BUILDING MULTI-SERVICES IN PERSONAL MOBILE DEVICES BASED ON PARTIALLY TRUSTED DOMAINS

Miguel Filipe Leitão Pardal
Instituto Superior Técnico
Departamento de Engenharia Informática
Av. Rovisco Pais, 1049-001 Lisboa, Portugal
mflpar@yahoo.co.uk

Alberto Manuel Ramos da Cunha
Instituto Superior Técnico
Departamento de Engenharia Informática
Av. Rovisco Pais, 1049-001 Lisboa, Portugal
alberto.cunha@inesc.pt

ABSTRACT

Services based on personal devices are usually supported by self-contained infrastructures with specific terminals, managed by a supervising organization that ensures a trust domain with overall consistency. Well-known examples are automated banking, mobile communications and transport ticketing. Recent developments in information technology – the Internet and mobile wireless networks – shifted expectations for customers and service providers, creating new opportunities for both.
In this paper we analyze existing self-contained services and identify challenges to multi-services supported by cooperative providers with partial mutual trust, as part of a work in progress that aims to provide models and tools to support their implementation.

KEYWORDS

Multi-service, Personal Device, Mobile Device, Trust, Self-contained service.

1. INTRODUCTION

In the last decade, **personal devices** like smart cards, mobile phones and palmtops have become common in people's lives. Together with mobile wireless networks, they enable information access anywhere with little effort and at reasonable cost. As such, they may play an important role in the effective delivery of large-scale valuable services that need a secure and timely access to meaningful information (Laudon K.and Laudon J., 2002). Figure 1 presents a very simple and abstract model of service delivery, where the user (U) has a personal device (D) that can be used in a terminal (T). The data networks (N) support the information flows with the business servers (S).

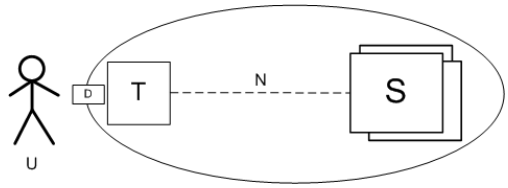

Figure 1 – Service delivery model based on personal mobile devices.

This model can describe several existing services, for instance: automated banking, mobile communication, pre-paid telephone calls, transport tickets, public identification, health card, toll payments,

etc. We call these **self-contained services**. Each example belongs to a vertical business area and has its own platform of devices, terminals and infrastructure. A supervising organization binds everything together, creating and maintaining a **trust domain**.

In this paper we analyze self-contained services and discuss some technology changes that enable multi-services, which have the potential to provide additional benefits both for customers and organizations.

2. EXAMPLES OF SELF-CONTAINED SERVICES

2.1 Automated banking

An automated banking user has a personal card that can be used in ATMs – Automated Teller Machines – to perform banking transactions. If the user provides the correct PIN – Personal Identification Number, a connection is established to the bank system over a private and secure network and the transaction executes. The security mechanisms are proprietary and not publicly documented in detail (Zoreda J. and Oton J., 1994).

Multiple banks can share a network, usually supervised by an inter-banking organization. Most of these platforms have become a generalized payment service for debits in retail, utility bills, taxes, etc.

2.2 Mobile communication

GSM – Global System for Mobile Communications – is a standard for digital, large-scale, wireless networks for voice communication, although data messages are supported through SMS – Short Message Service. GSM is widely used in Europe and in other parts of the word.

A GSM user owns a SIM – Subscriber Identity Module – card that is fitted in a mobile phone. A secret PIN activates the card, allowing the mobile phone to log on the network to make or receive phone calls. The authentication process is performed between the SIM card and the network operator.

User roaming between different networks is necessary because of territorial concessions to different operators and is possible because most trust is placed on both ends: the SIM card and the home network.

The network operators are expanding to provide value-added services based on data transmission. Some basic services, like telebanking, can be deployed over SMS messaging (Guthery S. and Cronin M., 2001), however GPRS – General-Packet Radio Service – brings new data transmission capabilities to existing GSM networks, and UMTS – Universal Mobile Telecommunications Service – and its IP-based protocols are another step forward in this direction (Patil B. et al., 2003). In all these cases, the network operator maintains tight control over which services can be deployed on its platform.

2.3 Urban mobility

Public transportation may involve many modes: underground, bus, train, and boat (CEN, 2001). A transports network can have many operators, even for the same mode. A transports authority usually supervises the overall transport network. Electronic tickets allow operators to keep accurate data of service usage, necessary to improve the overall effectiveness of the transport network.

Calypso is a standard for smart-card use in this industry (Levy F., 2001) (CNA, 2004), where the user's card is loaded with season or pre-paid tickets at points-of-sale. Ticket can be used across the transports network and are validated at entry points.

Urban traffic problems suggest the need for combined services like park-and-ride, where users are encouraged to park their cars at city outskirts and use the transports.

3. ANALYSIS OF SELF-CONTAINED SERVICES

A well-succeeded service offers a good cost-benefit relationship to the customer and to all the organizations in the value chain. Table 1 compares the self-contained services described previously.

Table 1 – Comparison of self-contained services examples.

Service	User Device	Terminal	Infrastructure	Supervising organization
Automated banking	Magnetic stripe card	ATM	Secure private network Bank servers	Bank(s)
Mobile communication	SIM Card	Mobile phone	Cellular Network Back-end servers	Network operator
Transportation	Smart-card	Point-of-sale Entry point	Transport network	Transport authority

The main strength of self-contained services is the standardization of their design and technology, which enables economies of scale and a simpler design of devices, terminals and infrastructure.

The supervising organization ensures the trust domain, but usually acts conservatively and focused on current business, making services difficult to extend beyond their original use, as each has its own security policy implemented using specific mechanisms (Anderson R., 2001). This leads to a situation of one device per service, which may be acceptable, but limits the number of services a user can access. For instance, to use all three services in Table 1, the user must carry three technically similar devices: the bank card, the SIM card (inside the mobile phone) and the transport card.

4. MULTI-SERVICES

The perception of customers and organizations towards electronic services has been evolving. The Internet as a large-scale public network presented an open and dynamic business environment. It would be interesting to take these features to device-based services and (Durlacher, 1999) presents some of the opportunities. Customers could use the same device for multiple services, with more convenience and other potential benefits. Service providers could reach customers through new channels not managed directly by them. Supervising organizations of public access infrastructures would have new ways of increasing their return-on-investment, e.g. services other than banking operations on ATMs.

New delivery approaches are necessary to achieve more open and dynamic services that can share resources between different organizations. **Multi-services** is an approach that composes devices, terminals and/or infrastructures of different self-contained services, supporting restricted information and functionality sharing. Figure 2 presents two multi-service alternatives for composing two services (A and B), at the user device level (left side of figure) or at the terminal level (right side of figure).

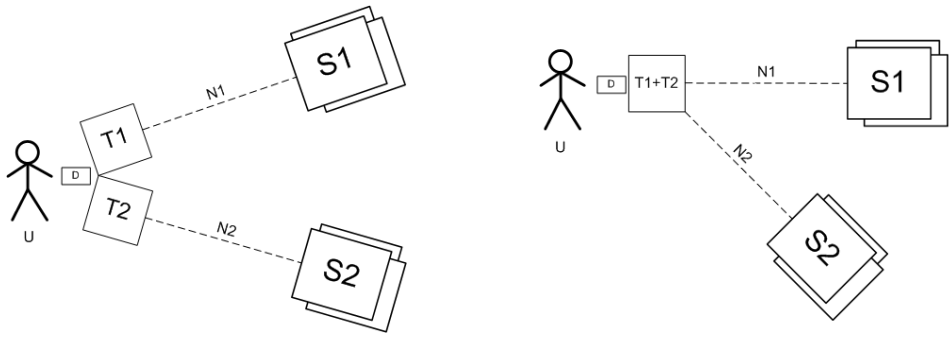

Figure 2 – Multi-service using the device or terminal.

From the user's perspective, multi-services are not new. There are already several examples of devices that enable access to more than one service, like co-branded banking/credit cards, tele-services on mobile phones, etc. However, from an organizational and technical perspective, these services are managed by a dominant organization, fully trusted by all associated business partners to execute service delivery

operations, e.g. financial transactions, customer registration and information, infrastructure operation, etc. In this sense, they are no different from self-contained services.

The first step of our work is the evaluation of the characteristics and requirements of **true multi-services**, i.e., services supported by cooperative business partners that agree to share information at a restricted level that excludes critical items like private security keys. The next step will be to define an architecture to support such services, including key management and distribution associated with loading of electronic contracts between different providers. Finally the proposed architecture will be validated and evaluated in a **pilot implementation**, with the use of a banking ATM network to load new season tickets in a secure transport card, assuming that the transport operator does not give up control of its security keys for ticket (contract) loading to the ATM service provider. Another possible scenario is the implementation of urban mobility policies on a city card such as park-and-ride, assuming a restricted amount of information sharing between public transport contracts and parking contracts on the card. The evaluation of the pilot will contribute to identify the approach's benefits and limitations.

An important characteristic of many of these systems that must be taken into account is that, due to their widespread use and location spread, they are **almost-never-connected**. This means that users, through their personal devices (cards, SIM cards), interact with local terminals (ticket validator, mobile phones), almost never directly connected to any central server. Therefore the distributed components of the system – personal devices and terminals – must enforce security on local interactions, without relying on remote server checks.

We share many concerns with the **related work** about interoperability and multi-services with the smart-card community (Schwarzoff T. et al., 2003; eESC TB7, 2003) but, rather than working to promote a standard framework for applications using cards or other personal devices, we are mostly concerned with security assurance mechanisms. Existing approaches assume a total trust domain, whereas we want to make partial trust explicit.

5. CONCLUSION

In this paper we presented self-contained services and the need for true multi-services. The problem we face is how to build these multi-services using cooperative self-contained service platforms, sharing information only up to a restricted level, and solving the security issues related with the identification and authentication of users and with the manipulation of electronic contracts.

The goal of our work is to develop models and tools to produce technical assurances that allow the organizations to establish the partial trust relationship between them to deliver the new service. Other expected advantages are the clarification of the organizational roles, opening prospects for more rapid deployment of integrated service delivery.

REFERENCES

Anderson R., 2001. *Security Engineering: A Guide to Building Dependable Distributed Systems*, John Wiley & Sons Inc.

CEN, 2001. *Reference Data Model for Public Transportation, ENV12896 revised*. CEN.

CNA, 2004. *Calypso Web site*. http://www.calypsonet-asso.org/, Calypso Networks Association.

Durlacher, 1999. *Mobile Commerce Report*, Durlacher Research Ltd, UK, www.durlacher.com.

eESC TB7, 2003. *Open Smart Card Infrastructure for Europe, Volume 5, Part 3 – Multi-applications – Basic technologies for multi-application cards and systems***.** eEurope Smart Card Charter**.**

Guthery S. and Cronin M., 2001, *Mobile Application Programming Using SMS and the SIM Toolkit: Building Smart Phone Applications*, McGraw-Hill.

Laudon K. and Laudon J., 2002. *Management Information Systems - Managing the digital firm - Seventh Edition.* Prentice Hall International Editions.

Levy F., 2001. *Calypso Functional Specification for Ticketing*. Spirtech, Paris, France.

Patil B. et al, 2003. *IP in Wireless Networks*, Prentice Hall PTR.

Schwarzoff T. et al., 2003. *Government Smart Card-Interoperability Specification, Version 2.1*. NIST, USA.

Zoreda J. and Oton J., 1994. *Smart Cards*, Artech House Publishers.