easyTransport: An Interoperable and Secure e-ticketing Model based on Contactless Smart Cards

Antonio F. Gómez Skarmeta, Gregorio Martínez Pérez, and Carmen M. Yago Sánchez

Abstract—***The introduction and use of electronic ticketing (e-ticketing) is an element of key importance for the good deployment of the public and private transport area across the world. In fact, it not only produces benefits for passenger transport operators, but it also creates an infrastructure, especially in urban areas, which can be used easily by other sectors. The use of secure infrastructures to support the payment and management of such kind of e-services is a growing area of interest. This article provides an overview of the current state of the art regarding e-ticketing systems, mainly in Europe, and describes a new proposed architecture, named easyTransport, based on the use of contactless smart cards, and where important items for an e-ticketing schema are in place, such as, ease of use, interoperability, standard-based, and multi-application.***

Index Terms—***contactless smart card, e-payment, public and private transport, e-ticketing infrastructure, security***

1. Introduction and Motivation

MARKET globalization, the development of the Internet and the new information technologies have established a new scenario for business. Passenger transport environment is not an exception. Although passenger transport services are a key factor in the development of modern cities, transport operators have to deal with a complicated fare management, traffic congestion, and final customers getting more and more concerned about delays. The use of technological tools may alleviate these problems, namely an automated e-ticketing system based on contactless smart card technology. These systems have the following features:

- Quick operation. This feature is derived from contactless technology whose transaction time is about 150-400ms, much lower than magnetic stripe cards (2 or 3 seconds) [1]. This is a key factor for users' acceptance of e-ticketing systems because they usually have to wait in a queue.
- Ease of use. To operate the card it is only necessary to bring it near the card reader even without taking it out of the wallet.
- Security and Privacy. Contactless cards are more difficult to duplicate than magnetic stripe cards [2] and it is also possible to define access rights and encryption mechanisms so that information is only accessed by authorized entities and the operations made with the transport card.
- Customized fare media. It is possible to offer more flexible tariffs and diversify the kind of tickets and passed offered to final customers.
- Better management. An e-ticketing system leads to a better usage of data. Then, it is possible to have a better planning, more accurate clearing and loyalty programs.

Because of these advantages, all over the world, e-ticketing systems based on contactless smart cards are being deployed, most of them using proprietary technologies. European cities like Paris or London already have e-ticketing systems. In Europe their wide implantation is expected before 2008 [3].

In the European Union, the interest for these e-ticketing systems not only comes from transport operators but from institutions. There are initiatives at national level like ITSO (Integrated Transport Smartcard Organisation) [4] in UK to provide a platform and tool-box for the implementation of interoperable contactless smart card public transport ticketing and related services and at E.U. level like eESC (eEurope Smart Card) [5] a European Commission initiative to promote the use of smart cards including e ticketing in transport applications.

Moreover, the standardization bodies are concerned about the necessity of developing standards at both technological and application level. ISO (International Standards Organization) has developed ISO 14443 [6][7][8][9], which standardizes the contactless technology and the

Manuscript received June 30, 2004. This work was supported in part by the Spanish Ministerio de Ciencia y Tecnología (MCYT) by means of the SAM project (TIC2002-04531-C04-04) and the Spanish Ministerio de Fomento, within its R&D 2002-2003 Project Framework in the Transport field.

T. C. Authors are with the Departamento de Ingeniería de la Información y las Comunicaciones, University of Murcia, Spain (e-mail: skarmeta, gregorio, carmen@dif.um.es).

European standardization body CEN (Comité Européen de Normalisation) is making an effort to obtain normative at application level.

In this context, we have considered interesting joining to the general effort with the development of a non-proprietary e-ticketing model, based on existent standards. This eticketing model, that we have called easyTransport [10] provides efficiency, reliability and security to fare collection processes without real changes in the infrastructure of transport operators, so migration has a low cost, as a real implementation has shown.

This model is suitable for any kind of passenger transport services, so it makes sense to offer the possibility of integrating several services in the same transport card. This is an added feature of our design: it allows transport operators from a geographical area to integrate their own prepaid fare media in a shared transport card.

This model also benefits from the advantages of a non-proprietary system: transport operators may analyze its specification to decide if it compatible with their current system, and any manufacturer may build components (e.g. smart cards) for the system; therefore operators are not tied to a proprietary technology or solution.

This article first describes the state of the art regarding e-ticketing systems. Then explains the easyTransport model proposed and then, how it was applied to a car park. Finally we conclude the article with our remarks.

2. State of the Art of e-Ticketing Systems in Transport Scenarios

Contactless smart card technology has led to the development of e-ticketing systems for public transportation based on it. These systems are substituting traditional ticketing systems (based on paper and magnetic stripe). Here, users introduce their tickets (and transport contracts) in their card and access the services through a touch and go system. The rapid growth and acceptance of these systems is not surprising because they present several advantages versus magnetic stripe cards based systems, as those commented above.

Because of these advantages, big scale implementations in Europe (Paris, London, Berlin, Rome or Moscow), America (San Francisco, Mexico D.F. or Santiago de Chile) or Asia (Seoul, Hong Kong, Singapore or Tokyo) are already working or will be in a short time.

But not only public transportation is implementing solutions for payment based on smart cards. The number of transport services using it is increasing, reaching for example touch and go road tolling systems, payment parking systems or car-sharing services.

The card is usually issued by an operator or by an association of operators, and sometimes it allows the access to different services (for example in Bremen, car-sharing users may use their card to access public transport [11]) but it is because of an agreement between operators, not for the existence of interoperability. So, it is perfectly possible that users have to use one card for each transport service they want to use in their city.

In fact, from here to 2008 it is expected that e-ticketing schemes will be broadly introduced in Europe, and there is a high risk of market fragmentation [12] if research laboratories, companies and standardization fora do not consider interoperability as one of the main features in their designs.

A. Interoperability and Standardization

Interoperability means that users could access to different transport services owned by different operators using a compatible medium (e.g. smart card). Thus interoperability is a key feature to get integrated payment systems. But to achieve interoperability, both technological and application standards are required. The standardization process is still beginning, while the technology is partially standardized although there are not application standards yet.

These e-ticketing systems usually employ proximity cards. These cards communicate with the reader by radio frequency within a distance less than 10 cm. The card physical characteristics and card-reader communication protocol is standardized by ISO 14443 1-4. Card commands and memory structures are not standardized. Some manufacturers use ISO 7816-4, which is currently the most common format, but others utilize their own proprietary systems. Security protocols are normally proprietary [12].

Europe is conscious of the necessity of standards. The European Commission has launched the eESC (eEurope Smart Card) initiative to promote the use of smart cards including e-ticketing in transport applications. Moreover, the European standardization body CEN (Comité Européen de Normalisation) is making an effort to obtain normative at application level; for example CEN/TC 278 WG 11 is working on both PrEN 1545 (evolved from ENV-1545) whose scope is the coding of data elements that e-ticketing is using, and prENV IOPTA which defines how the data defined in PrEN 1545 is structured.

There are also national initiatives to develop interoperable ticketing specifications; for example Norwegian Public Roads Administration has

published a preliminary version for interoperable electronic ticketing system [13] and ITSO [4], a British association of transport operators supported by the government, is developing specifications to provide a platform and tool-box for the implementation of interoperable contactless smart card public transport ticketing and related services in the UK.

B. State of the Art Summary

There is an important migration from traditional ticketing systems (based on paper and/or magnetic stripe cards) to e-ticketing systems. Actually, in the next coming years, it is expected the massive implantation of these systems in Europe for public transportation. But these e-ticketing systems are also useful for other transport services like road-tolling or parking. So, giving the user the possibility of integrating these services in a single card is a good opportunity to provide an added value for both operators and users. It could be even the first step for integration of e-services belonging to different environments like e-government, e-health or access control.

At this moment, cards usually only contain fare media marketed by an operator or an association of operators. In this context, we consider that a step that facilitates the transition from a single-operator e-ticketing scheme to a multi-operator e-ticketing scheme with shared fare media is the development of a efficient, reliable and non-proprietary e-ticketing model permitting transport operators to share a single transport card in a secure way at the same time they maintain their independence (i.e. each transport operator may have its own fare media and management processes). This is the motivation for our proposal of an interoperable e-ticketing model, that we have called easyTransport.

3. THE EASYTRANSPORT E-TICKETING MODEL

In this section, we introduce easyTransport, our design proposal for a non-proprietary and interoperable e-ticketing system based on contactless smart card technology for transport services such as public transport, car parks or road tolling. This e-ticketing system allows transport operators to have a better fare collection management as well as to offer a better service to final customers. The easyTransport model has the advantages of e ticketing systems described above such as quickness, flexibility, security or easiness of use. Moreover, our design offers also other interesting features:

- Non-proprietary. This feature avoids the dependency of operators from software and hardware providers and manufacturers, and allows transport operators to have a complete knowledge of the easyTransport e-ticketing model.
- Oriented to passenger transport services.
- Shared transport card. This feature allows transport operators from a geographical area to collaborate to have a shared transport card, offering users the possibility of storing in a single transport card, prepaid fare media for different services defined by several operators.

The easyTransport model is also being developed considering that, in the future, it may be integrated in a multi-application city card, which might be used for the e-services offered in a city such as access control, health care or e-government.

A. Actors involved in the easyTransport Model

The different actors interacting in the model, whose relationships are depicted in Figure 1, are:

- Transport operators. Companies offering transport services. These services may be related to mass transport like urban transport, or to user-oriented services like car parks or road tolling. These operators group in alliances to implement the model in a geographical area and offer a shared transport card.
- Users. People who use the transport services offered by operators. They have a transport card, which stores their tickets.
- Retailers. Commercial establishments (for example kiosks), which have an agreement with transport operators to distribute their transport card or reload their prepaid fare media.
- Hardware and software providers. Companies, which provide to the operators hardware and software, which is compliant with the model.

In our model, there is also another special actor, the *easyTransport Authority*, an independent entity creating the non-proprietary specifications of the model. It is also in charge of admitting and supervising the alliances between different operators.

The easyTransport model is implemented by alliances of operators. Each operator deploys its own e-ticketing system but its transport card is valid for all the e-services offered by any operator member of its alliance. These alliances are independent one from another but the easyTransport authority supervises all of them in order to provide the general security of the alliance, and guaranteeing that cooperation is not a risk for them. Transport cards belonging to different alliances are not compatible.

B. The easyTransport e-Ticketing System

The easyTransport e-ticketing system follows a front-office/back-office structure (see Figure 2) where the front-office groups all elements which interact with users, and the back-office processes and stores all the transactions made in the front-office. Both entities are explained in details in the next two sections.

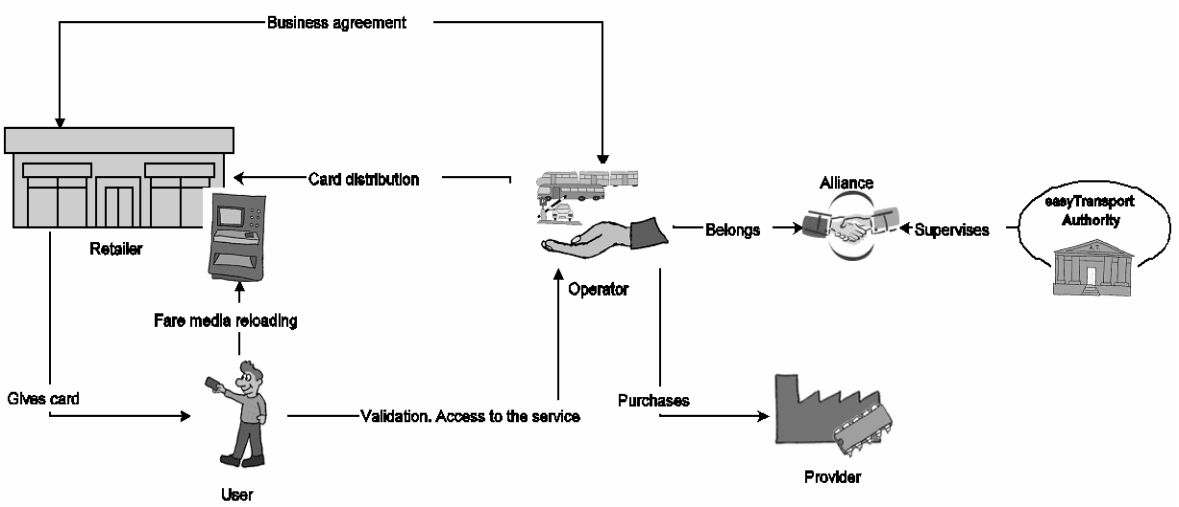

Figure 1 Actors involved in the easyTransport model and their relationships

1) Front-Office

The front-office makes all operations requiring interaction with users. Its two main components, because they are always present in every easyTransport implementation, are:

- Vending machine. It is used to introduce and reload prepaid fare media in the transport card and also to consult the state of the transport card.
- Validator. Users access the services by bringing the transport card near the validator, which selects the adequate fare media for the service, registers the transaction, and if it is the case, decrements a counter. This process is called validation. In certain services, like car parks, it is necessary to repeat the validation process to end the service (double validation).

In addition to these main components, there are two auxiliary components, which have human presence: the window and the inspector. The former has the mission of serving the users by giving them information about the system, answering their questions and solving any problems they could have. The latter is in charge of checking if the users are making a correct use of their transport card. He or she carries a device (for example a PDA) to interoperate with the transport card. These two auxiliary components can or cannot be present in the e-ticketing system depending on operator necessities.

Users interact with the front-office through their transport card, so a special attention has been paid to its design. This card is compliant with the ISO/IEC 14443 proximity contactless smart card standards and contains the prepaid fare media and data structures required to manage and secure them. These data structures take in mechanisms for allocation of new products, selection of the right product, checking of data integrity (such as an electronic signature or cyclic redundancy codes), backup to recover the data from a failed transaction and security such as access key or access rights.

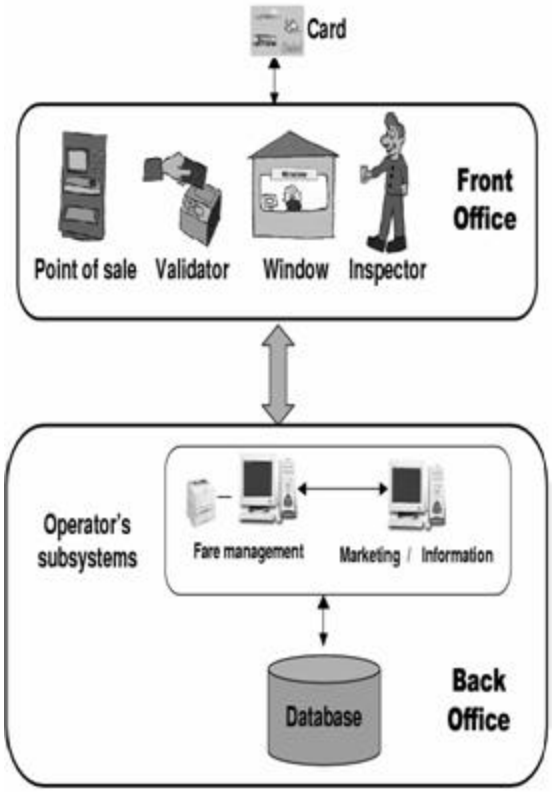

Figure 2 easyTransport e-Ticketing System

In order to provide the possibility of sharing the transport card, its memory is divided in common blocks shared by all operators of the alliance to store common information and private blocks specifics from each operator to store its fare media.

2) Back-Office

The easyTransport model does not define the way the back-office is organized because we consider that is strongly dependant from the business model and objectives of operators. Then, if we defined a fixed back-office, the model would not be able to fit the requisites of the operators or would suppose a disproportionate cost. However, in order to attend user petitions and for error recovery purposes, every back-office component in the easyTransport model has to store, at least, all transactions made by the front-office for either a year or the period fixed by the laws in case it should be higher.

The front-office/back-office communication may be done in an on-line or off-line way and using different media like GSM, the Internet or even magnetic support. However privacy and data integrity must be always assured. If the Internet is used, the channel must be secured and we recommend the use of public key cryptography, with similar experiences to those detailed at [14].

4. A CASE OF STUDY: EASYTRANSPORT MODEL APPLIED TO A CAR PARK

In this section we describe how the easyTransport e-ticketing system is currently implemented in a public car park, and what was the perception of final users and the cark park managers and employees regarding the use of this new system.

The goal of this real implementation was, without supposing significant changes in the car park operation, to implant the system to provide higher transaction speed because of contactless technology, flexibility due to higher storage capacity of smart cards, better fare management system as a consequence of the registration of all operations, and security as a result of communication encryption, access rights and the use of a public key infrastructure.

The car park initially offered two kinds of passes: a purse-pass oriented to sporadic users, which used a closed electronic purse and a temporary-pass oriented to habitual users who paid for a limited period of time.

The real implementation of the system indicates that users are quite proactive to use these new set of contactless technologies, mainly because they have the possibility of having faster transactions and they can use the same smart card for several services inside the car park and in the near future outside it (i.e. busses, trains, etc). Other considerations, such as, higher level of security are not very much of their interest, but are really sound to the company running the car park. However, the contactless manufacturer initially selected for the first real prototype provided some problems regarding working distances (no more than 7-8 centimeters); in fact, the driver in the car needed to be quite near to the validator to open the barrier, which supposed an important drawback for final acceptance of the system. It was solved with a new manufacturer, who provides higher smart card readers for the same contactless technology; thus, the same smart cards are used, but now with a working distance of around 20-25 centimeters, which is considered as acceptable by the final users and the car park managers and employees.

C. e-Ticketing System Architecture

The car park final implementation is shown in Figure 3 and it describes the LAN interconnecting the main elements (vending machines, and validators) and the window commented before. The main elements have the following functionality:

- Entry validators. There is an entry validator in any of the entrance gates of the car park (3 in the real implementation). They check the transport card looking for a valid product and register the entry time in both the card and the device. If one car driver has several cards (from several easyTransport implementations), the system selects its own card according to a product ID and a symmetric key. When these operations have been carried out, the entry barrier is opened.
- Exit validators. There is an exit validator in any of the exit gates of the car park. They register the exit time in both the card and the device, and if the user has a purse-pass they decrement the correspondent amount from it, and open the exit barrier.
- Vending machines. They are placed inside the car park and have an auto-explicative graphical interface in order to allow users to reload their passes and to consult their state (for example amount remaining or period of validity).

These operations have to be known in real time by a central element due to the necessity to know the state of the car park, i.e. the number of free places. In this architecture this function is performed by the window, which then it is not merely an informative element but becomes the core manager of the system. Then, besides being the adequate place to introduce the system to users and to solve their problems, the window

controls the car park state and orders the entry validators not to open the gates if the car park is full. To do this, the window needs to know the transactions made by the main elements. After this, the window sends all these data to the back-office, using SFTP with public key authentication as the main communication protocol.

The car-park security is oriented in two ways: the infrastructure must be protected from system failures, as well as from non-authorized access from the outside. To deal with system failures, the transaction registry is backed up on a secondary server, which provides redundancy to the architecture.

Administratively scoped multicast is used to ensure that both the primary and the backup servers receive the same information about the transactions being made. To prevent unauthorized access from the outside, the networked components of the architecture use private addressing (although the window has also a public address to communicate with the back-office).

These security levels and the flexibility of the final system were considered as the main advantages of the final implementation from the cark park managers and employees perspective.

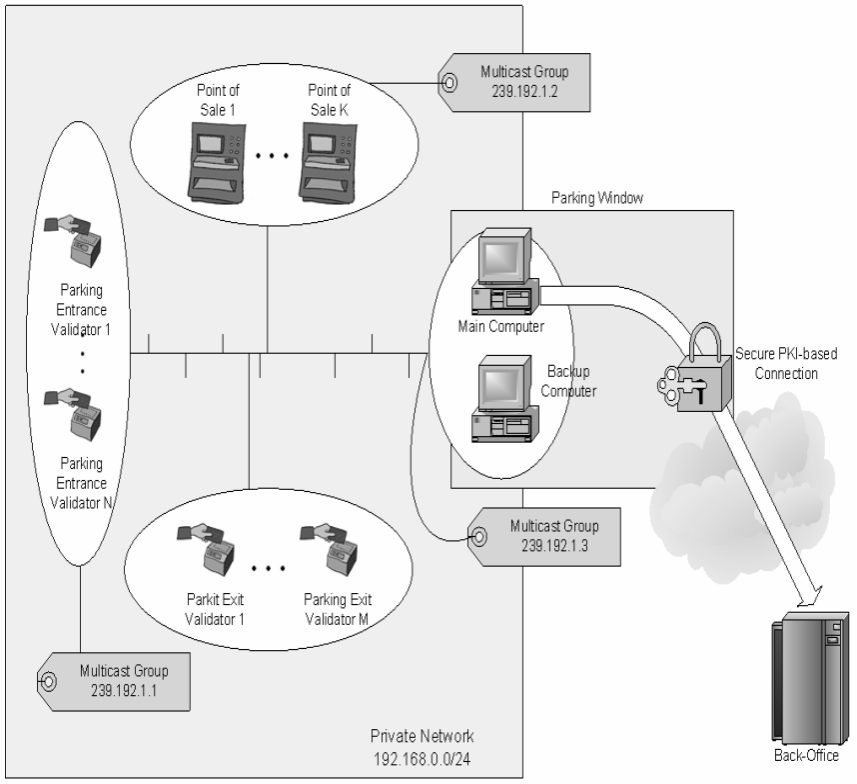

Figure 3 easyTransport car park infrastructure

5. CONCLUSION

In passenger transport environment, e-ticketing systems based on contactless smart cards are being deployed across the world. In particular, in the European Union, there is a special interest at both private and institutional sectors. Bodies of standardization are also involved in the development of normative for these e-ticketing systems: ISO has standardized the technology through ISO 14443 and CEN is working on application standards.

In this context we have proposed a non-proprietary interoperable e-ticketing system called easyTransport based on contactless smart cards and compliant with the existing standards. This system provides the e-ticketing advantages such as quickness, flexibility and security; moreover, it adds additional features: it is non-proprietary, can be implemented in different transport services (enabling intermodality), and allows transport cards to be shared by different operators.

The easyTransport e-ticketing systems are based on a front-office/back-office two-tier infrastructure whose implementation has been successfully tested in a car park.

Future work is oriented to integrate the easyTransport e-ticketing system in a city card multiapplication, which will provide besides eticketing several e-services such as e-health or e-government.

REFERENCES

[1] Pérez, G., "Telemática un nuevo escenario para el transporte automotor," *CEPAL –United Nations*, 2001.

[2] -, "Open smart card infrastructure for Europe," eEurope Smart Card, *eESC TB9 Public Transport*, 2003, Vol. 1, Part 3.

[3] -,"CWA 14838-1. Facilitating Smart Card Technology for Electronic Ticketing and Seamless Travel - Part 1: EU Policy and User Requirements," *CEN, European Committee for Standardization*, 2003.

[4] -, ITSO Integrated Transport Smartcard Organisation, http://www.itso.org.uk, 2004.

[5] -, eESC eEurope Smart Card, http://eeurope-smartcards.org, 2004.

[6] -, "ISO/IEC 14443-1 Identification Cards - Contactless integrated circuit(s) cards Proximity Cards Part 1: Physical characteristics," *ISO International Standards Organization*, 2000.

[7] -, "ISO/IEC 14443-2 Identification Cards - Contactless integrated circuit(s) cards. Proximity Cards Part 2 Radio frequency power and signal interface," *ISO International Standards Organization*, 2001.

[8] -, "ISO/IEC 14443-3 Identification Cards - Contactless integrated circuit(s) cards. Proximity Cards Part 3: Initialisation and anti-collision," *ISO International Standards Organization*, 2001.

[9] -, "ISO/IEC. ISO/IEC 14443-4 Identification Cards - Contactless integrated circuit(s) cards. Proximity Cards Part 4: Transmission protocol," *ISO International Standards Organization*, 2001.

[10] Yago Sanchez, C. M., "easyTransport: proposal of an e-ticketing model for passenger transport," Master's thesis, Computer Science Faculty, University of Murcia, 2003.

[11] -, "Bremen Paper. Transport and Car-Sharing: together to the better," *UITP – Union Internationale des Transports Publics*, 2002.

[12] -, "CWA14838-1. Facilitating Smart Card Technology for Electronic Ticketing and Seamless Travel – Part 2: Deployment of Smart Card Based Interoperable Ticketing Systems," *CEN, European Committee for Standardization*, 2003.

[13] -, "Specification for Interoperable Electronic Ticketing System," *Norwegian Public Roads Administration*, Preliminary version, 2003.

[14] Gomez Skarmeta, A. F., Martinez, G., Cánovas, O., Lopez, G., "PKI services for IPv6," *IEEE Internet Computing*, Vol. 7, No. 3, pp. 36-42.