7TH WCTR
SYDNEY AUSTRALIA
1 9 9 5

**TOPIC 18**
ENVIRONMENT AND
SUSTAINABLE MOBILITY

# IMPLEMENTATION ISSUES OF ELECTRONIC PAYMENT SYSTEMS FOR PUBLIC TRANSPORT SERVICES: A FINNISH CASE STUDY

RANDALL PEARSON
UNICOM Ltd
Pohjantie 3
02100 Espoo FINLAND

SAKARI RANTA
UNICOM Ltd
Pohjantie 3
02100 Espoo FINLAND

## Abstract

This paper addresses key issues relative to implementing and operating electronic payment systems for transport services. These issues include system equipment technology, clearing transactions, data security and institutional requirements. The example of an electronic payment systems for public transportation in Finland demonstrates the need to understand these issues and provides a case study of fulfilling the requirements they pose.

## TRANSPORT SERVICES

### The need for electronic payment in transport

Challenges of pursuing technical standards, achieving system compatibility and interoperability and the need for systems integration, go to the heart of implementation issues connected with the development of electronic payment systems in transport. Success in meeting these challenges can lead to obtaining the benefits offered by these systems and promote sustainable mobility within the transportation industry.

Electronic payment offers the potential to reduce risk and the labor intensive requirements of cash handling, the possibility to reduce congestion at toll plazas, and improve levels service in transport. Electronic payment can also serve to facilitate intermodality by making transport services more convenient. Administrative benefits to operators of transport systems that use electronic payment consist of expanded opportunity to accomplish systems integration. Further benefits are found in the possibilities to use electronic systems to as a component of total information management. Both systems integration and information opportunities offer the potential to improve operational efficiencies which in turn can contribute to enhancing the performance offered by various transport service providers.

### The Finnish example of public transport

The Finnish Ministry of Transport and Communications has pursued a detailed analysis of electronic payment systems for use in public transportation (FMTC 1994 No .1). The results of this study were successful enough to result in the development of a full specification for an Integrated Circuit Card (ICC or "smartcard") electronic payment system (FMTC 1994 No. 4). This specification ultimately formed the basis of plans for a full scale national implementation of a smartcard based electronic payment system for inter-city public transportation. Descriptions of this system and its elements, plus reference to the system specifications, along with accounts of system implementation progress form the basis of this paper.

Although the case is specific to public transport, it is the position of the authors that the implementation issues encountered in this case provide extremely relevant and valuable information for anyone embarking upon the development of an electronic payment system for transport services. The essential implementation issues encountered in this case could reasonably be expected in any implementation of electronic payment for transport and therefore the lessons learned are presented here for the benefit of other transportation professionals.

### Implementation issues

Although there is a great deal of detail in the subtlety and precision of implementing specific electronic payment systems, the approach of this paper will be to address four primary categories of implementation issues. The four categories addressed in this paper are methods of payment, security, clearing of payments, and institutional issues. Presentation of these issues here is by no means exhaustive. However, the attempt is made to raise professional awareness and alert them to the need to find resolution on these issues in order for their implementation to be effective and successful.

## METHODS OF PAYMENT

This section examines alternative payment methods considered by the Finnish Ministry for Transport and Communications. At the outset, the assumption was made that usage of smartcards would be studied based on their utility in serving electronic payment, and the clearing of system transactions. Different card technologies are reviewed here to compare their functional capabilities.

### Magnetic stripe cards

The magnetic stripe card was developed to replace coins and bills. This technology is mostly used for automatic teller machines (ATM) and credit cards. There are three magnetic tracks situated on the card where the first two tracks are read only and the last track is for reading and writing. Magnetic stripe cards normally have a relatively low byte storage capacity which consequently makes the card unsuitable for more demanding tasks. None the less, there are many positive aspects for the magnetic stripe card.

It provides an easy method of payment and it is already widely used. The cards are cheap to produce and they have a reasonable degree of security which represents an effective deterrent against the amateur criminal. One can handle transactions electronically which lowers processing costs. To be able to use the magnetic stripe card safely there must be some security checks done. These are checking for invalid cards and identifying the right user through a personal identification number (PIN). This also requires that the card reader has to be on-line with a central computer. There has been some discussion of in-terminal authorization for lower value transactions in case of on-line failures. Since it is possible to change the information stored on the card with appropriate equipment some surveillance of the magnetic stripe cards must be done. This has resulted in that the banks have phone lines for blocking the use of lost cards. Also the careless storage of the PIN can result in the misuse of the cards.

### Smartcards

The small capacity and the flaws in the security of the magnetic stripe card led to the research and development of other card technologies. During the early 1970s the French journalist Roland Moreno conceived the idea of embedding a programmable device within a credit card. He registered the first patent in France in 1974.

Moreno was not the alone in recognizing the significance of the microchip-technology credit cards. A Japanese inventor, Dr. Kunikata Arimura, had applied for patents for the world's first integrated chip card a few years earlier in March 1970, but he limited the patent to Japan only. His process which he defined as the 'Arimura Card' was 'a plastic card incorporating one or more integrated circuit chips (ICC) for the generation of distinguishing signals'. Arimura developed the first contactless card in 1978 (Bright 1988).

There are several types of smartcards, the names of which have not been universally agreed upon. Basically the cards can be divided into contact cards and contactless cards. Contact cards have to touch the card reader whereas the contactless can transact with the card reader at a distance. The smartcard definitions presented in Table 1 are those adopted by the Finnish Ministry of Transport and Communications.

*Memory cards*

A memory card can be either a contact or a contactless card. Technically, the memory can be set up either for a one time only write capability or it can be set up to be rewritable. Memory cards that are set up to be written only once cannot be changed after the initial write. This is usually the case with telephone cards. A public phone uses calling units from the card during the phone call until all the units have been used leaving the card useless.

Rewritable memory enables the recharging of additional payment units so that, for example, when the payment units on the card are running out, a passenger can go to a sales point to load more units into a card's rewritable memory.

Table 1 **Definition of different card types**

| Card Type | Definition |
|---|---|
| Smart Card | a plastic card which contains an I/O interface and one or more integrated circuits incorporating memory and possibly also a control logic, or a microprocessor |
| Memory Card | a smart card with an integrated circuit containing memory and possibly control logic, but no processor |
| Microprocessor Card | a smart card with an integrated circuit containing a processor and memory |
| Contact Card | a smart card (either a memory or a processor card) which communicates with the external world through contact on the card surface |
| Contactless Card | a smart card (either a memory or a processor card) with airborne communication with the external world |

*Microprocessor cards*

Processor card's microprocessor and memory are implemented by an integrated circuit, which communicates with the external world through a serial type I/O interface. The processor cards usually contain an operating system. This operating system, called the mask, is implemented in the integrated circuit's read only memory (ROM). Manufacturers provide the cards with a standard mask, but the mask can be designed for specific purposes of electronic payment systems. One of the more common functions of the mask is to perform the encryption for memory protection. The key is only known to the manufacturer of the cards and of the card readers. However this key can be set up so that the system owner/operator can change the key at the time of system initialization.

*Contact cards*

Contact cards communicates with the external world through contacts on the card's surface. The contact consists of eight pins where the data communication is performed serially through one of the contacts. Power, ground, reset and clock are connected through the other pins. Since the card is in contact with the card reader, no power source has to be implemented on the card itself. Thus the card will only be operational when in contact with a card reader.

*Contactless cards*

Communication of contactless card is airborne with signals transferred through an inductive or capacitive coupling. Power must also be transferred contactlessly, usually through an inductive coupling. This is a form of dedicated short range communications (DSRC), an area where there is a lot of activity for technical standards.

One can roughly divide the contactless cards into two categories based on the proximity of the contact. The close proximity cards can only be read at a distance of some centimeters. Other cards can be read at a distance of a meter or more.

## Technology selected for the Finnish electronic payment system

The microprocessor card was selected for its flexibility and the high degree of security attainable. Tests performed in Finnish trials showed that the use of contactless cards would improve speed of handling city traffic passengers, but on intercity journeys this would not have any significance. Additionally, this technology was selected because the cards' operating system make it possible to create additional applications which extend to different use. In the Finnish perspective, it is worth the larger step to accept a higher technology, rather than accept technology that would soon exhaust its limits. This perspective supports further development of application which can be integrated into the IC card.

## SECURITY

Complex systems, such as electronic payment, are only as secure as the weakest link in the whole chain. The following describes the information flow in this payment system and identifies those points that require special attention regarding security.

The basic transactions are created at the card readers or at the point of sale where the card is obtained or reloaded with payment units. These transactions are transmitted for local clearing electronically. Later the compressed data of the cleared transactions are sent to the central clearing for monetary apportionment and also for use in statistical analysis as well as system management.

### Data

One can distinguish three situations in the information flow of the system where the security needs special attention. The first situation is when the information contained on the smartcard is created. In order to reach an acceptable level of security the data is provided with an electronic encryption. The data can also be encrypted with the DES-algorithm or the RSA-algorithm (Rivest, Shamir, Adleman) can be used for asymmetric encryption. It is important that the integrity of the data is preserved and that any intentional or unintentional changes to the data will be recognized.

The second situation that needs attention is the data communication. Electronic transmission is used for the communication between the levels in the clearing system. The advantage of using electronic transmission is that it can be set up with its own protocol which provides a high degree of security and reliability. The protocol performs the checking of changes in the data sent, the resending of corrupt data packets and more. This type of protocol is also the subject of some current standardization efforts.

The third situation that needs attention with respect to security are the databases contained in the payment clearing process. In the Finnish system, only authorized persons have access to the database and only a select few have rights to change the information in the databases. The database users are grouped into different access groups and the usage of the database is strictly controlled.

### Communication

Apart from the file transfer protocol of the electronic transmission, there are no transmission protocols within individual levels of the clearing system. The higher level in the clearing system has the responsibility to control the audit trail of the transactions of the lower levels. Duplicate and missing transactions must be found and corrected. The closer to the origin the control, is the faster the errors will be detected and corrected. It is however, always possible to reconstruct the transactions in the case that a transmission fails. In case the communication does not function at all, it is also possible to transfer the data on a disk. The data on the disk must adhere to the same standard of security encryption to prevent manipulation of the contents.

### Database security and integrity

Database security means that database is free from danger or exposure to damage or attack. The possibility of physical damage has to be taken into account. There has to be means of backing up and restoring the databases. Backups in and of themselves are not the only factor. Database security is very much an external factor which depends on the people operating the system.

Consequently, the backing up of the data must be done consequentially and with care by the individuals performing this task. Lack of doing so is a great threat to the whole system.

Integrity means that the state of the database is complete. The contents of the database must reflect the actual truth and there must be no doubt that the information is free of corruption. Integrity can be seen as an internal factor. It is a feature designed into the application programs that act upon a database and the structures within. The design of integrity should be straight forward and well understood so that the implemented system will operate correctly. Since the clearing system indirectly deals with money there is no limit on how high the level of security and integrity can be.

### Operating access

There is still a need to be able to directly access the database and change its contents. If system errors are not found in the test phase or system initialization, the database may be vulnerable to attack or corruption. As mentioned above, only a select few have access rights to change the database. This access is strictly controlled and given only to trusted authorities. The operating access can be restricted to control the rights of those operating a sales point versus the bus driver operating a vehicle or an individual performing clearing operations. Persons who have the rights to operate a local clearing can grant the operating rights to sales points or vehicles operating in that area.

The verification of the access rights to a certain operating area is performed with administrative level smartcards. These are smart cards equipped with a PIN. As an example the bus driver has to enable the card readers in the bus with his/her administrator card before going to work. Only then will the system be operational. The buses standing in the depots should not have operational card readers.

### The black and gray list

The purpose of the black and gray list is to keep track of the invalid smartcards (ie those cards that have been lost or stolen). The black list contains the card identifiers of the passengers whereas the gray list contains the operation or access cards. The lists are generally maintained at the central level and transmitted to the lower levels for copying. The black list protects the passengers from misuse of the lost or stolen cards. There are three levels of action that a card on the black list requires. The usage of the card can be forbidden, the sales person or bus driver can be ordered to take the card into possession or the usage of the card can be a crime. It is also possible to extend the list to contain other messages like renewing cards or withdrawing faulty card series. The black list is checked at every sales points and card reader.

## CLEARING OF ELECTRONIC PAYMENTS (FMTC 1994 NO. 5)

With over 400 different service providers in the Finnish public transport network, the scenario arises where a single journey can involve a number of service providers. Under these circumstances a clearing system is needed to calculate and apparition electronic payments among multiple service providers. The central clearing and the smart card management program share the same database and are situated in the same local area network. There is only one clearing and smartcard management program operating in the central clearing system. Each of the local clearings have software specific to their own operating requirements. In the same way sales points have specific software for their own requirements.

### Central clearing and the external world

When the central clearing system was implemented, existing computer systems were taken into account. The central clearing, which gathers the information of the sales, the travel and the changed tickets from the local clearings, calculates the accounting entries and transfers them to the financial management system. Furthermore the central clearing can produce the invoices for the credit sales in the case where the sales program hasn't charged the customers directly. Charging customers directly using the sales program is faster than processing credit invoices in the central clearing system.

Another feature of the central clearing is to calculate the subsidies and charge the subsidized customers accordingly. The central clearing also maintains the system's basic data. The card management program is designed to create and manage the administrator cards and therefore the program shares the database with the central clearing. The central clearing system is the only part of the system that contains all information and is therefore a natural site for producing reports regarding the ticket sales, travel volumes and invoices.

## Central clearing functions

The central clearing system provides the following six groups of functions:

1. Maintenance of the system's basic data;
2. Invoicing Functions;
3. Accounting;
4. Communications;
5. Reporting; and
6. Miscellaneous Functions.

Each of these functions are briefly described below.

### *Maintenance of system's basic data maintenance*

The basic data consists of the customer register, the system's sales points and operators, tickets and tariffs and possibly the information of subventions. Changes in this information will be transferred to the local clearing systems and from there the information will be sent to the sales points. The card readers will get the latest information about the tickets and the tariffs. The time it takes for the changes to take effect depends on the transmission rates between the levels. All changes are time and date stamped and will only take effect at the moment of transfer from the central system

### *Invoicing functions*

With the invoicing functions the manager of the central clearing can produce reports of the credit sales and reports of the subsidies to be collected from subsidizing agencies. Furthermore one can view the credit sales and the previously printed invoices. The sales program provides the facility to make a fast invoicing of the credit sales and can also be applied for the smaller or local customers. The other invoices are prepared at the central clearing level.

### *Accounting functions*

The purpose is to gather the sales and aggregate travel information from the local clearings and to calculate the totals of the whole system. This service can only be executed by a person with primary user rights under the central clearing system. The central clearing produces the accounting entries for the system and takes care of the billing settlements between the sales points and bus companies (service providers). The central clearing only performs the calculation of the commissions according to the specified clearing agreement.

The central clearing receives the information from the local clearings on a daily basis. This information contains the sales, travel and ticket repurchase of all service points. Upon receipt of this information, the central clearing performs a structural and integrity check. In the case of any faults or error messages in the information received, the data is disregarded and a resend is required. If the information is still faulty, the data errors are solved based on the records at the local clearing level. A check of missing transactions is also performed after receiving information from a local clearing.

When a transmission is error free and successfully accepted, the clearing system calculates the commissions and prepares the accounting entries. The final calculation can be performed on a selection of sales points, both internal and external to the system as well as the bus companies.

*Communications*

This part handles the settings of the automatic communication to the local clearings as well as the communication to the parallel clearings and the central accounting system. The data can also be transferred on a diskette from the local clearings. By using manual transfer the chosen data can be sent at once to chosen local clearing. The service can be used if it is urgent that the local clearing receive the data. Otherwise the communication is performed automatically as specified.

## STANDARDS

Standards play a significant role in the development of electronic payment systems. Standards can serve as a platform on which system interoperability and compatibility can be achieved. There are a number of standards which need to be considered for use in the design of an electronic payment system for transport. They can be considered in two categories, technical standards and procedural standards.

The procedural standards could also be referred to as banking standards. These standards reflect requirements set by the financial industry and are used in connection with electronic transfer of monetary transactions. The majority of existing standards which impact electronic payment systems are technical.

### Technical standards

The topics addressed by the technical standards include card technology, card reader devices, and communication requirements. There a number of existing standards which address the physical configuration of the card itself and the placement of those elements which make the card functional. These standards cover topics relating to the placement of embossed characters which are used to imprint card numbers and individuals' names; and other standards which define requirements for the magnetic stripe and the quantity, sequencing, and location of bit information it contains. Also defined by standard are the dimensions of the card's physical size.

Standards for magnetic stripe cards are fairly mature due to the age of this technology and the fact that its use is reasonably well developed. Smartcards, and their standards are not as mature. However standards are on the books for smartcards and this provides the foundation for this technology. And it is beginning to become more widely used.

The distinction has to be made here that the existing standards mostly define the contact type of smart card. Further work still remains for the full development of standards for contactless smartcard technology. Some of this standardization work is focusing on the element of the physical communication link required. This standardization work is being pursued in a number of different fora including the International Standards Organization (ISO), the European Organization for Standards (CEN), and organizations in the United States.

### Banking standards

Without going into too much detail here, the primary message is that the banking industry offers very detailed and precise requirements for financial transactions and the cards used to perform those transactions. The primary concern is monetary security and authenticity of information which defines the transaction itself. Data security, data structure, encryption methods, and transmission requirements make up a large portion of the standards covering this topic.

# INSTITUTIONAL ISSUES

## Legal

Electronic payment enables the collection of information that was previously not as readily available. For instance the accurate information of passenger travel can be gathered. This raises the question as to what extent the passengers privacy must be protected. Electronic payment systems also make the user a customer as well, thus creating situations that have to be resolved with respect to consumer protection law. For instance, compensation for the contents of broken smart cards or refunding unused tickets, transaction receipts and more.

Additionally, principles of business practice from the commercial environment must be adhered to in the transport environment as well. As an implementation issue, these details must be incorporated into systems design based on local legal requirements as well as prevailing financial requirements.

In several cases, these details are addressed in the form of contracts, both implicit and explicit, between the service providers and the customers. In specific cases, such contracts are agreed to as a condition of the customers receipt of equipment (such as a smartcard or transponder) which will be used to effect the transaction of electronic payment. This is not radically different from current practice in regard to credit cards and, again, points to possibility of utilizing applicable measures from the banking industry.

The difference in a transport environment is the specific terms of the contract relevant to the service provided and the method of payment used. Furthermore the effect of existing jurisdictional boundaries and associated organizational policies must be taken into account. This accountability facilitates the system's acceptability to the transport service provider and user alike and also contributes to encouraging deployment.

## Privacy

In the Finnish public transport system, the smartcards are equipped with an identification number for unambiguous identification of the card. There are also no limits of the exchange of information between the smartcard and the clearing system at the time the card is presented to the card reader. Information can be both read and written at this time. The smart cards can be divided into two main functional groups, the personal card and the bearer card. Personal cards can only be used by the person who bought the card and this person must be able to prove his identity when requested. Bearer cards can be used by anyone possessing the card.

## Alternative solutions

If the card number is registered and collected in the travel information but the card number cannot be connected to the card holder, a card specific register is created. On the other hand, by not registering the card number the whole problem concerning privacy protection is solved. This forces the creation of alternative procedures in some cases. The card number is desired in following cases:

1. To be able to establish the amount of money or journeys stored on the card in case of a dispute.
2. Some municipalities subsidize their citizens' travel and therefore the information of the passengers' municipality is needed. The pupils may also form a special group if the city supports their travel.
3. There is an interest to study various passenger groups for planning and marketing

4. To support invoicing functions with the companies that have made an agreement concerning traveling on credit.

The cases mentioned in number two and three can be solved by adding a passenger group code on the card. Instead of reading the card number when collecting the travel information the group code can be read. The group code will not be enough for the invoicing function. More accurate information of the travel is desired to specify the bill. This type of credit sales will not be bound to a person but rather to the holder of the card. Therefore the travel information has to be contained on the invoice for check and in cases of complaint.

The biggest problem is the case where the passenger claims compensation for a destroyed card. If the travel information can be followed up, one can say exactly how much money or how many journeys the card contained. This way the system also would provide a benefit for the passenger. The card number is also required when locating stolen or lost cards. A black list containing the illegal card numbers can be sent to the card readers, which could warn and prevent the misuse of lost cards. Being able to compensate for broken cards and preventing the misuse of lost cards are also forms of protection but all at the cost of protecting the privacy

## CONCLUSIONS

Conclusions are offered here concerning the four categories which have been addressed in this paper. These are intended to summarize the implementation issues in such a way that exposes the open ended aspects of electronic payment. Such aspects must be closed on a case by case basis and depend on resolution of local constraints which will ultimately influence the final system design.

### *Methods of payment*

Different methods of payment will provide varying degrees of system flexibility. The flexibility of the of the payment method will impact the degree of system functionality and its compatibility and interoperability with other system applications for electronic payment. Choices made in connection with this element of system design will also determine the limits of the systems capacity to 1) provide the desired level of service to the users, and 2) expand for future use and system interoperability.

### *Security*

Security is a significant system consideration from the perspective of data integrity and financial protection. Banking requirements set high standards toward this end. But higher degrees of security come with higher implementation costs. The use of electronic payment technologies creates new opportunities and also new problems. Questions are raised about protecting individuals in matters of privacy and consumer protection. Contractual arrangements can go a long way toward solving these types of issues. But specific terms must be settled on under the prevailing constraints of the jurisdiction where a given system is implemented.

### *Clearing of payments*

The clearing system designed for the Finnish public transport system utilizes a modular structure which incorporates clear and well defined interfaces. This permits a flexibility which is easily extendable to accommodate the development of additional applications. This capacity for integration of other electronic payment systems is perceived as an assurance that the system as a whole will continue to grow an become an important element of transportation, and other services as well. As a financial function, clearing must also maximize the use of existing mechanisms provided by the banking industry. This point can reduce the need for "new" financial design and make electronic payment more accessible to the transportation industry.

*Institutional*

A great deal of technology is available to accomplish the tasks of designing electronic payment systems for use in transportation. But the importance of jurisdictional and legal requirements cannot be overstated. Resolution of these types of institutional issues provide the follow through which allows successful implementation at the local, national, or international level as well. While the banking industry provides substantial coverage of the institutional issues associated with electronic payment, there is still a lot of new territory which must be reconciled with respect to electronic collection of information. This is particularly relevant in connection with design decisions concerning what information is to be collected.

## REFERENCES

Bright, R. (1988) *Smart Cards: Principles, Practice, Applications*, Halsted, New York.

Finnish Ministry of Transport and Communication (1994 No. 1) *Payment Systems for Public Transport*, Ministry of Transport and Communication.

Finnish Ministry of Transport and Communication (1994 No. 4) *Specification for IC Card Systems Used in Public Transport Applications, Ver 1.0*, Ministry of Transport and Communication.

Finnish Ministry of Transport and Communication (1994 No. 5) *Specification for Clearing System in Public Transportation in Finland*, Ministry of Transport and Communication.