations, needs, motivation, mood), the characteristics of the designed system (e.g., usability, functionality, relevance) and the context (or the environment) within which the interaction occurs (e.g., social setting, meaningfulness of the activity) [2]. In other words, services must become personalized, contextualized, adapted, interactive, mobile, etc. while still concerning privacy. To achieve such scenario it is critical to know more about the users. Consequently, it is

[1] Corresponding Author.

mandatory to find a unified and standardized way of managing users data; that is, accessing, storing, creating and modifying it. However, before focusing on the methodologies, protocols or technologies, it is important to understand what kind of data will leverage an optimized user experience in the Internet of the Future. Hence, in a first instance our work proposes a user identity data structure/profile that encompasses: user preferences, social networks and relationships, policies, devices, profiling algorithms, new knowledge generation, among others. Based on this data structure we developed an architecture that allows security, trust and privacy to be assured throughout the entire data management process.

The remainder of this paper is organized as follows. Section 2 outlines work related to user data management and associated challenges. Further, section 3 describes the proposed generic human profile concept, its taxonomy, and discusses the technologies involved. Based on the previous principles, section 4 presents the proposed architecture and explains how the system works. Section 5 introduces the implementation work as well as its evaluation. The last section concludes the paper by outlining future work.

2. The Challenges of User Profile Management

Current service creation trends in telecommunications and web worlds are showing the convergence towards a Future Internet of user-centric services. In fact, some works [3] already provide user-oriented creation/execution environments, but these are usually tied to specific scopes and still lack on the capability to adapt to the heterogeneity of devices, technologies and the specificity of each individual user. Based on these limitations, the research in [4] identifies flexibility as the foundation for users' satisfaction, where the demand for different types of awareness needs to be present across the entire value of chain of a service. Despite most initiatives require or propose some sorts of user profile management systems; these are usually proprietary and include limited information about user preferences and contexts. Therefore, in order to make use of user information for a range of services and devices, there is a need for standardization of user related data and the architecture that enables their interoperability. These efforts have been seen at both fixed and mobile worlds and are usually taken under the European Telecommunications Standards Institute (ETSI), the Third Generation Partnership Project (3GPP), Open Mobile Alliance (OMA), among others.

Considering data requirements from a wide range of facilities and from different standardization organizations is the concept of Common Profile Storage (CPS) defined by 3GPP in [5], a framework for streamlining service-independent user data and storing it under a single logical structure in order to avoid duplications and data inconsistency. Being a logically centralized data storage, it can be mapped to physically distributed configurations and should allow data to be accessed in a standard format. Indeed, several approaches have been proposed to guarantee a certain interoperability degree and can be grouped into three main classes: syntactic, semantic and modeling approaches. The work in [6] proposes a combination of them to enable interoperability of user profile data management for a Future Internet. However, standardization, interoperability, flexibility and management are not the only challenges.

To improve the degree of services personalization it is important to generate new information from the existing one. In this sense, user modeling and reality mining techniques can be empowered to study patterns and predict future behaviors. Using these techniques, the work in [7] models users profiles into short-term and long-term interest. For that reason, user profiles should be capable of storing not only fixed parameters but also variable data structures. Furthermore, as the research initiative in [8] shows, privacy, security and trust are major topics that deserve a special focus in what concerns user profile and identity management. Moreover, there are other non-technical challenges related to a diversity of distinct regulations and high-level interests that sometimes are higher than the desired harmonization and user satisfaction.

3. Generic Human Profile

3.1. The Concept

The Generic Human Profile (GHP) represents a set of properties built within a generic structure that allows the services of the future to use user related information, while respecting their privacy, needs and concerns. Opening the door for opportunistic communications, user context is disclosed according to contextual privacy policies and settings, enabling systems and devices to sense how, where and why information and content are being accessed and respond accordingly. In addition, by using semantic, ontology and keyword technologies that understand the meaning of information and facilitate the accessibility and interconnection of content, it is possible to generate/infer new types of knowledge that can relate to users' behaviors, needs or intentions.

Nevertheless, despite the utility of such profiling algorithms, the user should be in control during the entire process. People will wish to manage their identities in different ways, sometimes opting for full disclosure, at other times disclosing only in an anonymous way that preserves their privacy. This is essential for establishing and managing trust and for safeguarding privacy, as well as for designing and implementing business security models and policies. By storing users external contexts, it will be possible to compare different sorts of data, so far not correlated improving on the one hand the algorithms, but on the other hand the user overall satisfaction as services become more contextualized, adapted and consequently personalized. Moreover, GHP envisages the integration of social data from different platforms, providing a unified way to access users' (Humans) friends' lists, among others, combining both online and offline social networks data. In the end, a crucial step will be the Profile Description Framework (PDF) to handle the transformation of a technical profile into a tradable and interoperable good. In this sense we believe that PDF will be at the heart of the GHP and the Future Internet.

3.2. Requirements and Technological Considerations

When thinking about the implications towards a Future Internet, user related data raise a series of questions. In what concerns security, we will need multi-factor authentication and authorization mechanisms that can be achieved by combining context-aware policy admission points with identity providers, providing an open and standardized data management service.

As for data storage and distribution, it is very likely to see trusted cloud service providers (probably telcos) embracing this opportunity, where all attribute data related to users in a specific context can be easily accessed and aggregated. Although a distributed but interconnected standardized logic to access this data is required, its physical storage can be done within walled garden domains. In this sense, it is expected that context itself will have a signaling protocol and a complementary distribution one. Depending on the evolution of mobile devices, there is also the possibility to assist to a shift where some of the users associated data is stored locally. In fact, a first step towards the combination of the previously enunciated mechanisms (local vs. remote storage) is being explored by the newly launched Vodafone 360 service.

Regarding the business aspect, it is necessary that the solution is flexible enough to allow different entities to be involved in the value chain and therefore contribute to overall service offering. Furthermore, scalability and performance will be crucial for the roll out of such initiative. Billing and revenue distribution are also topics that need to be addressed, otherwise, when ignoring them, the overall solution may become compromised.

3.3. Generic Human Profile Taxonomy

For our purposes, besides user's personal data, the system was also capable of collecting their affiliations as well as their friends. Figure 1 presents the taxonomy of the aforementioned user profile. As depicted, users have the possibility to control who views, distributes or modifies their information, what type of data is accessible and under which circumstances this occurs, including the possibility to control the way the profiling (reasoning and prediction) algorithms work. In addition, the GHP is capable of storing information from different social networks, where the information stored can vary from one community to the other. It is also possible to acquire external contexts that can be very helpful for new knowledge generation. Moreover, by aggregating data regarding user devices and their properties, it will enable services to easily adapt themselves to end terminals.

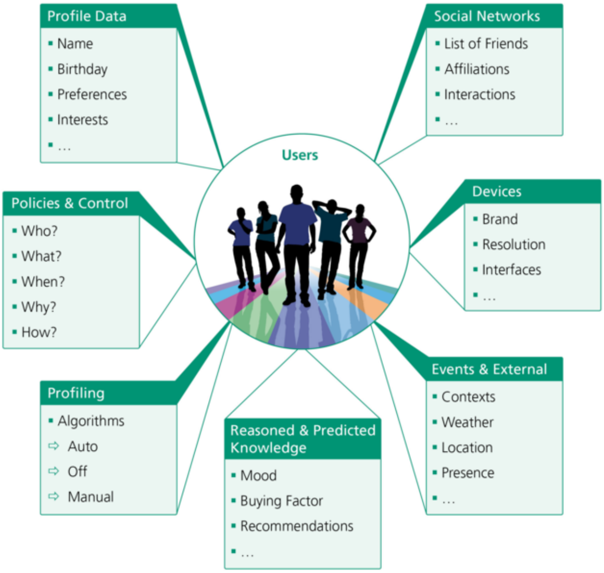


Figure 1. Generic Human Profile Taxonomy.

4. Architectural Approach

In order to realize the vision previously described it is necessary to transpose the Generic Human Profile concept into an manageable format. In this sense, this section presents the architecture, the components needed, as well as some some use cases, exemplifying how the system works.

4.1. General Overview

With the goal of achieving an efficient and secure way of managing user related data, our main concerns were:

- Advanced data management - allow the functions of data creation, modification, deletion, storage, acquisition, subscription, notification and syndication in a secure and efficient way.
- Authentication - act of confirming that someone is authentic and that the claims made by or about the subject are true.
- Authorization - function of specifying access rights to resources, according to a set of access policies.

To accomplish these objectives and to be compliant with the requisites specified in section 3.2, the architecture is mainly supported by a single component, the Human Enabler, and its associated modules. Nevertheless, other entities may be added to tailor extra functionalities. Figure 2 represents the disposition of the involved elements.

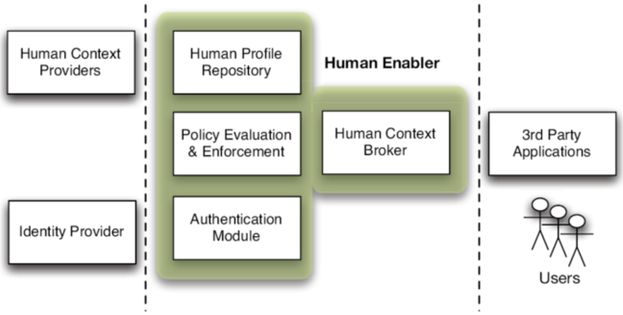


Figure 2. Overall Human data management architecture.

Before presenting how the system works, it is essential to understand which are the entities involved and what they do.

4.1.1. The Human Enabler

Acting as the main component of the entire architecture, the Human Enabler is composed by four distinct but complementary modules that are logically tight together, but can be physically separated (as long as basic security mechanisms are assured). They are:

Human Context Broker. Responsible for managing and processing all requests coming from the outside. Its interfaces allow direct access to recently cached information (context has always an expiration date) or an API for historical data. For the case of real-time context, it can be requested or subscribed. If the last occurs, when context changes, a notification is sent to the previously subscribed entity. Furthermore, it allows information to be updated, created or deleted using a specific ContextML format [9].

Human Profile Repository. Where all the users related information is stored (both real-time and historical). Basically it represents the physical implementation of the Generic Human Profile specified in section 3.

Policy Evaluation & Enforcement. This component implements an interceptor that may be applied on all critical interfaces and act as an intermediate system between the resource requestor and target resource. It intercepts both the request and the response. Based on the evaluation results, this entity decides to forward the message to the destination or send a deny message to the message originator. The Policy Evaluation Engine's main activity is the evaluation of policy conditions and execution of associated actions. In order to perform this activity, it has to first identify and return relevant policies from the policy repository based on the input data. The Policy Enforcement Engine of which the evaluation process is part of, builds an enforcement decision based on the results of the evaluation process execution and of the processes that imply invocation of other resource capabilities (request delegation) that are stipulated into evaluated policies.

Authentication Module. Responsible for authenticating all requests coming from third-party applications or on behalf of other users. It interacts with the Identity Provider to confirm the authenticity and integrity of the requests intercepted by the policy interceptor.

4.1.2. Identity Provider

An identity provider will allow users and 3rd party applications to come to a commonly agreed level of authentication for users and shall be able to produce the necessary formatting of authentication and authorization tokens. Even though self-asserted identity attributes will still be very prevalent in the GHP, there are also scenarios possible where the workflows will require token assertions of trusted attribute from identity providers. For an easy management of the roles or personas of users in this context, an identity provider will play the central role in such a user-centric setup. The identity providers in that sense can offer a secured life-cycle management of digital identities for users.

4.1.3. Human Context Providers

Entities capable of obtaining basic or reasoned contexts from sensors, networks, devices, social networks or other data sources. Moreover, they provide and deliver this information in an interpretable manner, making it available to other components. They can act as standalone applications or publish their information into the Human Enabler through specific control mechanisms [9].

4.1.4. Third Party Applications and Users

Represent the entities responsible for requesting Human related information. A third-party application can make requests on behalf of particular users or by itself (considered as well as a user in the system).

4.2. How the System Works

Assuming that the main functionality of such architecture is to request user related data, we will use this use case to demonstrate how the different components/modules communicate between themselves. Figures 3 and 4 illustrate these interactions.

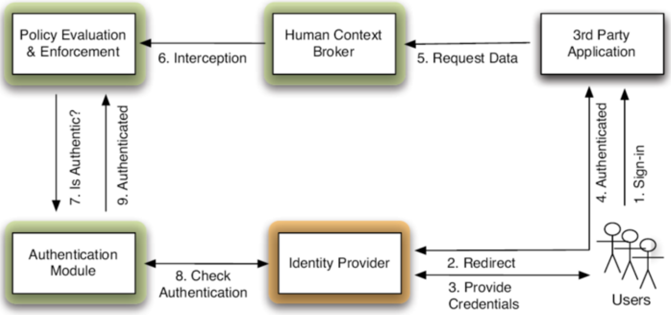


Figure 3. Authentication procedure for user related data requests or subscriptions.

In the future it is expected that most applications have some Internet based dependency. In this sense, all user requests must be somehow authenticated (1). In our particular scenario, the user is given the option to choose his favorite Identity Provider (IdP). When he does this, his request is redirected accordingly (2). Afterwards the user will authenticate according to the desired level of permission of the 3rd party application (3-4). The offered authentication methods can vary according to each IdP's capabilities of validating user identities. While offering tailored service towards users, applications might require extended user related information (e.g., list of friends, location, weather, preferences, recommendations). Within the proposed solution, all requests are sent (5) to the Human Context Broker (HCB). Prior to being processed, these are intercepted (6) by the Policy Evaluation & Enforcement module (PEEM). Before checking or enforcing any type of policy, the component forwards the request (7) towards the internal Authentication module so that the assertions provided by the third party application can be cross checked (8). Once this is done, the PEEM is informed (9) and continues its operations.

After the request is duly authenticated and authorized, the PEEM requests the desired context information (10). Then, the information contained inside the response is initially evaluated towards the provider/operator policies (stored inside the PEEM) and then cross checks against user self defined policies (the ones owning the context). Depending on the implementation, this information may be located inside the Human Profile Repository (HPR). In this situation, these policies need to be fetched (11) so that the response can be verified and correctly authorized. The main reason why requests are not evaluated right upon a request is sent to the HPR is related to the fact that in some cases, the policies are temporally or spacially dependent and therefore they can only be evaluated when the response/trigger occurs (this applies particularly for subscribed information). After being evaluated, the response is enforced towards the HCB (12), which is in charge of forwarding the message towards the third party application (13). Using the requested context data together with the remaining application logic, the user is targeted with a personalized and adapted service experience (14).

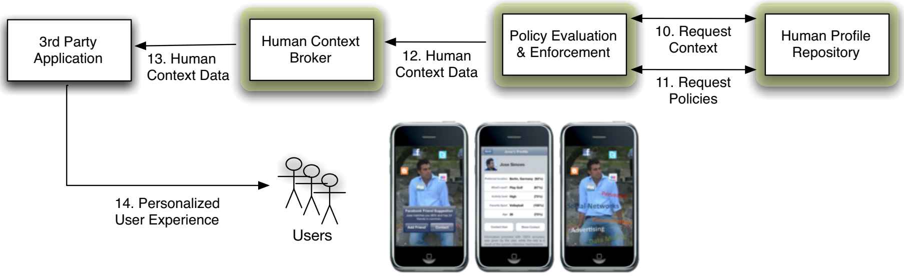


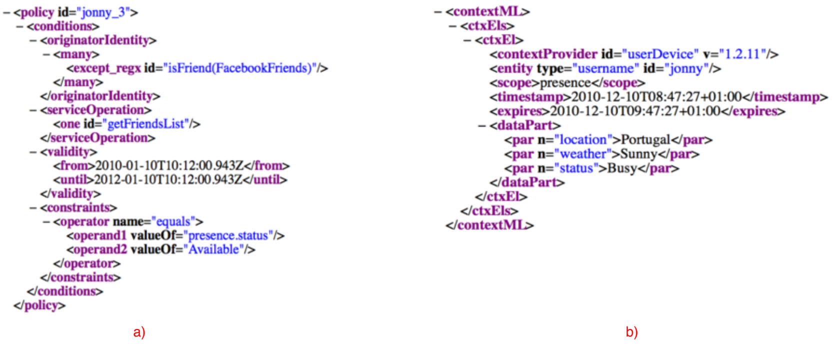
Figure 4. Authorization procedure for user related data requests or subscriptions.

Although not depicted, the Human Context Providers are usually the entities that trigger system responses (when some context is updated) and consequently the authorization process. Based on the aforestated principles, it is up to the application (entity requesting context) to adapt delivery and customization accordingly. Within the C-CAST project we used several components distributed across session, network and transport layers aiming to improve the balance between efficiency and personalization for multiparty multimedia delivery in group communications [10]. Such implementation based on the presented architecture allowed the improvement of real-time Quality of Service (QoS) management, consequently increasing the user overall perceived QoE.

5. Implementation and Evaluation

With the purpose of evaluating the proposed system architecture, we developed a testbed environment involving the aforementioned components. The PEEM was represented by the FOKUS XPOSER [11], [12], an Open Mobile Alliance (OMA) compliant implementation for policy evaluation and enforcement. As an Identity Management Provider we used FOKUS Generic Unified IDentity Enabler (GUIDE) [13], which supports multiple state-of-the-art identity management technologies, such as the Security Assertion Markup Language (SAML) 2.0 [14] and OpenID 2.0. Both the HPR and the HCB were implemented as an extended version of the UASO Context Broker [15], whose scopes (contain the description of a specific type of context) were extended to integrate a simplified version of the GHP taxonomy introduced in Figure 1. The Context Providers (CxP) used within the tests were developed under the C-CAST European Project [16] and involve, Device CxP, Weather CxP, Location CxP, Social Networks CxP, among others. It is important to notice that in our testbed we assume that a trust relationship exists between all the components inside the Human Enabler, otherwise, extra security mechanisms should be enforced. Finally, we developed an augmented reality application to explore the potential of the presented architecture.

What if there was a way for users to simply point their mobiles at people and automatically know more about them? By using the phone location, compass APIs and the context information about other users (accessible through the Human Enabler), it is possible to emerge in a new way of interacting with people. To show how this translates into context and policies stored within the Human Enabler, figure 5 gives a short example. On the other hand, figure 6 provides some examples of what could be possible to



```
- <policy id="jonny_3">
  - <conditions>
    - <originatorIdentity>
      - <many>
          <except_regx id="isFriend(FacebookFriends)"/>
        </many>
      </originatorIdentity>
    - <serviceOperation>
        <one id="getFriendsList"/>
      </serviceOperation>
    - <validity>
        <from>2010-01-10T10:12:00.943Z</from>
        <until>2012-01-10T10:12:00.943Z</until>
      </validity>
    - <constraints>
      - <operator name="equals">
          <operand1 valueOf="presence.status"/>
          <operand2 valueOf="Available"/>
        </operator>
      </constraints>
    </conditions>
  </policy>
```

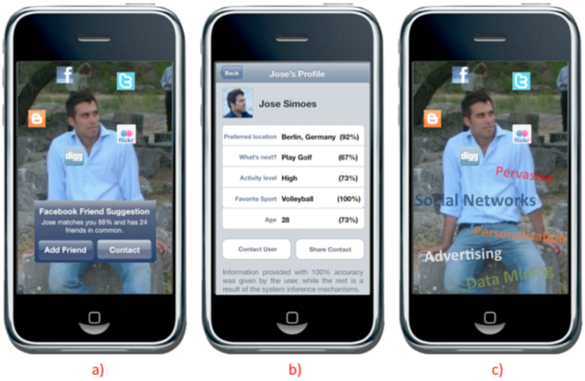
a)

```
- <contextML>
  - <ctxEls>
    - <ctxEl>
        <contextProvider id="userDevice" v="1.2.11"/>
        <entity type="username" id="jonny"/>
        <scope>presence</scope>
        <timestamp>2010-12-10T08:47:27+01:00</timestamp>
        <expires>2010-12-10T09:47:27+01:00</expires>
      - <dataPart>
          <par n="location">Portugal</par>
          <par n="weather">Sunny</par>
          <par n="status">Busy</par>
        </dataPart>
      </ctxEl>
    </ctxEls>
  </contextML>
```

b)

Figure 5. a) Policy example b) Piece of user ’Jonny’ context data.

achieve. In scenario a), the user wants to know more about the publicly available information regarding the Facebook profile of the person currently being tracked, while b) on the other hand provides basic profile information that the person in the picture decided to share at that precise moment within that context, improved with the system inferred information. Case c) presents a summary of keywords that better define a person’s profile within the Digg community (this could give a quick overview of someone’s interests). In this sense, we can see that the services presented can be provided directly by the Human Data Repository (exposed by the Human Enabler) but at the same time, be a combination of previously reasoned information (can be provided by other applications) with specific application data itself.



Facebook Friend Suggestion
Jose matches you 88% and has 24 friends in common.

Jose's Profile

Jose Simoes

Preferred location	Berlin, Germany	(92%)
What's next?	Play Golf	(67%)
Activity level	High	(73%)
Favorite Sport	Volleyball	(100%)
Age	28	(73%)

Information provided with 100% accuracy was given by the user, while the rest is a result of the system inference mechanisms.

Figure 6. Example of a Human Social application: a) Facebook option, b) Personal Profile option, c) Digg option.

As mentioned earlier, all the information disclosed by the user is dynamically managed by himself (through the policies) and can be updated in real-time (using the Human Enabler). Depending on the time of the day or event the user is attending, he can decide which information can be retrieved by the system. Such applications will also help to promote collaboration and enrichment of existing content, as they can provide the interfaces to interact with it and consequently the user himself. Again, such personalized, contextualized, interactive, mobile and adapted experiences will allow users to engage with next generation services as these will respect their privacy but at the same time address their needs, concerns and desires. For third party applications the benefits are even more evident, as technology will allow them to better understand their customers and therefore tailor their solutions accordingly.

6. Conclusions and Future Work

Merging digital and physical worlds will create unprecedented ubiquitous user interfaces enabling a set of seamless rewarding user experiences. In our work, by extending regular user profile data (user preferences) to accommodate social, context, device and policy related information, we open the path to a new era of services where these can become user behavior aware, paving the way to understand their needs, desires and intents. Together with other security considerations (authentication, privacy and trust) this work may have considerable social and economical impact in the Internet of the Future. In a way, it will improve users perceived Quality of Experience by changing the way they see, use, consume and interact with content and services in any futuristic scenario.

References

[1] J. Hourcade et al., Future Internet 2020: Visions of an Industry Expert Group, European Commission Information Society and Media, Apr. 2009.

[2] M. Hassenzahl, N. Tractinsky, User experience - a research agenda, Behavior & Information Technology, Vol. 25, No. 2, pp. 91-97, April 2006.

[3] C. Baladron et al., User-Centric Future Internet and Telecommunication Services, Towards the Future Internet, IOS Press, 2009.

[4] F. Liberal et al., QoE and *-awareness in the Future Internet, Towards the Future Internet, IOS Press, 2009.

[5] G. Bartolomeo, T. Kovacikova, User Profile Management in Next Generation Networks, Proceedings of the 5th Advanced International Conference on Telecommunications, Venice, May 2009.

[6] 3GPP TR.32.808: 3rd Generation Partnership Project: Technical Specification Group Services and System Aspects; Telecommunication management; Study of Common Profile Storage (CPS) Framework for User Data for Network Services and Management (Release 8).

[7] C. Wei, C. Haung, H. Tan, A Personalized Model for Ontology-driven User Profiles Mining, Proceedings of the International Symposium on Intelligent Ubiquitous Computing and Education, May 2009.

[8] C. Sorge, J. Girao, A. Sarma, Privacy-enabled identity management in the Future Internet, Towards the Future Internet, IOS Press, 2009.

[9] Delverable 12 - Specification of context casting service enablers, context management and context brokering, C-CAST Project (ICT-2007-216462), http://www.ict-ccast.eu/deliverables.php 2009

[10] S. Sargento et al., Context-Aware Multiparty Services Delivery: Evaluation and Experimentation, Future Network Mobile Summit 2010, Florence (Accepted for Publication)

[11] XPOSER - an eXtended POlicy-based, Semantically enabled sErvice bRoker, www.open-soa.de/xposer/

[12] N. Blum et al., A Service Broker providing Real-time Telecommunications Services for 3rd Party Services, 33rd Annual IEEE International Computer Software and Applications Conference, 2009

[13] A FOKUS Generic Unified IDentity Enabler - www.id.open-ims.org

[14] J. Hughes, E. Maler, Security Assertion Markup Language 3 (SAML) 2.0 Technical Overview, http://saml.xml.org/, 2005.

[15] M. Knappmeyer, N. Baker, S. Liaquat, R. Tonjes, A Context Provisioning Framework to Support Pervasive & Ubiquitous Applications, 4th European Conference on Smart Sensing and Context, 2009.

[16] Context to Content Casting - European 7th Framework C-CAST Project (ICT-2007-216462) - Provide an End-to-End Context-Aware Communication Framework, http://www.ict-ccast.eu/