A proposal for a payment system for public transport based on the ubiquitous paradigm

Carmelo R. García, Ricardo Pérez, Joaquín Caraballo, Francisco Alayón, and Gabino Padrón

Dpto. Informática y Sistemas, Universidad de Las Palmas de Gran Canaria, Edificio de Informática y Matemáticas, Campus Universitario de Tafira, 35017 Las Palmas , Spain
(rgarcia, rperez, falayon, gpadron)@dis.ulpgc.es

Abstract. Automatic payment systems (APS) play an important role in the productive activity of the passengers transport companies. The companies using APSs profit from an improved security and commercial speed and their clients from a reduction in the trip cost. We describe how to apply the ubiquitous paradigm in order to improve APSs and present an APS model that allow clients to use different mobile devices such as contactless smart cards, cellular phones or PDAs as means of payment. The system has the necessary mechanisms to be used in a combined way in different services contexts (public transport, parking, museums, etc). Suitable aspects of the system are the flexibility to implement different payment schemes, and the scalability to incorporate new mobile devices as means of payment. These characteristics are consequences of the system architecture, based on two main generic elements: the mobile device model and the user application model.

1 Introduction

The spread of mobile communication and information support devices is motivating the enterprises' interest in incorporating them as automatic payment systems. The use of those devices in the payment systems has some advantages: speed and comfort when accessing services, improved simplicity for tackling optimization of outstanding aspects of the management of services such as: security, access delays, availability, demand variation, and exploitation costs reduction because of the fact that expenses are shared with the clients, as they provide the devices to support payment. The development of those new payment systems poses some technological challenges, mainly due to the lack of standardization. A careful system design will allow the enterprises to adapt themselves in a non-traumatic manner to the wide variety of communication devices and models, and to face comfortably technological advances that will make possible new services. In this article, we describe an automatic payment system based on a variety of mobile communication and information support devices that are currently increasing both their use and their technological development.

2 Aims and requirements

Payment automation provides service-oriented enterprises with many benefits: simplifies the interaction of users with payment systems, allows the enterprise to customize the types of payment media and adapt them for the different client characteristics, improves fare system by optimizing information flows, increases security and fraud control, and decreases exploitation costs, by using resources provided by the clients themselves. Also, mobile devices versatility makes possible a greater services offer flexibility and their combination (transport with tickets for cultural and leisure activities, parking, etc). The development of this automation has some requirements that we can summarize as: availability of versatile payment devices, supporting a variety of modes and customization parameters, development of processing and communication mechanisms permitting us to reduce interaction to the minimum, and development of mechanisms guaranteeing data and transactions security. Nowadays, contactless smart cards fulfil rather well those requirements. They are being incorporated in the latest years into enterprises payment systems. Next qualitative step is being carried out by mobile communication and data support systems, as they make possible the progress towards more evolved payment systems. We believe that a payment system based on those devices can offer the following properties. Scalability; it is the ability to incorporate new payment functionalities means of payment, communication systems, and clients. Security; it is the ability to detect wrong transactions, both fraudulent and caused by technical or accidental failures. Maintenance easiness; it is the ability to detect and respond to operation failures of its elements. Also, it is the ability of its physical and logical elements to be easily updated. Robustness; it is the ability to work in adverse physical conditions, both due to environmental reasons and to a massive and continued use. Speed.; ability to carry out every transaction that is required in order to provide services access to the users at speeds that do not interfere with productive organization activity. Plain interactivity; it is the ability to permit the users to easily employ the means of access to the services.

In the next section, we will describe the most outstanding aspects of an automatic payment system based on mobile devices. This payment system is being developed to be used in a passengers public transport context. Passengers transport, in special in the public sector, is the economic activity where we can notice the most important advances in this field. Our payment system combines the acquired experience in the development of mobile information systems with ubiquitous computing ideas and concepts.

3 Description of the system

Before we describe our system, we explain some general aspects about classic automatic payment systems that will help to understand the design principles of the system. In the first place, we can identify in a payment system the following three elements. One, Users: the company that uses the payment system to provide a service and its clients. When several companies share the payment system, there is a third user: the system management authority. Two, applications; programs needed by the different kind of system users. We can classify the applications in three types: applications of the service provider company, client applications, and if the system is used by several companies, the multi-service management applications. And three, the platforms; these are the stations that host the applications. We can classify them in two types: non-mobile and mobile.

From a point of view of the management information systems theory, an automatic payment system is a transactional information system [1]. In our system the ubiquitous paradigm [2] was applied in order to use several types of mobile devices (contactless smart cards, cellular telephones and PDAs) as means of payment used by the clients. Also, this paradigm was applied to develop a general model of client applications; this model is independent of the mobile device used by the clients as means of payment. Figure 1 represents a general vision of our system. In this model the non-mobile stations are associated with the platforms used by the transport company. If there are several services providers companies integrated into the payment system, one of them is associated to the system management authority. The mobile devices are used by transport clients to obtain information about the service and to pay if. There are two kinds of models supporting payment transactions: a centralized model where the payment devices interact with a central host by means of a long distance mobile communication infrastructure, and alternatively, a non-centralised model where the payment devices interact directly with the mobile platforms installed on the vehicles using local communications infrastructures such as IEEE 802.11, Bluetooth, infrared, etc. Currently, we can find an example of payment system based on the centralised model in the public transport company EMT, that operates in the metropolitan area of Malaga (Spain), in this case the clients can buy the trips tickets and to charge smart cards using a cellular telephones by the SMS service. In our opinion, this scheme has the following objections. First, the client must support the cost of the SMS service (about 0.1 €), and second, the response time of the SMS service that forces to the client to realise an advance payment before to take bus. Our model is oriented to support a non-centralised model in order to resolve these problems. Another interesting example of payment system working in the public transport is the Calypso System, this system is working in Paris, Lisbon, Constance, and Venice, it is based on the intelligent contacless smart card as payment media, a consortium of 26 partners participate in this system [3]. Finally, to mention the HONG Kong Octopus card [4] used in Hong Kong as multi-service payment media to access to public transport, restaurant, supermarkets, pay phones, soft drink vending machines, etc. Over 7 millions of transactions are recorded on a daily basis, for a value over US$ 6.5 millions. In this kind of payment system which covers different companies and service is important to consider the cost of the recovery management; in general it is about 1% of the recovery.

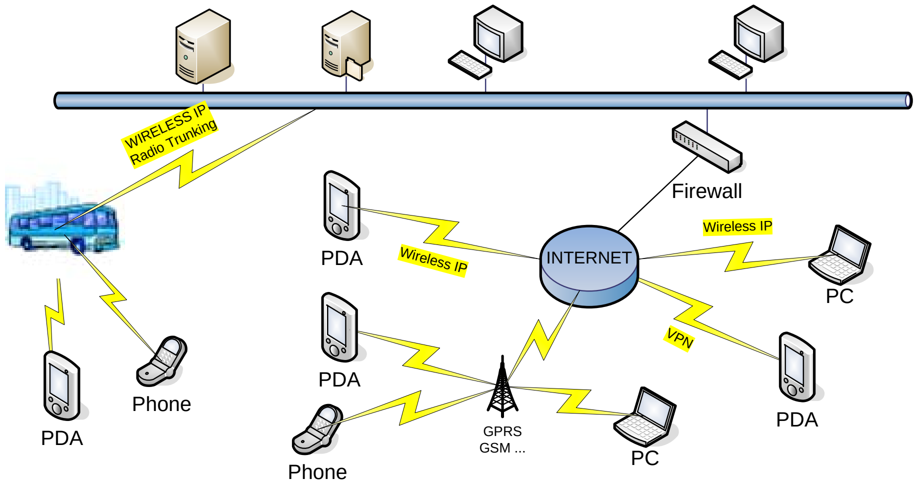


Fig. 1. General Vision of ubiquitous payment system for passengers public transport

From the point of view of the state of the art, the second model, a non-centralized scheme, has a greater interest, for this reason in this paper we concentrate on how we have designed this non-centralized model of payment system. In this design the ubiquitous paradigm has played an important role permitting us to achieve an integral, scalable and flexible payment system architecture.

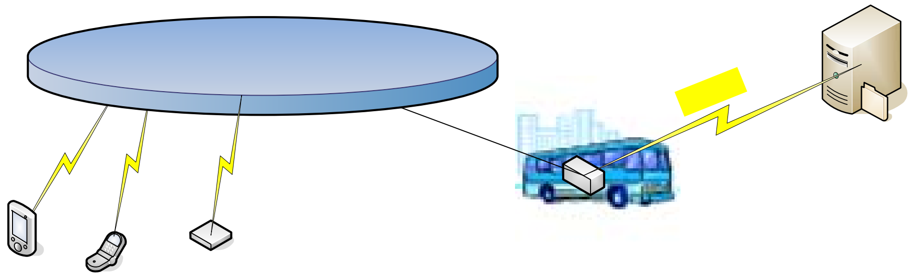


Fig. 2. Wireless local network supporting a non-centralized payment system.

The ubiquitous software is characterized by its high capacity of integration of the physical environment. As a consequence of this integration, the ubiquitous software is able to work in an autonomous and spontaneous way at different environments. For this reason, the ubiquitous software development must fulfil the following principles [5]. Border principle: The environments must be defined by information and not physical or technical limitations. Thus, the environment detection depends on information context borders instead of physical borders. These borders must not limit the interoperability between systems. Volatility principle: In ubiquitous systems we must assume that the number of users, devices and applications in a ubiquitous environment is unforeseeable. Therefore, it is necessary to specify a set of invariant functional principles which manages system execution.

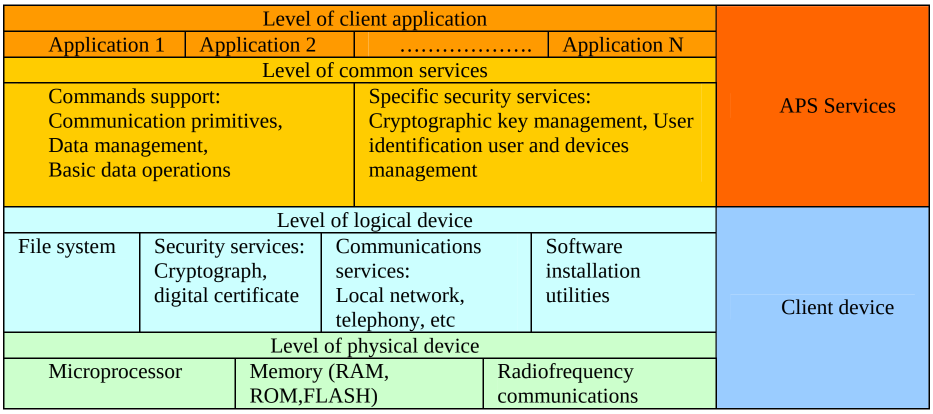
To apply these properties, our system is structured in two ambits. Common services ambit formed by all the elements that permit all the applications users to access to the different client services provided by the companies. In this ambit, we define the invariant functional principles of our system. User ambit formed by the user tools allowing the system interaction. Specifically, in our system these tools are the mobile devices used as means of payment by service clients. Next, we explain the most important aspects of these invariant functional principles that are: the model of client applications and context applications and the concept of virtual payment device.

3.1 Client applications and contexts applications

In our system, a client application is defined as a set of structured data and a set of commands for its manipulation. Basically, these commands permit us to perform: communications with other remote applications, simple arithmetic and logical operations and storage operations. The sets of structured data are composed of data units characterized by two properties: identification and type of access permitted. By means of these data unit we represent the different and relevant aspect of the client applications such as: client identifications, device identifications, general parameters of the payment system, specific parameters of the payment system oriented to the clients and payments accounting. A context application is associated to a specific service such as transport, parking, etc. A client application that permits the user to access to a specific service is associated to the corresponding context. In a multi-service payment system we can find different contexts. In each context, the associated application permits the client to pay the service in different ways depending on the parameters stored in the application data. The extreme case will be a payment based on personal characteristics of the client. The client application commands are executed following a common scheme:

1. Context identification: The local infrastructure sends context identification packets.
2. Context information request: When a client application identifies a context, it sends an information context request, producing an information interchange between the client application and the local infrastructure.
3. Data transformation: A subset of the client application data is modified and generated by the client application or by an application running on the local infrastructure.
4. Transaction confirmation: The client application confirms to the infrastructure the complete execution of the client application commands.

We can emphasize the data transformation step, which can run both on the client payment device, and on a specific station of the local infrastructure. Thus, the client application commands can be executed in a distributed way. This capability is motivated by several reasons: First, with this execution scheme the client applications are independent of the client devices capabilities. Second, in order to improve the security, we can ban the execution of certain operations on client devices. Third it allows us to support the dynamic nature of certain aspects of the payment systems.



Level of client application

Application 1 | Application 2 | ………………. | Application N

Level of common services

Commands support: Communication primitives, Data management, Basic data operations

Specific security services: Cryptographic key management, User identification user and devices management

APS Services

Level of logical device

File system | Security services: Cryptograph, digital certificate | Communications services: Local network, telephony, etc | Software installation utilities

Client device

Level of physical device

Microprocessor | Memory (RAM, ROM,FLASH) | Radiofrequency communications

Fig. 3. Model of virtual payment device

3.2 Virtual payment device

We have defined a virtual payment device in order to establish a common client applications execution support that isolates the specific characteristics of real client devices. It integrates the variety of technologies and functionalities used nowadays as means of payment such as contacless smart cards, cellular telephones, PDAs, etc. To define this model of generic payment device we have taken into account aspects and working principles of devices and products of the market, specially JavaCard [6] and Symbian operating system [7]. The virtual payment device is a virtual machine composed of four layers:

- Physical device layer: It is composed of the physical elements of the device. Its minimum requirements are: about 16 Kb of storage capacity and radiofrequency communications capability.
- Logical device layer: It consists of the software support provided by device's manufacturers. At this layer, some common services are provided: communications, cryptography, file system, etc.
- Common services layer: It is the first level supplied by our system. Basically it provides the client applications execution support and the specific mechanisms for security.
- Client application layer: It is composed of the different applications installed on the payment device.

3.3 Security

In general, the security is a critical aspect of any payment system. Thus, there are international specifications on the payment systems [8], specially we have considered the CAO recommendations about passwords security in contactless smart cards [9]. Considering that in our system the means of payment are supported by non-proprietary technology devices such us PDAs and cellular telephones, security is a key issue. We have distinguished three main security matters. First, authentication of client application; a client application can not be replicated, for this reason any client application has to be associated to a unique user and a unique payment device. In our system, every client application verifies that it is running on the device where it was installed. Thus, a basic requirement of the payment device consists of providing a service to get the unique identification key associated to the device at run-time. Second, access control to the applications; any access to data structures and application commands have to be done by authorized users. If an unauthorized access is detected, the transaction has to be rejected. And finally, transactions control; unauthorized client applications must be detected and rejected by the infrastructure. Another transactions control aspect consists of the detection of incomplete transactions. When it happens the system have to complete the transaction by itself. Finally, the system has to permit auditory processes that allow the company to verify the fulfilment of the security principles. To achieve this requirement it is necessary the traceability of clients operations.

4 An example for public transport

In this section, we illustrate how the system has been applied to the public transport context. Specifically we explain how to implement two kind of electronic tickets. Ticket of fixed travels: It consists of finite number of trips with departure point and arrival point that can not vary. Every time the client uses this ticket, one trip is decremented. Transport electronic money: It consists of an amount of money that can be spent to pay an arbitrary trip. The use of the electronic tickets follows these steps:

1. Context detection: The application is waiting for the context detection state. Before it is reached, the application can request some information. For example to use the transport electronic money, the application must request the destination point.
2. Authentication of the application: This step consists of sending a context authentication packed in an element of the infrastructure. This permits the client application to leave the waiting state.
3. Context information request: In this step the client application requests some context information in case it is needed to run any command.
4. Validation: The client application sends a data packet and commands packet to an element of the infrastructure to validate the application.
5. Confirmation: The validation element of the infrastructure sends to the client application the updated data.

6. Registered: The client application registers the updated data in its data structures stored in the payment device memory.
7. Transaction notification: The client application sends a packet of complete transaction notification to the infrastructure.

The data used by these client application examples are the following. Client personal data; this set of data consists of at least a unique identification key associated to the clients and a unique identification key associated to the application. Electronic ticket configuration data; they specify the type of electronic ticket and other specific parameters needed by the electronic ticket. And finally, movements history registering all use of the ticket.

6 Conclusions

In this paper we have described the main aspects of an automatic payment system for public transport. This system can use as means of payment different types of mobile devices: smart cards, PDAs and cellular telephone. This outstanding capacity improves the traditional payment systems used in the public transport context. Another outstanding property consists of the reduction of the operation costs thanks to two factors: the use of local communication infrastructures and the use of general purpose devices, avoiding devices based on proprietary technology. Finally, we have based our model on the ubiquitous paradigm, in order to achieve the initial objectives of the system; specifically regarding flexibility and scalability. As a final consequence we can affirm that this paradigm provides techniques and ideas which can improve the traditional payment systems.

References

1. Caddy, I.: Will the real MIS please stand up? WIT Transactions on Information and Communication Technologies, Vol. 32. WIT Press (2004) [69-78].
2. Weiser, M.: The computer for the 21st century. IEEE Pervasive computing, mobile and ubiquitous systems, Vol. 1, num. 1 (reprinted with permission Copyright 1991 by Scientific American Inc). IEEE Computer Society (2002) [18-25].
3. Community Research & Development Information System: http://cordis.europa.eu/telematics/tap_transport/research/projects/calypso.htm
4. Smart Card Alliance, Hong Kong Octopus card: http://www.smartcardalliance.org
5. Kindberg, T , Fox,, A.: System Software for Ubiquitous Computing, IEEE Pervasive Computing. Mobile and Ubiquitous Systems, Vol. 1, nº 1, IEEE Computer Society (2002) [70-8].
6. SUN Microsystem. Java Card Technology. http://java.sun.com/products/javacard.
7. Stichbury, Jo. Symbian OS explained. Symbian Press (2004).
8. ISO/IEC 14443 Proximity cards. International Standard Organization (2001).
9. ICAO Recommendations. Report of the 33rd meeting of ISO/IEC JTC1/SC17/WG8 (rev. 1),(2004).