Reconfigurable Systems with a User-Centric Focus

Giovanni Bartolomeo, Stefano Salsano, Nicola Blefari-Melazzi
*DIE, Università di Roma "Tor Vergata", {stefano.salsano, giovanni.bartolomeo,
blefari}@uniroma2.it*

Abstract

Today's reconfigurable radio systems have several interesting functionalities ranging from traditional reconfigurable systems operating at the physical layer only to fully fledged reconfigurability. Along this path we envisage a shift of perspective from a terminal-centric approach to a user-centric one. The main characteristics of this evolution are the provisioning of an unique user identity to be used over different RATs, and the increasing importance of profile information, needed to configure, customize and personalize terminal capabilities and. In this paper we i) examine a possible choice for a unique user identifier ii) propose a user profile and design a distributed approach to manage user profile information iii) introduce the "Dataweb" paradigm under standardization in the Oasis consortium and iv) show how it may be used to link all the expressed concepts.

1. Introduction

Reconfigurable systems will make it possible for a terminal to use a wide range of communications systems, ranging from cellular, wireless local area networks, wireless personal area networks, radio/tv broadcast networks, without duplication of hardware.

In the more advanced scenarios, the reconfiguration should be possible "on the fly" by downloading new SW modules on a wireless channel.

The E2R II project, co-founded by the European Union under the IST framework program, deals with the whole set of issues related to reconfigurable radio systems. Among these issues, E2R II is addressing the definition of a communication channel between terminals and base stations named "Cognitive Pilot Channel" (CPC), driving the reconfiguration process.

The CPC discovers which communication bearers are available, selects which SW module should be activated or even downloaded according to the user needs, performs authentication/authorization procedures and makes it possible to download the modules themselves. The CPC functionality is not limited to software radio reconfiguration of devices but it includes the higher layers functionality allowing a personalization of terminal and services alike. It may be implemented as a dedicated physical channel or it may be transmitted over one or more different Radio Access Technologies (RAT). A logical view of the CPC channel is given in Figure 1, where an entity called Access Network Controller (ANC) communicates with the terminal over the CPC, in a scenario comprising several RATs.
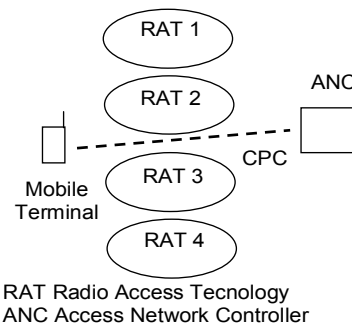

Figure 1: Logical view of the CPC channel

Dealing with different RATs, one fundamental point is the mechanism used to manage the user identity, different radio bearers using different addressing mechanisms. In addition, it is desirable to have an uniform solution which offers an easier interface to arrange profile information, managing user identity, access context infotmation.

In this paper, we i) examine a possible choice for a unique user identifier to be used over different RATs; ii) propose a user profile; iii) design a distributed approach to retrieve users profile information that does not require the mandatory presence of a public network operator; iv) introduce the "Dataweb" paradigm under standardization in the Oasis consortium and v) show how it may be used to link all the expressed concepts.

2. User identifier

If we want reconfigurable systems move from a terminal-centric approach to an user-centric approach, we need to univocally identify and address each user, across different RATs.

It is well known that IP addresses made a giant leap in

this regard; however we still have several different working ways to identify terminals/users: (i) IP addresses; (ii) IMSI/IMEI in UMTS/GPRS/GSM; (iii) Phone numbers in PSTN; (iv) MAC addresses, when not "shielded" by IP; (v) Bluetooth addresses; (vi) Application addresses (e-mail, suitable identifiers assigned by the providers).

These options are to be understood not as addressing schemes working at different OSI layers; the list is meant as possible alternatives to identify *end-users*, for reconfigurability purposes. From this point of view, there are existing proposals trying to provide a unique identifier to be used when on the move and over different RATs:

- IETF SIP, using the SIP "Address of record"
- IETF mobile IP using the "home" IP address of a terminal
- ITU-T E.164 (with a more limited scope), using telephone numbers
- 3GPP Generic Access Network architecture, which considers IMSI as Mobile Subscriber identity, even outside the context of a cellular access network

However, finding a comprehensive solution is not an easy task. Several issues need to be taken into account: unique identification of users, allocation of identifiers, resolution of identifiers, user privacy, interoperability with different networks, user preferences support ("profile"), context support (e.g., device availability,…).

The European Telecommunications Standard Institute, ETSI, proposed an "Universal Communication Identifier" (UCI): a single, unique user identifier, stable and immutable over time, used for all kinds of communication with a given user (phone/video call, messaging, emails, etc.). The UCI is specified in [2] and its main architectural elements are shown in Figure 2; these include the Personal User Agent (PUA) and the Service Agent (SA).

The UCI could be a very interesting solution for our needs. In addition, the current E2R-II system architecture can be used without adding further mechanisms to implement most of the functionality required by the PUA and the SA. The adoption of the UCI within the E2R framework could also bring benefits for the spreading of this standard proposal. Considering the binding of the E2R-II system architecture with existing standards, the implementation of the UCI framework through E2RII system elements could represent a bridge between the UCI proposal and a number of other existing standards (e.g., OMA DM, UMTS, ALL IP, etc.). Finally, we mention that we are developing a demonstrator of our proposed solution, showing identification of the user through different terminal devices, exploitation of user preferences (user profile), context awareness (e.g. which terminal device the user is using, etc.)
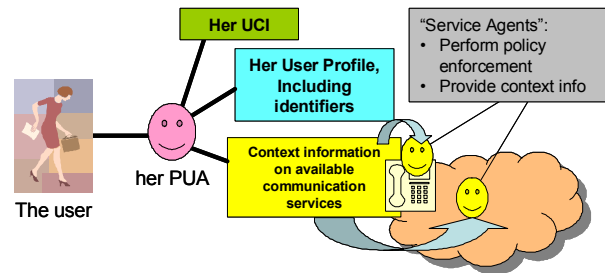

Figure 2: UCI's main architectural elements

3. Profile definition

The concept of user profile as understood in this paper has a very wide meaning. It is the repository of all the information related to the user, his devices, the services he uses, the networks and so on. It also includes information and data under the user control and information and data under control of the users' applications and services.

A complete solution for handling user profiles basically includes two different aspects. The first one is the definition of the profile schema. The second one is the definition of the architectural entities managing profile information and interactions among these entities.

An attempt to provide such a universal solution is the GUP (Generic User Profile) [3] defined by 3GPP, which has been developed taking into account the requirements of a future cellular network. The 3GPP GUP specification provides a data description mechanism and an architecture with interfaces and mechanisms to handle the data. Note that the GUP specification does not provide a concrete schema for a user profile, rather it provides a framework to define such a schema. Starting from the work carried out in 3GPP on the GUP, in the context of the Simplicity project [4], we have defined a concrete schema for a user profile, named Simplicity User Profile (SUP); The proposed SUP includes five components (Figure 3): user profile, device profile, network profile, service profile and PID (Personal Identification Device) profile, being the PID a device that can assist the user in presenting his identity and transferring his profile information to the networks, the terminal devices, the services. The most known example of PID is the Subscribe Identity Module (SIM), anyway other solutions (including java cards, memory cards or even mobile phones) are possible. The SUP is a "User Level" representation of the user himself and of his surrounding "information and communication technology" world. Suitable XML schemas have been defined in order to describe each component [5]. For each component we investigated existing proposals and standards and integrated them in our proposal whenever possible. A

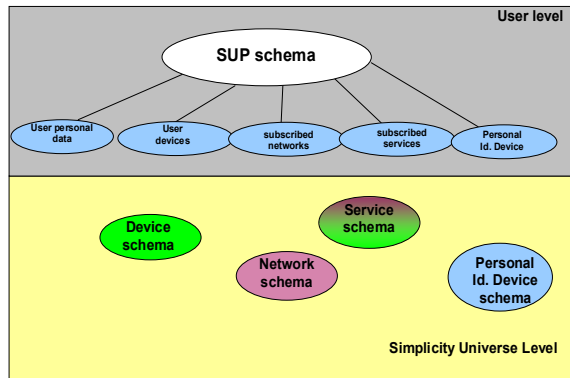description of the different profile component is provided in [10].

Figure 3: User Profile – Abstract view (xml schemas)

To conclude this section, we note that the limitation of this approach proposed by 3GPP (and adopted by Simplicity) is that it foresees a standardization agreement or the prevalence of a "de-facto" standard for the definition of a complete user profile schema.

4. OASIS' Dataweb, XRI and XDI

Oasis' "eXtensible Resource Identifier" (XRI) and "XRI data Interchange" (XDI) aim to define standard mechanisms is to allow any electronically represented data be shared independent of the application or domain from which they have been originated [6]. The novelty of XDI, compared to similar approaches (like the aforementioned 3GPP GUP), is that this technology, in order to solve the problem of interoperability between different data formats and between different domains, does not mandate a particular data format to conform with. Each organization ("authority" in XDI terminology) may still keep its own data format; the interoperability is guaranteed by two complementary mechanisms: first, data (and metadata or data "types") are bound to one or more resource unique identifier (XRI) [7], which is an extension of the current Internationalized Resource Identifier IRI defined in RFC3987 [8]. This solution allows to associate a semantics to the legacy data model, without relaying on ontology models like OWL [9]; second, XDI provides a distribute, secure and ubiquitous available mechanism for sharing data, very similar to what the Web actually does for presenting data to the navigators: the data-links. A data-link is similar to the well known hyperlinks; anyway it is intended to be used by software applications (instead of humans) for accessing data. Data-links introduces also access control mechanism, which is exactly what we need for our scenario. In the last

section, we will explain how it is possible to manage access control to profile data using XDI data-links.

5. Architectural aspects

The proposed architecture is shown in Figure 4 and described in details in [10]. The entities that manages profile information are called Profile Managers (PM). A PM is able to store and retrieve profile information on request of another entity which is generically denoted as Profile Requester Entities (PRE). PMs may reside both in the terminal (central Profile Manager, cPM) as well as in the network nodes (remote Profile Managers, cPMs).
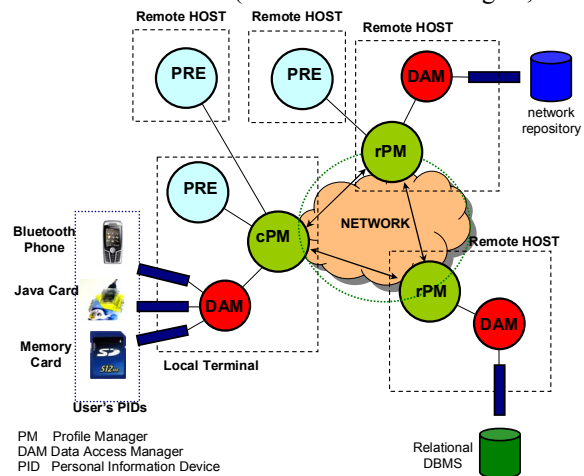

Figure 4: Proposed architecture for handling profile information

The main two relevant interfaces are the PM-PM interface and the PRE-PM interface; though these interfaces are defined using WSDL (Web Services Description Language), the implementation of the communication can rely on different solutions (e.g. SOAP, middleware like CORBA or JXTA, agent communication platforms like JADE). We are currently implementing the solution using the JXTA platform [11].

To access the profile information, the Profile Managers exploits the Data Access Manager (DAM). This element translates the requests coming from the PM into a form suitable for the native communication mechanism used by the data repository (e.g. the PID, a relational database, a distributed storage system).

We argue that the components specified in the GUP architecture have a counterpart in our approach. The role played by the GUP server corresponds to the one of the Profile Managers and the GUP's RAFs are very similar to the Data Access Managers, as they both provide a common interface which hides the implementation details of different data repositories. The difference between the two models lies in the way user's data are handled: unlike the GUP architecture, which mandates a single central

entity in the network to manage the user profile, we use trusted distributed peer entities.

6. Exploiting XDI links for linking user identity, profile and context data

Let us consider the example depicted in Figure 5, which uses XDI/XRI to create a representation linking user identity, profile and context data. First, it is important to provide a way to identify the user. The user therefore may be identified by an XRI, like "@Acme*SamHamilton", this tells that the user Sam Hamilton has an account with the Acme corporation; This identifier may be linked to any other identifier used by any Operator or Service Provider; for example a network operator which traditionally uses Sam's SIM IMSI to identify its subscribers might maintain backward compatibility using a so called XRI cross reference [7], expressed as "@Acme*SamHamilton*(@MobileOp/+IMSI)".
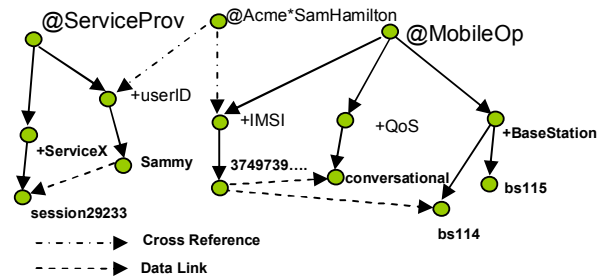Similarly, a Service Provider may link its own subscriber identifier to Sam's XRI.

Figure 5: A sample XDI/XRI graph

Second, Sam has his own user profile, which might be an instance of 3GPP GUP and contain Sam's preferences and policies; each instance of them can be addressed by one XRI, like: "@Acme*SamHamilton/+preference/pref487"

Despite these data may physically reside on the terminal, on the Sam's Personal Identification Device or somewhere in a network repository, the distributed nature of XDI and the use of XDI links helps in maintain a logically unitary representation of Sam's profile information. Note that this approach also stresses the idea that the user profile belongs to Sam and not to one single Operator, as it is correct in an environment with heterogeneous networks available.

Finally, context information could be linked the same way, as depicted in Figure 5: When Sam's SIM connects to a UMTS network, the operator database is updated to reflect the change. This could be represented by establishing a XDI link between the user identifier and the identifier of the base station which the user's terminal connects with.

This unified representation allows to answer a number of queries just by "navigating" the established links. Possible queries include: "How many users are actually using this base station?", "Which RAT/operator my device is connected to?", "What QoS is delivered to the user?", and so on. The aforementioned questions might be originated by different subjects like Operators, Service Providers, etc. Since is important to prevent that unauthorized subjects access these data, XDI defines also a mechanism of authorizations based on "contracts" associated to each links [12].

7. Acknowledgments

References

[1] G. Bartolomeo, S. Salsano, N. Blefari-Melazzi: "Exploiting Access Control Information in User Profiles to Reconfigure User Equipment", International Workshop on Ubiquitous Access Control (IWUAC 06), July 17, 2006 - San Jose, California, USA.

[2] ETSI EG 202 067: "System framework", ETSI TR 103 077: "Maximizing the usability of UCI based systems", ETSI EG 202 249: "Guidelines on the usability of UCI based systems".

[3] 3rd Generation Partnership Project. 3GPP Generic User Profile (GUP) 3GPP TS 29.240.

[4] N. Blefari Melazzi, S. Salsano, G. Bartolomeo, et al. "The Simplicity System Architecture", 14th IST Mobile Summit, 19-23 June 2005, Dresden, Germany

[5] XML schemas for Simplicity User Profile: http://netgroup.uniroma2.it/SUP

[6] Drummond Reed, Geoffrey Strongin, "The Dataweb: An Introduction to XDI, A White Paper for the OASIS XDI Technical Committee - v2", April 12, 2004

[7] OASIS consortium, "Extensible Resource Identifier (XRI) Syntax V2.0", Committee Specification, 14-11-2005

[8] M. Duerst, M. Suignard, "Internationalized Resource Identifiers (IRIs)", IETF RFC 3987

[9] OWL Web Ontology Language, W3C Recommendation, http://www.w3.org/TR/owl-features/

[10] G. Bartolomeo, N. Blefari-Melazzi, F. Martire , S. Salsano, "Defining and Using Profiles to Personalize and Manage Reconfigurable Services", 15th IST Mobile Summit 2006.

[11] The JXTA home site, www.jxta.org

[12] http://www.oasis-open.org/committees/download.php/15292/Link Contracts.doc.