

Design and Implementation of a Service Provisioning Platform using Smart Cards

Vincent Guyot¹ and Nadia Boukhatem²

¹ Pierre & Marie Curie University
LIP6 - UMR 7606 CNRS
8 rue du Capitaine Scott
75015 Paris - France
`vincent.guyot@lip6.fr`

² GET-Télécom Paris/ENST
LTCI - UMR 5141 CNRS
46 rue Barrault
75013 Paris - France
`nadia.boukhatem@enst.fr`

Abstract. After having used multimedia services from his desktop computer, the mobile user wishes today to access these services whatever the terminal or network used.

In this paper, we propose an autonomic service provisioning solution to mobile users and suggest the use of a smart card as an autonomy enabler. Service portability, adaptation and session mobility management is handled entirely by the smart card.

1 Introduction

Autonomic networking covers a large spectrum of themes centred around the networking "selfware" concept. The aim is to develop networking systems capable to react to context changes without explicit user interaction. The development process towards these objectives will certainly be evolutionary and gradual. In this paper, we focus on autonomic provisioning of network services and propose adaptable/context-aware service provisioning solutions allowing the mobile users to access their services through heterogeneous terminals and access networks in a seamless way. We suggest the use of a smart card as an autonomy enabler. For the user, service portability, adaptation and session mobility management is handled entirely by the smart card. To access his services, the user has only to insert his smart card whatever the terminal. Our solution is developed as a first step towards a totally autonomic service provisioning and deployment. Indeed, autonomy here concerns the point of view of the user rather than the network.

The mobile terminals have evolved. From simple telephony mobile phones, they got memory and execution environments to become intelligent terminals.

The recent developments of wireless technologies and mobile access networks, covering large areas and providing increasing rate, allow the mobile user to remain online wherever he is. The evolution of both terminals and access networks enable the development of new services where mobility is of a main concern [1]. In addition, the services have to be personalizable and portable, and have to adapt automatically to the used terminal [2]. When the user switches from one terminal to another, he should be able to resume his session suspended from the previously used terminal [3].

Since fifteen years, the smart card is impossible to circumvent within mobile networks security. The recent technical evolutions within the smart card field enable the smart card to embed much data processing power.

We propose a service provisioning architecture based on the usage of a personal smart card. This architecture has been developed in the context of various research projects³. This environment enables the mobility of the session, the personalization and portability of the services, in a secure way.

This paper is organized as follows. Related work is presented in section 2. In section 3, we provide the main requirements of the service provisioning system. The benefits of using a smart card are explained in section 4. We describe the architecture of the service provisioning system in section 5 and give its main characteristics in section 6. Technical details about our implementation are finally provided in section 7.

2 Related Work

Related work has been done in several European research projects, investigating different ways to realize service provisioning.

The CAMELEON project [7] investigated the application of Agent Technology for the purpose of providing service ubiquity. The project developed an agent-based Service Roaming by implementing an Adaptive Profile Manager and a Personal Agent Manager [8], featuring service provisioning.

In [9], Shiaa et al. describe mobility support in TAPAS (Telecommunication Architecture for Plug And Play Systems), a platform and application development environment based on agent technology. The session mobility is handled by agents, both on the local terminal and remote servers, using session information stored in a local server.

³ I3[4], MMQoS[5] and Safari[6]

Bo You proposed an architecture [10] for User Mobility based on a personal smart card. The card contains a unique identifier to authenticate the mobile user. However, this solution relies on remote servers to enable session mobility.

Only few researches have been done on the provision of services to mobile users through smart cards. The CESURE project provided a framework [11] to build adaptable applications using a smart card to store the description of the user's environment. Such information is retrieved from the card to build an application with different parts downloaded from remote servers.

The common view of service provisioning is based on interactions between the terminal and remote service provider servers, where different services, session information and profiles are stored. Our approach is different: we put a part of the remote server's functionalities within the smart card to enable autonomy. In addition, using a smart card in such a way avoids expensive networking connections and brings benefits to the end user (see section 4).

3 Service Provisioning

The service provisioning platform has been developed considering the following requirements:

Autonomy in service provisioning To access his services, the mobile has only to insert his smart card on the available terminal. The smart card handles all the operations to provision services automatically and in a seamless way (service portability, adaptation to the current context and terminal capacities, session mobility, etc.).

Service Portability The mobile user may use different kinds of terminals. He should be able to access his services whatever the terminal used. The aim of service portability is to make the service usable through different kinds of terminals. The behaviour of the service may be modified according to the type of the terminal used, and restricted to a subset of features.

Service Personalization The mobile user wishes to use his services depending on his own criteria. The service personalization enables to handle preferences previously set by the user. When the services are installed within a given terminal, they are personalized according to the needs of the user. The user can modify his preferences at every moment, within the limits given by his contract.

Session Mobility When he switches from a terminal to another one, the mobile user should be able to continue to use his services in a seamless way. For this purpose, it is necessary to save the state of the ongoing work environment when the session suspension occurs. This state will have to be restored to enable the session to be resumed on the new terminal. The services have to provide session information describing their working state to enable a future restoration. From the user point of view, his session is mobile.

Security Management The mobile user accesses his services following an agreement made with his service provider. The user pays to use his services and wishes to use them in a secure way. There is a need to forbid the unauthorized access so that nobody else could use the user services. Moreover, the personal data that the user may provide when he uses his services should remain private. Finally, the service provider wants to control that a given user remains within the limits of his service contract.

Operation and Management cost reduction The provision of adaptable and personalized services to mobile users introduces complexity and overhead in service management. Solutions have to be found to limit the service management costs and ensure profitability to network/service providers when offering new services to the mobile users.

4 Benefits of Using a Smart Card

We benchmarked several smart cards available on the market [12]. We observed they have been significantly improved during the past few years. Technical evolution permitted the birth of new powerful smart cards. The speeds of calculation and transfer are getting faster and faster. At the same time, the size of embedded memory is rising up. In 70s the memory within smart cards was only few bits, now it is possible to store several mega-bytes in a secure way within the new smart cards. For all these reasons, we think the smart card is a perfect versatile token to enable personalized services to be provided to the mobile user.

We put within the smart card features used to be localized in remote servers (see figure 1). The mobile user has only to insert his personal smart card within a terminal in order to rebuild his personal working environment from the smart card.

Several actions are automatically done when the user insert his smart card within the terminal, and when he removes it:

After having inserted the smart card:

- deployment of the services within the terminal,
- service personalization according to the user's profile,
- resuming the session from embedded session information.

Before removing the smart card:

- session information updating within the smart card,
- removing the previously installed services within the terminal.

This innovative way of realizing service provisioning through the usage of a smart card brings several advantages:

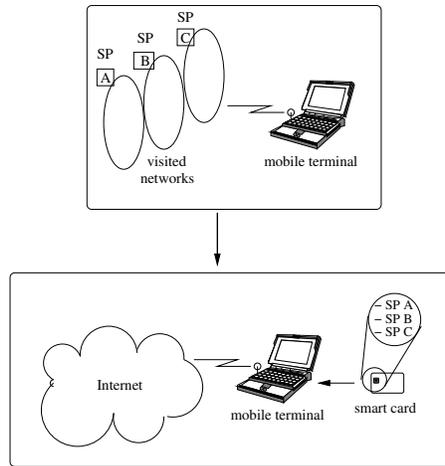


Fig. 1. Service provisioning model evolution

Services Availability The services of the mobile user are always available. They follow the mobile user, stored within his personal smart card.

Scalability Retrieving information locally, from the smart card, avoids expensive connections to remote servers. This behaviour gives a good scalability to the system, avoiding remote servers that are bottlenecks.

Session Mobility Enabling A big challenge is to provide session mobility to the user. Using a smart card gives facility to achieve this goal, by recording session-specific information within the card when terminal switching occurs. When the user inserts his personal smart card within another terminal, the information stored within his card enables him to continue the use of his services in a seamless way.

Tight Billing A smart card is a secure environment that cannot be modified freely by the user. It enables to pay like a banking card, or through prepaid credits like public phone cards.

Enhanced Security The usage of smart cards to access services prohibits unauthorized access. The traditional couple login/password, which remains unsecure, is no longer required to access remote servers. To secure the usage of the smart card, it is possible to use authentication mechanisms, such as a password or biometric methods, preventing to use a stolen card. The network operator knows that the user is not able to modify his subscribed connection parameters, as they are stored within his smart card.

Autonomy Until now, the mobile user had to configure the terminals that he wanted to use, in order to be able to use his personal services. Using a smart card, this is not the case anymore: his smart card configures his services automatically in order to retrieve his personal working environment.

5 The Architecture

We divided our architecture into three parts [13] to achieve its objectives (see figure 2). These parts are located in different components of the system:

- the CU (Card Unit) is within the smart card,
- the TU (Terminal Unit) is within the terminal,
- the SP (Service Portal) is within the network.

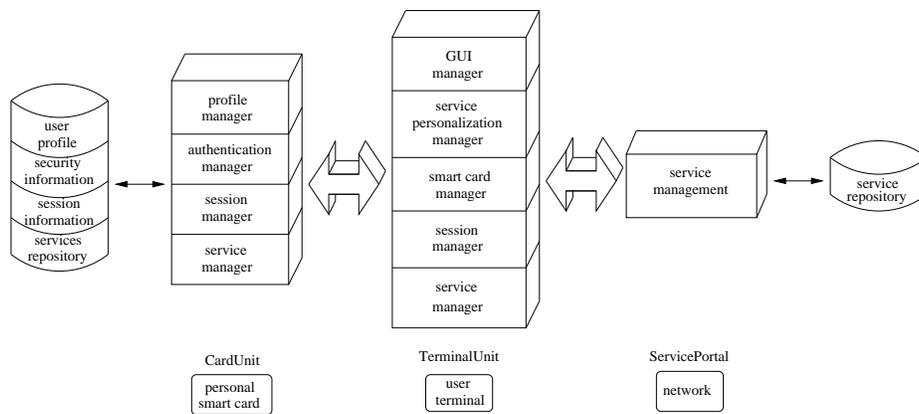


Fig. 2. Architecture components

5.1 The CardUnit

The Card Unit (CU) is the personal component of the platform, stored within the smart card. The user carries it wherever he is.

The CU handles several tasks:

- Authentication of the smart card holder and of the terminal used,
- Handling of the user's profile,
- Recording and Retrieving the session information,
- Providing the user services.

5.2 The TerminalUnit

The Terminal Unit (TU) is the generic part of the platform. It is built in every terminal of the network operator. It will be personalized by the smart card.

The TU handles several tasks:

- Provision of a graphical interface to the user,
- Personalization of the services, according to the user profile,
- Authentication of the smart card provider,
- Handling the session mobility (suspend/resume),
- Handling new services available from the network operator.

5.3 The ServicePortal

The ServicePortal (SP) is a part of the platform that is within the network, enabling the use of new services.

The SP handles several tasks:

- Presenting new services from services providers,
- Downloading new services for the mobile user.

6 System Characteristics

The service provisioning system has been developed to allow the mobile user to benefit from service personalization and session mobility.

6.1 Service Personalization

The smart card is a safe place to keep sensitive data. New smart cards embed enough memory to store the preferences and the services of the mobile user. The profile and the services being stored within the smart card, it is no longer required to connect to remote servers to retrieve them. The availability of the user profile and services eases the service personalization step.

The processors embedded within the smart cards are faster and faster each year. The smart cards are now powerful enough to ensure the profile and service management. On demand, the smart card can provide the user's preferences to the terminal and manage his services. The mobile user can also modify his preferences, within the limits authorized by his network/service provider.

The different components enabling service personalization [14] are presented in figure 3.

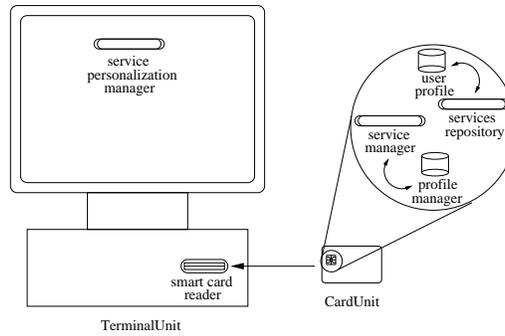


Fig. 3. Components involved in service personalization

- CU's profile manager
It handles the user profile, which is stored within the card. The profile manager has two different tasks. It replies to the requests from the TU's service personalization manager, sending back the user's preferences stored within the user profile. It also has to update the user profile. The profile manager is the only entity able to modify the profile stored within the card.
- CU's services manager
This service manager provides the user's services which are stored within the services repository to the TU's service personalization manager. Also, when the user subscribes new services, the service manager stores them within the service repository.
- TU's service personalization manager
This program has to provide the user with his personal services. It communicates with the CU's profile and service managers to load and configure the services according to the user profile.

6.2 Session Mobility

Different components enable session mobility, both within the smart card and the terminal used. They are presented in figure 4.

- TU's card manager
Within the terminal, it waits for the smart card being inserted.
It handles the mutual authentication between the terminal and the smart card.
- CU's authentication manager
Within the card, the authentication manager participates in the mutual authentication between the smart card and the terminal.
- TU's session manager
The session manager runs within the terminal. After the smart card is inserted, it obtains the session information from the CU's session manager. It

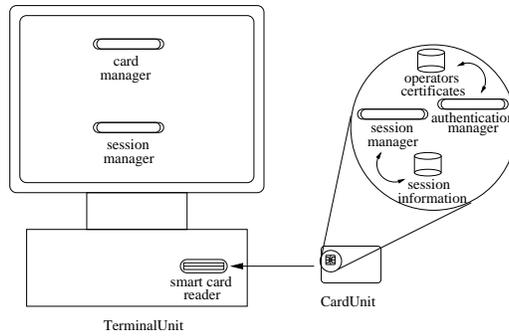


Fig. 4. Components involved in session mobility

enables the session mobility.

A graphical interface enables the user to suspend his session and to store the information of the session within his smart card.

- CU's session manager

Within the smart card, the session manager provides the information to resume a session, and updates the information within the card, after suspending a session.

7 Implementation

We developed a distributed smart card application with both on-card and off-card parts. Our platform has been implemented with portability expectations. Therefore we wrote the off-card part and the services in Java. The on-card part of the platform has been written in JavaCard to be able to use it as-is with different smart cards all embedding JavaCard 2.1 Virtual Machine.

To access the card reader, we used Java OCF standard classes. Since only the card reader PC/SC driver was available, we used a PC/SC to OCF software bridge. Under UNIX systems, we used pcsclite, the PC/SC opensource implementation.

We developed an administration tool to load the personal data within the smart card, such as certificates, the user profiles and small services.

In order to evaluate the capabilities of actual smart cards to handle session mobility, we implemented real services and observed how fast the cards are to suspend and resume a given user session.

These tests are made on several running services: a clock, a stock manager and an email client. The services are all stored within the card and have to be

downloaded from the card. Session information to retrieve is composed of the list of the active services, the location of the active windows, the previous display resolution and service-specific session information such as email text or the stock manager remote server address.

We suspended the session. We measured the time between the moment when the system is notified by a click on the appropriate button and the moment when the system notifies that the card can be safely removed. This moment corresponds to the upload of session information within the smart card. Depending on the used smart card⁴, the suspension of the session takes 0.8s to 7.1s. Finally, we measured the time to restore the session in a usable manner on the screen. Depending of the used smart card, the restoration of the session takes 4.7s to 51s. The shortest times are obtained by the most recent cards of our testing panel. 1s to suspend and less than 5s to resume a session is fast and very usable in real conditions.

8 Conclusion

During the last few years, technology evolved significantly within the field of smart cards. The processing power increased at the same time than storage capacity and communication capabilities. Smart cards can now enable service provisioning.

This work provides a new solution for service provisioning to the mobile user by using a smart card. Our current implementation runs on laptops and workstations. We expect to provide a version running on PDA-based platforms soon. This next step will ease service provisioning in the real world.

References

1. Y. Li and V. Leung. *Protocol Architecture for universal personal computing*, volume 15 of *IEEE Journal on selected areas in communications*. October 1997.
2. E. Koukoutsis, C. Kossidas, and N. Polydorou. *User Aspects for Mobility*. Acts Guideline SII-G8/0798.
3. G. Forman and J. Zahorjan. *The challenge of mobile computing*. IEEE Computer, 1994.
4. I3 project. <http://www-rp.lip6.fr/i3/>.
5. MMQoS RNRT project. <http://www.mmqos.org/>.
6. SAFARI RNRT project. <https://safari-rnrt.rd.francetelecom.com/>.
7. ACTS CAMELEON project. <http://www.comnets.rwth-aachen.de/~cameleon/>.
8. A. Macaire, D. Carlier, and P. Paradinas. A Personal Agent Manager for Mobile Users. In *EMMSEC*, 1999.
9. Projet TAPAS. <http://tapas.item.ntnu.no/>.

⁴ Our benchmark panel of smart cards is composed of 30 different Java card models.

10. Bo You. Mobile Card Architecture for User Mobility and VHE in Heterogeneous Network Environments. In *Communication Networks & Services Research (CNSR)*, Moncton, Canada, May 2003.
11. CESURE project.
http://www.telecom.gouv.fr/rnrt/rnrt/projets_anglais/cesure.htm.
12. V. Guyot. La Carte à Puce, Vecteur de Mobilité/Smart Card, the Mobility Enabler. PhD thesis, LIP6, 2005. <http://rp.lip6.fr/~guyot/these-VincentGUYOT.pdf>.
13. V. Guyot, N. Boukhatem, and G. Pujolle. Smart Card, the Mobility Enabler. In *5th Workshop on Applications and Services in Wireless Networks (ASWN)*, Paris, France, 2005.
14. V. Guyot, N. Boukhatem, and G. Pujolle. On Smart Card based Service Personalization. In *International Conference on Software, Telecommunications and Computer Networks (SoftCOM)*, Split, Croatia, 2005.