A SERVICE BROKERING PLATFORM FOR PROVIDING PERSONALIZED AND SECURE CONTENTS

Alessandro Andreadis
Department of Information Engineering, Siena University, via Roma 56, 53100 Siena, Italy

Giovanni Luca Daino
Agorà ICT, via Massetana Romana 12, 53100 Siena, Italy

Keywords: Personalized services, Service brokering, User modelling, XML technology, Security and privacy.

Abstract: During the last years, 3G standardization activities led to new directions both in the network and the service provision architecture. As a result, new concepts of service portability have been defined, as well as new topics related to security issues. Taking into account such an input, we moved to promote the development of a new generation of user-friendly and personalized information services for citizens as well as students and bank customers, accessible any-time, any-where, with any technology. In order to realize a personalized and trusted secure access to information services, we propose here a service brokering architecture. Based on Java and XML, the system implements user profiling techniques to tailor contents in a way that is independent of the specific device (fixed or mobile) used to get access. Such a new approach should carry to a fruitful user-friendliness and security in service managing, enabling the user to access services in an intuitive, trusted and personalized way, both in terms of service portfolio and user interface.

1 INTRODUCTION

In the field of mobile communications, 3G standardization activities over the last years led to new directions both at network layer and in service provision architectures. The growing diffusion of different communication devices (mobile phones, notebooks and PDAs) has been the trigger for an increasing demand of services as well as for new business opportunities for service providers. The present communication paradigm expects a user to be able to access his services independently of his location in a transparent way. Key concepts in the definition of such a new service generation are mobility, portability, personalization, trust & security. These service features converge in the definition of a new *3rd Generation Partnership Project* (3GPP) network concept: the *Virtual Home Environment* (VHE). The service platform presented in this paper, partially funded under the EU IST SM-PAYSOC contract (SM-PAYSOC project, 2005), has been designed and developed according to this concept, in order to provide a trusted, personalized and secure infrastructure, applicable to different application domains, ranging from student services, public administration services for citizens, payment services and health care services. Secure standard communication techniques (IPsec, VPN, etc.) have been used and JAVA, XML and XSL have been the leading technologies to set up the whole framework and to perform service personalization. After a general description of personalization and services issues, we illustrate the system architecture, giving details on the blocks which constitute the core implementation of the VHE concept and explaining how dynamic adaptations are performed. The basic mechanisms for providing security features are then described, before coming to results and conclusions.

2 PERSONALIZATION AND SERVICES

Personalization issues, both in terms of user interface and services, have been faced within the VHE framework of the 3GPP with the aim at

Andreadis A. and Luca Daino G. (2006).
A SERVICE BROKERING PLATFORM FOR PROVIDING PERSONALIZED AND SECURE CONTENTS.
In *Proceedings of WEBIST 2006 - Second International Conference on Web Information Systems and Technologies - Internet Technology / Web Interface and Applications*, pages 303-309
DOI: 10.5220/0001254103030309

supporting personal service portability across network boundaries and between terminals (3GPP 2000, 3GPP 2002). The main objective of this idea is to present users with the same personalized features, user interface customization and services, in a consistent way, whatever network and terminal they are using, wherever they are located.

The user should be given the possibility to manage services as well as their appearance, through a *Personal Service Environment* which is made of personalized services and user interface (compatible with terminal capabilities), consistent set of services from the user's perspective irrespective of access modality (e.g. fixed, mobile, wireless etc...), and global service availability when roaming across mobile networks.

The user's Personal Service Environment is a combination of personal and services information (Caokim & Sedillot, 2002), describing how the user wishes to manage and interact with communication services. It combines a list of services subscriptions with a set of preferences associated to terminal interface, to services and to other information about user's experience of the system.

Moreover, it should be possible for the user to be aware that service personalization could be limited by technical constraints, imposed by the adoption of different terminals and serving networks.

Significant efforts have been done in the EU PALIO project (Andreadis et alii, 2003) and in the VESPER project (Moura et alii, 2002) in order to implement the adaptation and personalization concepts, trying to adapt and to scale multimedia contents to different user devices and access networks.

With respect to this approach, in our architecture the concept of content adaptation refers to rendering issues rather than to scalability issues, offering the same contents and services regardless of the type of terminal the user is adopting.

The VHE concept has been interpreted, enhanced and implemented through a Java-based infrastructure, aiming to achieve ambitious results in terms of service personalization and adaptation to different user profiles and different access devices. VHE is managed by a middleware between the user and the set of distributed services which are belonging to different service providers.

It is made of two different components: the Service Broker and the User Modeller (SM-PAYSOC Consortium, 2004).

3 SYSTEM DESCRIPTION

Figure 1 represents the general system architecture for accessing distributed services through personalized and secure interactions. Security mechanisms are provided on different devices (PCs, PDAs, kiosks, mobile phones) by the use of a suitable token. Different tokens are supported (e.g., smart card, USB pen, SIM card), thus allowing the user to adopt the preferred technology. The token is equipped with a powerful chip which interoperates with a *Public Key Infrastructure* (PKI), certification/registration authorities and related mechanisms in an IPSec environment.

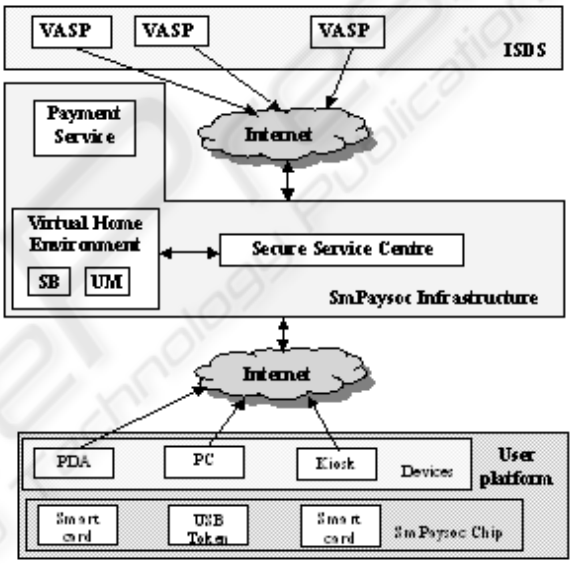

Figure 1: high-level system architecture.

Information and Services Distributed Space (ISDS) represents the whole set of services made available by different service providers. It is a co-operative space where different organisations, public or private, and providers contribute to the territory description and knowledge. Value Added Service Providers (VASPs) offer information about traffic, services of public administrations and local products.

The *User Platform* comprises user devices for fixed or mobile access, equipped with the powerful chip for supporting multi-service and multi-token secure transactions.

The *SM-PAYSOC infrastructure* includes the VHE, Secure Service Centre and Payment Service blocks.

The *VHE component* is the core of service personalization, aiming to provide the user with a

common look and feel interface and service experience, regardless of location, networks and terminal. The VHE is composed by the *Service Broker* (SB) and the *User Modeller* (UM). SB is the interface between the user and ISDS. It manages the personalization of content, service and information space for the environment visited by each user, according to the user "habitat". The UM is the basic component for service personalization. It keeps the user preferences in dedicated databases and selects the proper user profile.

The *Payment Service* processes online payments, offering the customer with the convenience of submitting his credit card or other forms of payment, and the vendor to actually receive the money from this transaction.

The *Secure Service Centre* (SSC) provides trust, confidentiality, authentication and protection in the services and grants legacy of the transactions.

In the following sub-sections we provide details on the core element of the system architecture, i.e., the VHE component.

3.1 Service Brokerage and User Modelling

The key requirement of VHE is to provide a user with a *Personal Service Environment* which consists of personalized services, customized user interface and a consistent set of services that is independent of access technologies (e.g., fixed, mobile, wireless etc.). The Service Broker and User Modeller modules have been designed with the aim to manage service adaptation and user profiling issues (Daoud & Mohan, 2002). The Service Broker represents the real core of the system architecture in a service perspective. It is a middleware that is capable of satisfying user needs and requirements in a dynamic and personalized way. It implements some functional elements, as defined by the 3GPP VHE standard (3GPP 2000, 3GPP 2002) designed for UMTS network, giving emphasis to session, connection and adaptation management.

In particular, the Service Broker implements the following functionalities:

· automatic identification of the terminal type adopted by the user;

· user authentication;

· check for the active profile;

· information adaptation on the basis of the specific profile;

· personalization of the service environment;

· session routing towards the proper service provider, who is in charge of the required service;

· management of session tracking (opening, maintenance and closing of the session during the interaction with service).

Figure 2 shows the modular structure of VHE architecture.

The Service Broker communicates with the User Platform through HTTP request/response messages. The framework for such a complex infrastructure is based on Java technology. XML/XSLT is the mark-up language used to exchange information with service providers inside ISDS and HTTP is the communication protocol.

The *Connection* module handles the communication between user and Service Broker, identifying the user access device through the proper field in the header of its HTTP request message.

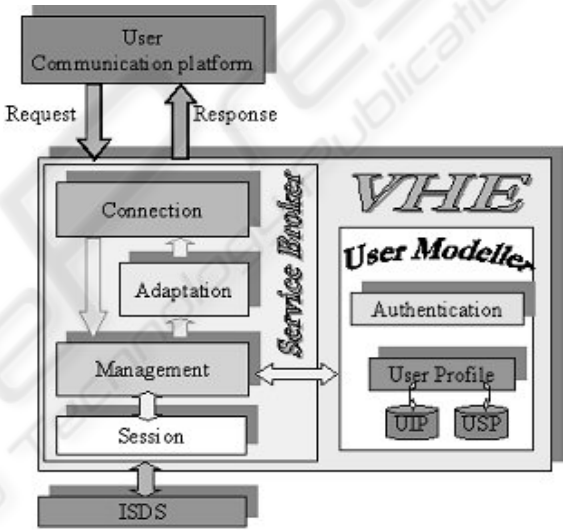

Figure 2: VHE structure.

The *Management* component is the control logic of the whole system, coordinating all the activities within VHE framework. In particular, it interprets the information flow, identifying the type of session required (user authentication, preference setting or service activation/interaction) and activates the necessary resources.

The *Adaptation* unit performs the content personalization on the basis of the access device and user preferences in terms of interface (font size, font color, font type, background color etc. within the terminal capabilities). Adaptation is carried out through proper transformations made by a XSLT Processor.

The *Session* module is the interface between the external service space and the Service Broker, setting up XML over HTTP connections.

Finally, the *User Modeller* manages user related functionalities. It gives emphasis to personalization and user profile management. Informative content adaptation is performed on the basis of User Profiles that are stored in "ad-hoc" databases (UIP and USP in fig.2) inside the UM module within the VHE block. In particular the User Modeller handles the user authentication process (in connection with the Secure Service Centre) and selects the proper User Profile (Bougant et alii, 2003) to be activated for the current session. A User Profile is expressed by the pair User Interface Profile/User Service Profile (UIP/USP). USP is the service portfolio subscribed by the user for that specific profile; UIP contains user interface preferences and indications about graphic layout and rendering options for the fruition of the subscribed services.

3.2 The Adaptation Mechanism

The Service Broker has been designed to perform the adaptation process, in order to provide customized services to different users. Basically, a set of user preferences is used to dynamically set up a user profile, in form of XSL stylesheet. The XSLT (W3C Recommendation, 1999) processor hosted in the Service Broker matches the XML service info coming from the VASP with the customized XSL stylesheet (fig.3), thus generating the customized HTML page to be presented to the user.

This procedure is performed for every single service interaction taking place between user and service provider. In order to allow the Service Broker to perform the adaptation process, a general XML schema has been defined, taking into account VASP requirements in terms of service interface features and user requirements related to usability and accessibility.

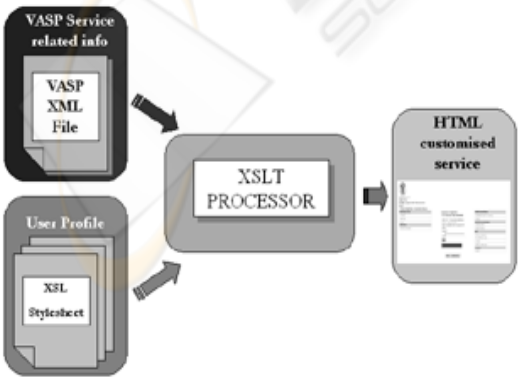

Figure 3: XSL transformation.

The XML schema (fig 4) used to validate XML files coming from the VASP, defines a common set of components that can be used to build single pages for each service. Each of these tags represents a certain area of the display and will always be rendered in these positions regardless of their location within the XML document.

The primary elements of interest are the ones that are contained within the root <smpaysoc> element, namely:

The <header> tag represents the top of the page. It can contain text and image elements. The example contains an image and some text lines, which are laid out according to the <row> and <cell> tags inside the <header> tag.

The <menu> tag represents a menu list of services and options. It can contain a header and several menu items. In the example, there are two menus - one on the left and one on the right side. This is defined by an attribute of the <menu> tag [type="left" or type="right"]. The header is rendered differently from the items, as seen in the example. The menu items also react by changing color when the mouse pointer moves over them.

The <interactions> tag represents a series of controls, offering the possibility to interact with the current service. In the example, the interactions area contains a radio button, a checkbox and some text areas, but it can also include several different elements (text field, combo box, images, etc...).

The <browsings> tag at the bottom of the page offers controls for navigating the web site. In the example the browsings area contains two buttons.

The <object> tag represents embedded objects such as Java applets and ActiveX controls. These objects are not visible when the screen is rendered, but their functionalities are available for use by embedded scripts.

The <parsed script> tag represents Javascript function calls, which can, for example, invoke methods on the embedded objects. The <parsed_script> tag does not have a visual representation either.

The <card_interactions> tag contains instructions for interacting with the token, including, but not limiting to, writeObject, readObject, deleteObject and listObject. These instructions are executed during the page loading. The <card_interactions> tags also provide an abstraction layer so that the service providers do not have to manipulate the scripts directly and can use these tags in a standard manner instead, reducing the possibility of errors and providing a more robust interface.

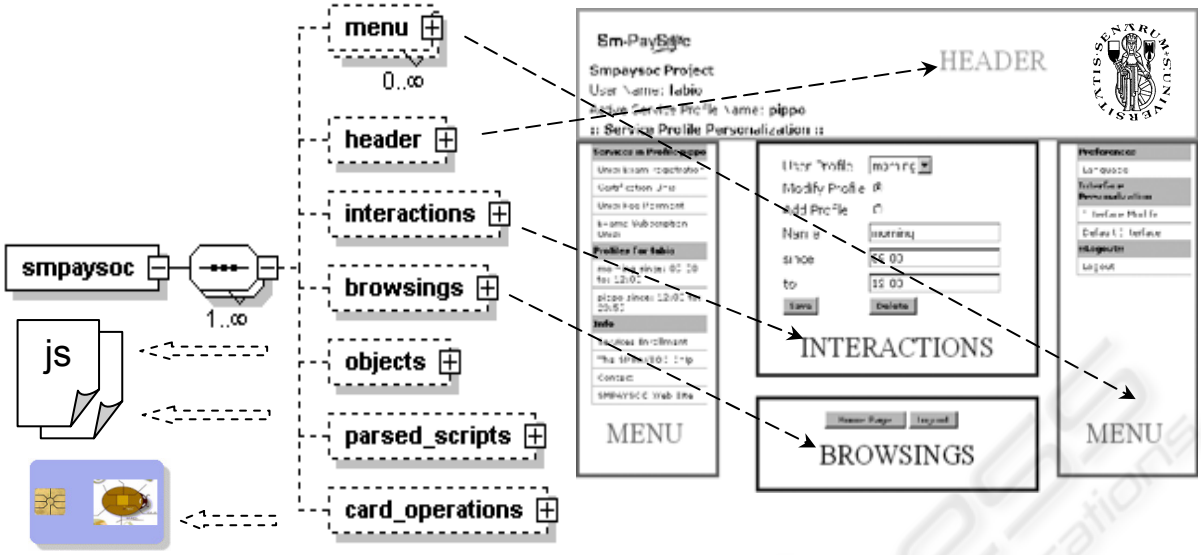

Figure 4: XML schema and related output.

The layout within each of the elements which correspond to visual elements of the page (header, menu, interactions and browsings) is controlled by the use of <row> and <cell> tags within the XML. Looking at the example, in the header area, the image and the five lines of text are in individual cells, which in turn are contained in different rows. If the text cells were to be moved into the image row element, they would all appear in one line across the top of the page. This behavior is identical to the <TR>/<TD> behavior in HTML tables (indeed when the transformation is applied that is what the <row> and <cell> elements become respectively).

Aiming to ease the design of services compliant to such an XML Schema, a proper tool has been implemented, to be provided to VASPs. As a result, no XML programming skills are required to set up services and it will be easier to design different services to be deployed through this framework.

4 SECURITY ISSUES

Security and privacy issues have been carefully taken into account in order to provide the user with the possibility of interacting with services in a trusted way and of performing payment transactions through a secure service infrastructure.

The Secure Service Centre plays the main role in this respect. It initialises the token for first usage, generating keys on board of its chip with a web interface compliant to PKCS#11 standard. It gives the credentials to the user, certifying its own keys and registering him in the system. It manages the authentication of the user toward the VHE, through an authentication propagation mechanism based on the X500v3 certificates. It provides network security services through *Virtual Private Network* (VPN) links inside the system architecture. Inside the SSC a complete PKI is realized in order to offer all the security services of a standard PKI. SSC implements the middleware for VASPs and users, who can take advantage, on different services, of digital signature apposition and verification.

The SSC is responsible of user and network authentications, by managing the propagation of User-Network authentication toward the VHE environment. It deals with the design definition and implementation of the Trust Infrastructure based on the PKI.

In our system the single user is identified by its own Public Key. The Public Key is associated to a Private Key. The Digital Certificate is a digital document identifying a user inside the PKI he belongs to; the certificate holds the public key of the user (and other personal information), it is not falsifiable and it can be distributed without limitation. The private key is never divulged and, thanks to the chip and middleware design, it cannot be exported or modified once it has been created inside the chip. The user doesn't know its value, but he can only use it. The user enables the usage of the private key stored inside the chip crypto-engine, simply by digitising a secret PIN (applying the security concept "something you have plus something you know"). Two users can communicate in a secure way with each other through their respective certificates. For "secure way" we mean the fact that each user is sure of the identity of the

other user and the communication can be encrypted in order to avoid malicious eavesdropping or dangerous attacks.

Inside a PKI, certificates management is submitted to a specific authority: the *Certification Authority* (CA). The CA guarantees the identity of every entity belonging to the PKI, by furnishing, publishing, revoking and suspending Digital Certificates. The CA has a database (repository) containing all the released certificates together with their status (active, suspended, revoked). SSC assures authentication of both data flow and actors and at the same time it protects sensitive data, infrastructure resources and information on user terminal and personal/financial data.

Security mechanisms are applied on the links between the terminal and the SB and in some cases between SB and VASP. This is done in order to avoid illegal use of contents and services and unlawful eavesdropping to the users whereabouts and actions. The security feature also protects the system infrastructure from any hacking activity and prevents even registered system users, system administrators and technicians from the ability to access personal data collected about any other user of the system. The SSC interacts directly and/or is the intermediary toward the SB and VHE for granting high level security and trust.

The authentication mechanism validates the right to use the entity that is accessing the system, either when the access is originated by the users, by the terminal applications, or by the system's initiative via the token. The administrator of the system is able to remove and prevent usage by terminals that have been marked as stolen.

The adoption of the secure VPN allows to tailor the service delivery according to different usage and access to the system community. At the same time, the exploitation of a secure VPN allows us to distribute the whole infrastructure all over the Internet, with no cost impact due to leased lines.

The token is the passport for gaining entry in this service infrastructure, allowing to access the same resources in the same way, irrespectively of operating systems and adopted terminals.

5 RESULTS AND CONCLUSIONS

Testing activities has been carried out in a multi-service and multi-platform environment, involving many different users and access devices (PC, PDA and kiosk). Two types of tests have been conducted: a portability test, where a single user accesses the platform several times with different devices; a personalization test, where different users access the platform with the same device.

Several service scenarios were considered, such as students requesting University certification of their scholastic carrier (with all data about their exams), to be downloaded and stored on the chip, but also citizens wishing to pay for their children the school canteen fee. Figure 5 reports some snapshots of the system output on different devices. As a matter of fact, a Common User Interface has been designed following the User Centred Design approach (Carroll, 1995, Andreadis et alii, 1997). According to this approach, we have carried out three iterative cycles of the following tasks: user requirements analysis – feedback to the designers – new implementation – user evaluation. As a result, a simple but efficient user interface has been achieved, allowing a user-friendly service interaction that has been positively evaluated by different groups of users involved in the testing.

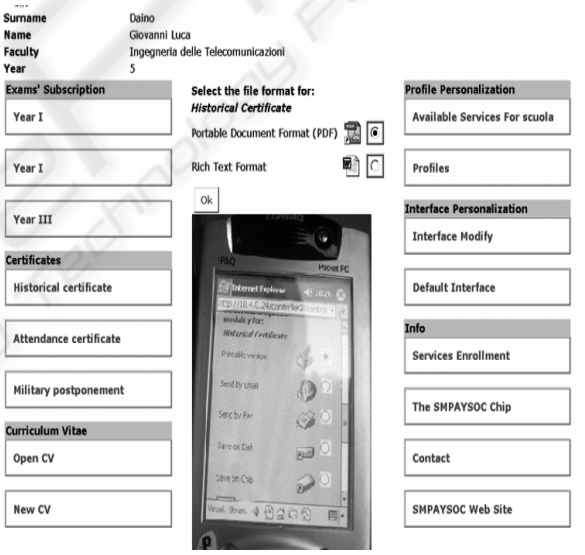

Figure 5: service output for kiosk and PDA.

Referring to personalization, several tests have been performed, to provide users with the chance to define preferences in terms of both services and user interface. As for services, every single user is allowed to create his profile only with the services he is interested in. On the other side, several efforts have been devoted to user interface customizations, allowing users to modify many interface parameters (font color, type and size, background color, menu colors, etc.). Some default settings have been defined to match specific needs of some groups of user. In particular, low-vision user requirements have been taken into account by designing a default

profile which implements colors contrast, according to specific rules defined by a Swedish study (Persson, 1990) on this relevant topic.

Results coming from this work are expected to provide a solid background for those implementing fixed and mobile services, introducing an innovative infrastructure to allow VHE features into a multi-purpose secure service platform. In a user perspective, these results should carry to a new security and user-friendliness in service managing so that only the needed content is provided to the user, in a trustful way that best fits to his preferences.

REFERENCES

3GPP (2000). TS 22.121, Service aspects; The Virtual Home Environment; Stage 1.

3GPP (2002). TS 23.127, Virtual Home Environment (VHE) / Open Service Access (OSA); Stage 2.

Andreadis, A., Fedele, P., Giambene, G., Santoro, J. (2003). Service adaptation and personalisation in the PALIO project. In *International Conference on Universal Access in Human-Computer Interaction UAHCI, vol.4, Crete, Greece, June 22-27 2003* (pp.294-298).

Andreadis, A., Marchigiani, E., Rizzo A. (1997). The AVANTI project: prototyping and evaluation with a cognitive walkthrough based on the Norman's model of action. In *Conference on Designing Interactive System: Processes, Practices, Methods and Techniques Amsterdam, the Netherlands, August 18-20 1997*.

Bougant, F., Delmond, F., Pageot-Millet, C. (2003). The user profile for the virtual home environment. In *IEEE Communications Magazine, Vol.41, Issue 1, Jan. 2003* (pp.93-98).

Caokim, S., Sedillot, S. (2002). Profiles management for personalised services provisioning. In *2nd European Conference on Universal Multiservice Networks. ECUMN 2002 Colmar, France, April 8-10 2002* (pp.315-321).

Carroll, J.M. (1995). *Scenario-Based Design*, John Wiley & Sons, New York.

Daoud, F., Mohan, S. (2002). Strategies for provisioning and operating VHE services in multi-access networks. In *IEEE Communications Magazine, vol.40, Issue 1, Jan 2002* (pp.78-88).

Moura, J.A., Oliveira, J.M., Carrapatoso, E., Roque, R. (2002). Service provision & resource discovery in the VESPER VHE. In *IEEE International Conference on Communications, ICC 2002*, *Vol.4*, *New York, US, April 28-May 2 2002* (pp.1991-1995).

Persson, L.O. (1990). Adaptation to chronic disease and handicap: a critical analysis and summary. Department of Psychology, University of Goteborg, Sweden.

SM-PAYSOC Consortium (2004). CEC Deliverable 03.04: VHE & Services Design.

SM-PAYSOC project (2005). Web site URL: http://www.smpaysoc.org

W3C Recommendation (1999). XSL Transformations (XSLT), http://www.w3.org/TR/xslt.