

Personalization and User Profile Management

G. Bartolomeo¹, F. Petersen² and M. Pluke³

¹ University of Rome Tor Vergata, Rome, Italy

² Apica, Biot, France

³ Caste Consulting LTD, Ipswich, UK

Abstract—Personalization and effective user profile management will be critical to meet the individual users' needs and for achieving e-Inclusion and e-Accessibility. This paper outlines means to achieve the goal of the new ICT era where services and devices can be personalized by the users in order to meet their needs and preferences, in various situations. Behind every instance of personalization is a profile that stores the user preferences, context of use and other information that can be used to deliver a user experience tailored to their individual needs and preferences. Next Generation Networks (NGN) and the convergence between telephony and Internet services offer a wide range of new terminal and service definition possibilities, and a much wider range of application in society. This paper describes the personalization and profile management activities at European Telecommunications Standards Institute (ETSI) Technical Committee Human Factors, together with relevant experimentations in recent European research projects.

Index Terms—NGN, Personalization, Profile Management.

I. INTRODUCTION

A. What is a Profile?

The concept of a profile usually refers to a set of preferences, information, rules and settings that are used by a product or service to deliver customized capabilities to the user. In practice, many products and services already contain profiles that are specific to that product and unrelated to any other. Commercial and technical constraints will dictate that having profile components associated, and co-located, with each product or service is likely to remain a common model for profiles. This model is reflected in proposed system architectures such as the 3GPP (3rd Generation Partnership Project) GUP (Generic User Profile) [1]-[3]. There will be a number of user characteristics and preferences that will apply independently of any particular product or service (e.g. preferred language or need for enlarged text). Users frequently find themselves moving from one situation to another throughout a typical day (e.g. at home, driving, working). In each of these situations, users will have different needs. At present, an increasing number of products already provide the user with ways of tailoring their preferences to these situations.

ETSI EG 202 325 [6] describes the personalization and profile concept and presents guidelines to manufacturers and service providers in shaping their product and service requirements in ways to maximize human and social benefit. This work identifies how to make it easy for users to specify their situation dependent needs in ways that

require the minimum need to understand the potentially wide range of such products. In order to achieve the best user experience, there is a need to ensure inter-operability of services, devices and the users' preferences defined in their profiles.

B. The Work of ETSI Human Factors

The ETSI Technical Committee Human Factors work (Specialist Task Force STF342), funded by EC/EFTA (European Commission/European Free Trade Association) [10] under e-Inclusion, is standardizing a User Profile Management architecture together with profile object specifications aiming at simplifying interoperability between different products. The outcomes of this ETSI Human Factors project will highly benefit the personalization of services and devices. From the users' point of view, relevant benefits will include:

- Personalized services and devices will provide a better user experience.
- Allowing reuse of users' existing knowledge will help them to manage new terminal devices and services, thus leading to faster and easier uptake of new technologies.
- Synchronization and harmonization of profiles across services and devices allow much faster and easier use of services and devices.
- A profile, that suits a specific situation and that handles many areas, will only need to be defined once. The end-users will not have to re-enter their preferences each time they acquire new services and devices.
- Enhancement of emergency telecommunications, in which the user might allow emergency services to have access to useful information in their profile that would help them to provide appropriate aid to that user.

To manufacturers and service providers, these profiles will be critical to the uptake and success of new and advanced communication services, especially among the larger market of non-technically astute, or non-technically inclined. Development costs and time to volume markets will be decreased. In addition, larger user segments will be reached more easily, thereby ensuring quicker uptakes of key technologies.

II. PAST AND ONGOING ACTIVITIES IN ETSI

A. Concept and Guidelines by ETSI

ETSI, with funding from the EC/EFTA, has described the concept and developed guidelines [6] relevant to the

users and their need to manage their profiles for personalization of services and terminals.

For a single product or service it may be difficult for a user to manage all of the information needed in their profile. Typically, users' interactions with profiles include checking, adding to, modifying or deleting information in their profile, being notified whenever entities access their profile, and understanding or controlling how their profile affects the service or capabilities that they experience.

B. Standardization of Profile Objects

Currently, the range of parameters that can be set by users and the values that may be set will not be consistent between different devices or services, or even between comparable services and devices from different vendors. Where such diversity exists, it makes it impossible to transfer the settings that have been set for one device or service to another similar device or service in a way that ensures that the same outcome will be achieved.

However, this problem can be resolved if different devices or services of the same type had consistent sets of parameters having value ranges producing identical effects. For terms like "very loud" or "large text" to be useful, they should always result in the same standardized user experiences. For this to be achieved, these terms need to map to technical descriptions that have universal applicability across a wide range of usage scenarios and device connections. In a more advanced scenario, settings in one proprietary form might be automatically converted to settings in another form on a similar device or service from a different supplier. Indeed, users will benefit greatly where mechanisms exist to automatically set many device and service specific and proprietary settings to values based upon information and preferences stored in their profiles.

The realisation of this objective depends on standardization of profile objects and the ways in which these are expressed. In order to define a broad set of objects, The ETSI Technical Committee (TC) Human Factors (HF) project collects input from end-users and their representatives, including people with disabilities. As well, the project is cooperating with relevant projects such as the IST-Simple Mobile Services [14] project, targeting mobile user's needs, as described in section IV.

C. Architecture

The ongoing ETSI Human Factors project is developing an architectural framework for achieving the personalization and profile management concept described in [6]. This project describes both network and terminal issues, as some of the functionality could be implemented in the network and some in the terminals and SmartCards. New generations of SmartCards like (U)SIMs hold an increasing amount of profile data as well as processing capability, which makes them useful for implementation of the profile concept. In principle, other means such as USB sticks and RFID (Radio-Frequency Identification) can be useful as well to store either profiles or "pointers" to profile data distributed across the Network. In order for a profile to be effective, the following architectural capabilities have been identified:

- Store and retrieve the profile data. It is likely that there will be multiple profile storage locations. These locations will probably not store the total profile but

only components that apply to a device or service, in addition, various locations may have different persistence and priority levels. A "Profile Storage Agent" is the entity that stores information about the profile data and the locations of data repositories of profile data related to users. Users require the data to be stored in a secure manner with user agreed levels of privacy applied to the availability and distribution of that data. Ideally, profile data should always be available, over all networks, from all supported devices and services, including fixed and mobile services allowing service continuity and optimal user experience. Changes of data at different locations should be consistent, which may be ensured by synchronization of data and transaction security. However, although the user's profile data is distributed amongst devices and services, it should be possible to ensure that users maintain the concept of centralized profiles which cover all of their devices and services.

- Process the profile data and initiate achievement of the behaviour encoded in the profile rules. In order that the rules in a profile can be translated into the behaviour the user desires, it is necessary for the profile processing agent to operate upon the rules. A "Profile Processing Agent" is responsible for ensuring that all the operations required by the profile rules are carried out and it will need to initiate operations on a variety of devices and services referred to in the profile. For efficiency and effectiveness it is likely that the Processing Agent will have its functionality distributed between multiple devices and services.
- Activate and de-activate variants of the profile in the appropriate circumstances. Users continuously move from one situation to another throughout the day (e.g. at home, driving, working) as depicted in Fig. 1. In each of these situations, users might have different needs for how they would like their ICT resources arranged. They should be able to specify their context dependent needs in ways that require the minimum knowledge of specific products. This is possible through a "Profile Activation Agent", responsible for the activation and de-activation of variants of the profile, whenever needed. The activation or deactivation may be rule driven, as a result of a user request or as a result of an event (for example, whenever a device is turned on).

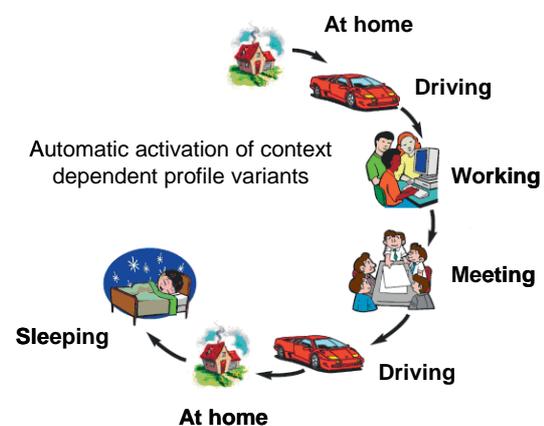


Figure 1. Some situations which might require change of user profile variants

In order to map the aforementioned capability into technologies, this project will evaluate latest network and device standards. Some of them have been implemented and experimented with by recent European research projects as described in section III and section IV.

III. THE USER PROFILE CONCEPT IMPLEMENTED IN EUROPEAN RESEARCH PROJECTS

The Open Platform for User-centric service Creation and Execution project (OPUCE) [13] has developed a system called User Information Management that treats in a uniform way profile, identity and context information through different subsystems mainly based on open source and standards. Developed as part of OPUCE, the open source implementation [21] of Open Mobile Alliance (OMA) XML Document Management (XDM) [18] is used to store and retrieve profile data from different XML repositories. In addition, OPUCE has also developed profile schemas extending the ones already specified by OMA XDM profile schema, [20].

The End to End Reconfigurability-II project (E2R-II) [12] has investigated the use of OMA Devices Management (DM) [18] to handle profile information coming from mobile terminals. "Device Management" refers to the remote management of the device settings from the point of view of the various "Management Authorities", including manufacturers, operators and service providers. In the context of 3GPP GUP, DM technology has been chosen as a possible implementation of GUP "Repository Access Function" inside the end user equipment, as DM allows remote managing of device configuration in an efficient way, especially optimized for wireless and cellular connections. During the project lifecycle, E2R-II also developed four DM "Management Objects" covering user, network, terminal and service profile information; these objects have been registered in the Open Mobile Naming Authority (OMNA) [5].

The Simplicity project [15] has widely investigated the use of a physical plug-in device called "Simplicity Device" (SD), enabling users to store their preferences in order to make it easier to personalize services and devices. The SD can be seen as an abstraction of a key for the user toward the ICT world; prototypes have been implemented using different technologies such as smart-cards, USB devices, mobile phones with short range connectivity like Bluetooth or Near Field Communication (NFC), each of them having different processing capability and storage size. In terms of security, the SD has been designed as a combination coupling simple end user authentication (e.g. using a PIN code) with the proof of possession of a physical token able to mutually authenticate with the network. It is worth noting that this mechanism is similar to the one currently used in GSM systems; however, the novelty consists in its exploitation for accessing a number of different services in addition to simple phone calls or messaging, reusing the same network infrastructure; this is in line with recent works from 3GPP on Generic Authentication Architecture and Generic Bootstrap Architecture [3].

A relevant aspect in User Profile Management is privacy. The DISCREET project [11] has developed a number of techniques helping end-users to take care of their privacy in a simple way. Particularly relevant to the subject of this paper, the project has developed a "pseudonymization"

algorithm by which users, assisted by one or more of "identity providers", can use telecommunications and Internet services without necessarily disclosing their real identity, whilst still allowing legitimate entities (e.g. legal authorities) to identify users whenever their behaviour is not compliant with laws.

IV. ETSI HUMAN FACTORS AND IST-SMS TRIAL

Collecting relevant results from the Simplicity and DISCREET projects, and in close cooperation with ETSI Human Factors, the Simple Mobile Services (SMS) project [14] will start a trial in Autumn 2008. The trial will take place in the campus area of the University of Rome "Tor Vergata" and will provide communications and Internet services to a wide community of mobile phone users of different age and gender, exploiting several concepts related to profile and identity management. This trial will see the University of Rome "Tor Vergata" acting as a profile provider – thus following creation, storage, processing and maintenance of different profiles – for a meaningful number of users (about 100 students plus a number of people including teachers, researchers and administrative people).

A. Provided Software

Trial participants will be provided with a software application to install on their mobile phones, Fig. 2. This software, called MOVE (Mobile Open & Very Easy), allows users to access different "data-centric" services, mostly built on the user-friendly concept of Mobile Electronic Memos (MEMs).

MEMs are electronic notes inspired by emerging data formats like Microformats [16] and Google Data API [9]. Each MEM contains an extensible, structured set of attributes associated with a specific class of information and can be used by humans and applications to exchange information related to a person, a service, the status of an ongoing activity, etc. MEMs could be considered as a first prototype implementation of "Profile Objects" and allow the amount of information to be entered manually by users when interacting with services to be drastically reduced, a key feature for mobile services.



Figure 2. MOVE, the application software provided to SMS trial participants

In order to drive different kinds of communications (phone calls, emails, instant messaging) among trial participants, according to user defined policy rules, the provided application software uses a unique user identifier in form of a SIP address mostly compliant with the UCI concept [7].

B. Smart Card Web Server and SIM Based Services

In addition, trial participants will be provided with a special SIM card able to store sensitive profile data, identity information and digital certificates. The interface toward this special SIM card will be based on an implementation of OMA Smart Card Web Server [17] which allows information stored in the card be accessed from the user equipment using https connections (Fig. 3).

This new interface provides a communication channel between terminal and smart card which is logically separated from those already existing today. It enables applications in the terminal to communicate with the SIM independently from the current telecom-based communication between these two entities. The widely deployed and well known HTTP protocol enables especially non smart card developers to easily set up a communication from other entities to smart card based services.

In particular, two kinds of Smart Card Web Server (SCWS) services will be exploited for the trial: secure storage and management of profile data and digital signature.

Especially private information about the user and secret keys and passwords will be stored on the SIM card to assure the required security and privacy. A management application on the SIM decides about granted access or protection. In order to hold user information or customized session data related to services, the implementation of the SCWS provided for the trial allows data to be stored as key/value pairs. For avoiding overlapping, keys may be qualified using a namespace indicator. These data entries (similar to browser cookies), can be created, updated or shared between services. Depending on the sensitivity of the data, specific security conditions must be fulfilled (e.g. entering a PIN). Some examples of use cases include:

- After entering a protection PIN, the user is able to view her profile on the phone, and to eventually update it
- Personal settings like bookmarks/favourites or themes could be stored so that they are always available to the user even if the mobile device is changed
- Third party services could request user data to pre-enter it in forms for user's convenience (automatic form-filling)
- Third party services could request user's passwords as a single-sign-on login

Sometimes, during transactions, the identity of the originator must be proven or data consistency has to be verified. To solve this problem, a digital signatures service is made available on the trial's SIM. The SIM contains a generated public/private key pair for the owner and the

SCWS provides an interface so that third party application can request data to be digitally signed by the SIM.

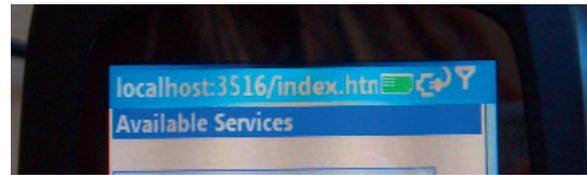


Figure 3. Smart Card Web Server Gateway on a real phone

C. Context Management

Possible trial goals also include evaluation of mechanisms for automatic activation, deactivation and processing of profile variants; as described in section III.C, this will be mostly done in a seamless way, requiring knowledge of context information. The following categories of context are considered: presence, location, time, interaction with physical objects in users' proximity and other kinds of real world context information (e.g. meteorological conditions). In SMS, context information is distributed across a set of nodes, which include both network nodes and end-user equipments. In each node there is a corresponding "Context Peer" which is in charge of performing operations related to its own managed context data. A hierarchical addressing mechanism has been implemented so that all available context information is identified by a corresponding "key". Context information can be transmitted from node to node and the context framework makes it possible to subscribe to a specific context information change so that whenever context information is altered on a remote node a notification is received by the subscribed Context Peer.

At the time of writing, SMS is evaluating the possibility of extending this work in order to include solutions for linking, synchronizing, accessing and translating data expressed in different formats compliant with the eXtensible Resource Identifier Data Interchange format as defined by OASIS [4].

V. CONCLUSIONS

Personalization will be critical to the uptake and success of new and advanced communication services. Profiles promise to ease the conflict between the benefits of common technology deployments versus diverse social and cultural demands, and variations in individual physical and cognitive abilities and preferences. In order to achieve this goal, ETSI is standardizing an architecture and objects for profiles.

ACKNOWLEDGMENT

We thank the members of ETSI Human Factors and other companies and individuals who provide us with useful input and comments to our work.

REFERENCES

- The links hereafter reported have been last accessed on July, 18 2008.
- [1] 3GPP TS 22.240: 2005, Technical Specification 3rd Generation Partnership Project; Technical Specification Group Services and System Aspects; Service requirement for the 3GPP Generic User Profile (GUP); Stage 1, 3GPP, Sophia-Antipolis.
 - [2] 3GPP TS 23.240: 2007-06, Technical Specification 3rd Generation Partnership Project; Technical Specification Group Services and System Aspects; 3GPP Generic User Profile - architecture; Stage 2, 3GPP, Sophia-Antipolis.
 - [3] 3GPP TS 33.220: 2007-12, Technical Specification 3rd Generation Partnership Project; Technical Specification Group Services and System Aspects; Generic Authentication Architecture (GAA); Generic bootstrapping architecture, 3GPP, Sophia-Antipolis.
 - [4] OASIS: Advancing Open Standard for the Information Society (OASIS), eXtensible Resource Identifier (XRI) Data Interchange format (XDI) Technical Committee, homepage <http://www.oasis-open.org/committees/xdi/>.
 - [5] E2R-II: Profile Management Objects, <http://e2r2.motlabs.com/dissemination/standardisation>
 - [6] ETSI EG 202 325: 2005, Human Factors (HF); User Profile Management, ETSI, Sophia-Antipolis.
 - [7] ETSI EG 284 004: 2007, Telecommunications and Internet converged Services and Protocols for Advanced Networking (TISPAN); Incorporating Universal Communications Identifier (UCI) support into the specification of Next Generation Networks (NGN), ETSI, Sophia Antipolis.
 - [8] ETSI Human Factors STF342, homepage http://portal.etsi.org/stfs/STF_HomePages/STF342/STF342.asp.
 - [9] Google: Google Data (gData) API, <http://code.google.com/apis/gdata/>.
 - [10] i2010: 2005 A European information society for growth and employment, EC, Brussels, http://ec.europa.eu/information_society/eeurope/i2010/index_en.htm.
 - [11] IST-DISCREET project, homepage: <http://www.ist-discreet.org/>.
 - [12] IST-End to End Reconfigurability-II project, homepage: <http://e2r2.motlabs.com/>.
 - [13] IST-Open Platform for User-centric service Creation and Execution (IST-OPUCE) project, homepage: <http://www.opuce.tid.es/>.
 - [14] IST-Simple Mobile Services (IST-SMS) project, homepage: www.ist-sms.org.
 - [15] IST-Simplicity project, homepage: <http://www.ist-simplicity.org/>.
 - [16] Microformats: <http://www.microformats.org/>.
 - [17] OMA SCWS: Open Mobile Alliance, Smart Card Web Server, specifications, http://www.openmobilealliance.org/release_program/SCWS_v10_C.html.
 - [18] OMA-AD-XDM 2006: Open Mobile Alliance, XML Document Management Architecture, Version 1.0, http://www.openmobilealliance.org/release_program/docs/XDM/V1_0_1-20061128-A/OMA-AD-XDM-V1_0-20060612-A.pdf.
 - [19] OMA XDM 2006: Open Mobile Alliance, XML Document Management, specifications, http://www.openmobilealliance.org/release_program/XDM_archive.html.
 - [20] OMA 2007: Open Mobile Alliance, XML Document Management, user profile schema, http://www.openmobilealliance.org/release_program/docs/XDM/V2_0-20070724-C/OMA-SUP-XSD_xdm_userprofile-V1_0-20070724-C.txt.
 - [21] The OpenXDM project, homepage: <https://openxdm.dev.java.net/>.
 - [22] TISPAN: Terms of Reference, http://portal.etsi.org/tispan/TISPAN_ToR.asp.

AUTHORS

G. Bartolomeo (giovanni.bartolomeo@uniroma2.it), ETSI STF 342 expert, is with the University of Rome "Tor Vergata", Rome, Italy. During past years, he has participated in several European projects (SIMPLICITY, E2R-II and SMS) addressing personalization, device reconfigurability and user profile management.

F. Petersen (francoise.petersen@apica.com), is working as an independent consultant. She is leading the ETSI Technical Bodies Human Factors HF and eHealth activities on Personalization and user profile management and is also working on "ICT in cars" within the ETSI Technical Committees Human Factors and Intelligent Transport Systems (ITS). She has been working during ten years at the Swedish telecom operator TeliaSonera. Prior to that, she gave courses in Computer Sciences at Lund University in Sweden.

M. Pluke (mike.pluke@castle-consult.com), is working as an independent user experience consultant. He is currently participating in ETSI work on Personalization and User Profile Management and is also leading ETSI work on "ICT in cars". He is also currently participating in the European Committee for Standardisation (CEN) Workshops on "Discovery of and Access to eGovernment Resources" and "Functional Multilingual Extensions to European Keyboard Layouts". He previously worked for the Human Factors division of British Telecom and led internal and external work on user interface standardization.

About ETSI: The European Telecommunications Standards Institute (ETSI) produces globally-applicable standards for Information and Communications Technologies (ICT), including fixed, mobile, radio, converged, broadcast and internet technologies and is officially recognized by the European Commission as a European Standards Organization. ETSI is a not-for-profit organization whose 700 ETSI member organizations benefit from direct participation and are drawn from 60 countries worldwide. For more information, please visit: www.etsi.org.

About ETSI STFs: Specialist Task Forces (STFs) are teams of highly-skilled experts working together over a pre-defined period to draft an ETSI standard under the technical guidance of an ETSI Technical Body and with the support of the ETSI Secretariat. The task of the STFs is to accelerate the standardization process in areas of strategic importance and in response to urgent market needs. For more information, please visit: <http://portal.etsi.org/stfs/process/home.asp>.

This work was supported by EC/EFTA (European Commission/European Free Trade Association) and by the European Union's Sixth Framework Programme for research and technological development (FP6).

This article was modified from a presentation at the 21st Symposium on Human Factors in Telecommunication (HFT 2008) in Kuala Lumpur, Malaysia, March 2008. Manuscript received 18 July 2008. Published as submitted by the authors.