EMV SPECIFICATION USAGE WITHIN PUBLIC TRANSPORT AUTOMATED FARE COLLECTION

D JOUBERT and E BIERMANN*

Techso (PTY) LTD, P.O.Box 35, The Innovation Hub, Pretoria, 0087
* Tshwane University of Technology, Private Bag X680, Pretoria, 0001

ABSTRACT

The fare media that are used to collect the fares within the South African public transport industry are mostly closed and proprietary systems, which are based upon proprietary interfaces. These fare media are of a contactless type as contact based interfaces are impractical.

The contactless payment media as part of the banking industry have since caught up with the transport industry, as it currently finds a new contactless low value payment market. The banking industry is however more focussed on security and interoperability aspects than the transport industry. Card associations govern the standards that banking industries use, and do not create small islands of non-interoperable solutions.

For this reason, a payment medium is selected as a fare medium device as a possible solution to interoperable fare media. The payment media, however, lacks certain data elements that the public transport industry needs in order to carry out functions like calculating distance based or concession fares. The purpose of this article is to demonstrate a feasible approach to implement a contactless bank issued EMV smartcard within public transport for Automated Fare Collection.

1 INTRODUCTION

Before Transport for London issued its contactless Oyster Transport smart card, it worked with paper-based magstripe tickets. It was a solution that enabled a magnetic stripe ticket to be read and then transferred across a conveyor system to beyond the access control mechanism for the commuter to collect. The maintenance of such a system is time-consuming and expensive, owing to the mechanical nature of the system. Even contact smart cards are considered inefficient to public transport as they need to be inserted correctly, there is contact wear and tear, and the communication speed is slower than that of contactless (Hendry, 2007:56).

Thus, the move to a contactless interface where no physical contact is required appears to be a logical step. To date, the transport industry has used the contactless interface smart cards for its electronic fare collection purposes more than any other contactless smart card implementation (Dewe, 2009;Morgan, 2009;Pretorius, 2009). Contactless payment media interface standards emerged in 2002 with the first contact less payment cards issued by MasterCard. Visa followed three years later and licensed the technology interface standard from MasterCard in 2005 (Hendry, 2007:153). The banking industry therefore seems to be "*catching-up*" with the contactless fare media

industry although they will be issuing contactless payment products based on open standards.

This still leaves a gap between the transportation industry and the banking industry, as not all commuters have bank accounts. This means that an anonymous prepaid payment product must be issued and supported by the banking industry which can be used within the public transport industry. According to Beghin et al. (2008:1),40% of adult South Africans did not have bank accounts in 2007. Thus 12.6 million adults need access to fare media without having to open a bank account. According to the Smart Card Alliance (2008:8), the major reasons that individuals generally don't get a bank account are the following:

- They think they do not have enough money for the account or the service costs.
- They do not trust the bank with their information.
- There is a cultural barrier.
- They are used to a cash-based culture.

Several pre-paid versions exist on magstripe platforms that cater for anonymous usage without having to have a bank account, however their usage is limited due to the fact that transactions have to occur online, and via a contact interface (Smith, 2008a). This is where pre-authorized debit is able to enter as a possible solution to the gap between the payment and fare media industry (Abou-Rhame, 2009), as it is implemented on a smart card based technology, thus allowing for offline and contactless spending.

2 PRE-AUTHORIZED DEBIT

The concept of pre-authorized debit allows the banking industry to offer a pre-paid payment instrument with off-line transaction processing capability which is ideal for use within the transit industry. Some aspects that make pre-authorized debit ideal for Electronic Fare Collection are:

- Anonymity: The card holder can be anonymous. Transactions are however tracked and recorded for auditability.
- FICA exemption - The Financial Intelligence Centre Act (South Africa, 2001) requires all account holders with a bank to be identified through national identification documentation as well as proof of residence. The Act is put in place to reduce money laundering. Low value payments, which include pre-authorized debit payment products, are currently in the process of being considered as an exemption to the Act with certain pre-set limits with regard to (Smith, 2008a):
    - the maximum balance the card can carry at any time ;
    - a maximum calendar month loading limit; and
    - a maximum value per transaction.
- Security: As the card and the account at the bank, the "*shadow*" account, will always be in a 1:1 relationship, monetary value cannot be created on a card without the "*shadow*" account first being securely updated, this is done to have a fully auditable system.
- Offline use: Transactions can occur without the Point-of-Sale (POS) device having to connect to the acquiring bank's authorization infrastructure to approve

a transaction.
- Contactless use: Transactions can be executed without having to have physical contact with the Point-of-Sale.
- Speed: Transactions are currently specified by payment card associations to be below 500 milliseconds, thus it can be utilized within the public transport environment.

The banking industry in South Africa does not entertain pre-paid debit payment cards with the card being the only entity maintaining the balance. According to Smith (2008a), the risks associated with injecting money into the National Payment System (NPS) are too great. Thus the concept of pre-authorized debit payment cards where the card balance is mirrored in a shadow account at the bank is far more secure, because a value can only be "*loaded*" onto a card's shadow account via a secure online transaction process. Pre-authorized debit payment media are therefore based upon a secure Europay, MasterCard, and VISA (EMV) specification.

2.1 The EMV Specification

According to Smith (2008b) the South African banking industry has selected the EMV standard as its smart card based payment media standard with which all banks have to comply if they wish to issue smart card based payment media for use within the NPS.

The EMV standard describes the transaction process flow between the smart card and terminal at two levels and both of these levels need to be certified by an independent third-party for compliance (Hendry, 2007:150):

- Level 1 - The electrical and protocol layers; and
- Level 2 - The application requirements, message and data structures, transaction flows, security, and user interface.

The transaction flow of an EMV transaction will be brie y examined according to the implementation of MasterCard Worldwide (2009). According to Radu (2003:Chapter6), the following is a summary of what occurs during an EMV transaction (items are sequential):

- Card + Terminal: The terminal reads all the available applications on the smart card and selects the EMV application it is entitled to.
- Card + Terminal: The terminal initiates the EMV application by informing it of the business environment of the terminal. This is done so that the card can do risk management.
- Card + Terminal: The terminal reads the EMV application data from the card to deter-mine the correct transaction options to specify.
- Card + Terminal: If the card indicated that it wanted to perform offline data authentication, the terminal would comply by executing offline data authentication.
- Terminal: The terminal processes restrictions to determine if the card is entitled to the financial services it is requesting.

- Card + Terminal: Card holder verification is done mutually by card and terminal if required.

- Terminal: Terminal risk management is done based upon the perspective of the acquirer for acceptable lower and upper floor limits.

- Terminal: Terminal action analysis is done based upon the results of the terminal risk management, and can force a transaction to go online to the acquiring bank for assistance in determining the risk associated, or it can deny or reject a transaction based upon the terminal risk management parameters.

- Card: Card risk management is done in the same fashion as the terminal, but the parameters are based upon the card holder and the issuing bank.

- Card: Card action analysis can deny, allow, or request online transaction authentication on behalf of the card holder and the issuing bank.

- Card: Application cryptogram is created for each transaction and is unique. This cryptogram displays the card's participation in the transaction and cannot be used again. The card can also decides if it wanted to go online through the card action analysis.
- Terminal: If the card wanted to go online, and online transactions were allowed on the terminal, then request authorization for the payment.

- Terminal: When authorization is received (deny or accept the transaction), respond to card request so that card can start finalizing transaction.

- Card: Finalize transaction with authorization.

- Card + Terminal: Process any issuer scripting. When issuer has been authenticated, these scripts can contain updated parameters or any other sequence of commands.

According to Kotze (2009),the card reader and card interaction can be seen clearly within a high-level interaction as illustrated in Figure 1 as:

- The terminal has found a single card in its charge proximity through anti-collision mechanisms as indicated in the standard International Standards Organization (ISO) 14443.

- The terminal requests the card to supply it with all the applications on the card that comply with the MasterCard PayPass specification. The card responds with a File Card Indicator (FCI) containing the list of the applications that comply.

- The terminal then selects the PayPass application that it wants through a specific Application Identifier (AID). The smart card will respond with an FCI that contains information specific to the PayPass application that was selected.

- The terminal will request the Get Processing Options (GPO) to determine the selected application's required information. . The smart card will respond with an Application Interchange Pro le (AIP) and an Application File Locator (AFL), which in turn show where additional information that the terminal might require is stored within the smart card.

- The terminal will then read the records indicated within the AFL.

- The terminal will finally request a Generate Application Cryptogram (GEN AC) to create a unique application cryptogram based upon the transaction that has taken place. This Cryptogram is transmitted to the terminal and the terminal can verify that the card with which it is communicating is a legitimate card. If the terminal can decipher part of the cryptogram, the transaction is approved and the application cryptogram is passed to the acquiring bank.

The process previously discussed within the bullets can be seen in Figure 1.

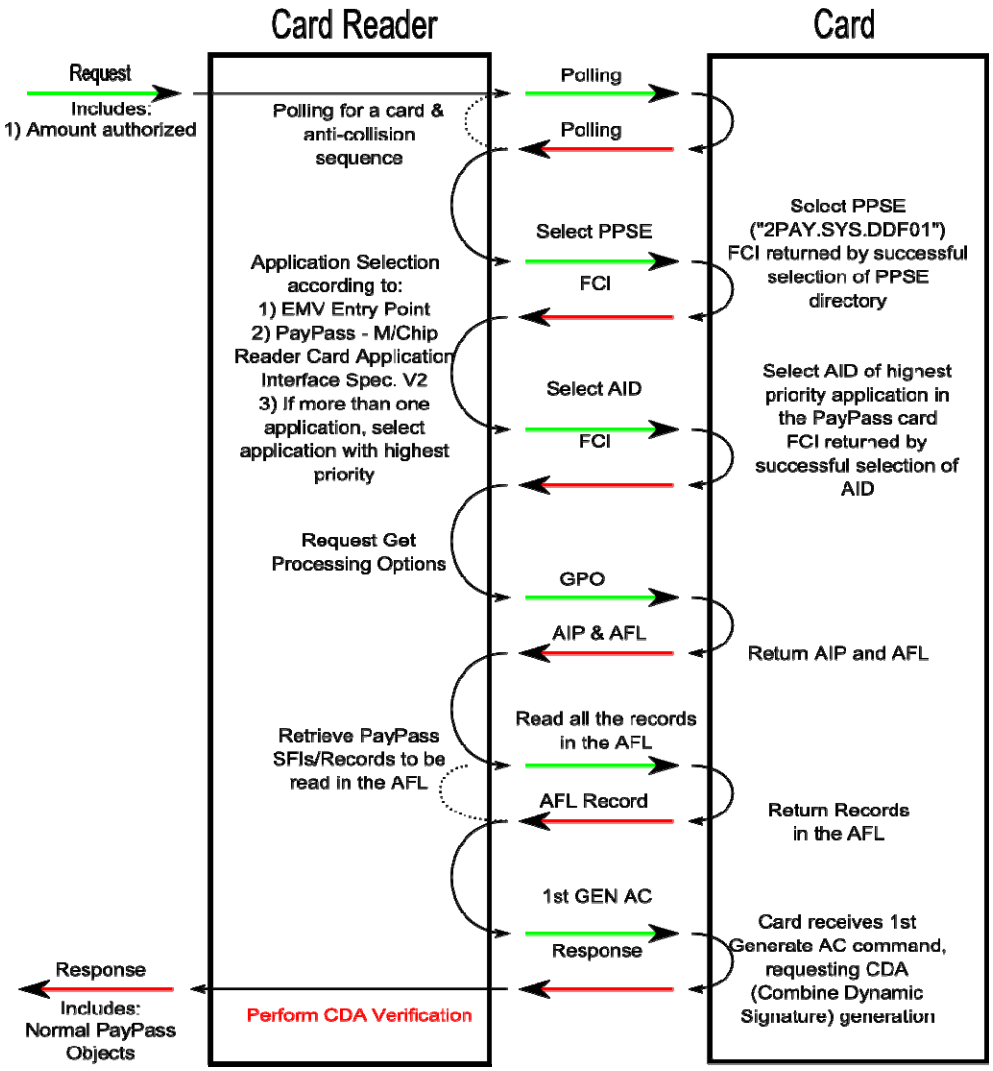

Figure 1: A MasterCard PayPass Transaction According to Kotze (2009)

2.2 Public Transport Accommodation within EMV

The EMV standard does cater for a discretionary data area for use by Issuing Banks, although no shared usage has been agreed between Issuing Banks. Although not part of the original EMV standard, MasterCard Worldwide (2009) has created a method within their EMV implementation to store and retrieve unformatted data blocks (correctly referred to as Tags) for public transport usage. These data blocks were first used within their Kaohsiung payment and fare media project with great success. MasterCard World-wide (2009) further divided the data blocks into two sections:

- Unsecure data blocks: These data blocks can be read from and written to by any terminal with the capability of selecting and understanding ISO 7816 commands.
- Secure data blocks: These data blocks can be read from by any terminal with the capability of selecting and understanding ISO 7816 commands, however, writing to these data block locations require the strict permission from the issuer via a script.

Thus, updating these data blocks can only happen during an online transaction within EMV. As retrieving the scripting from the issuer can take some time (more than 3 seconds), the card holder is required to insert the card into a contact interface to update the secure data blocks for the practical reason of forcing the card to be connected to a terminal for the whole duration of a transaction and the script retrieval process.

There is no difference to the normal EMV transaction. The only additional is the point at which these data blocks can be read or written to within the EMV process.

3 THE PUBLIC TRANSPORT REQUIREMENTS

Apart from the monetary value that is securely loaded onto payment media for the banked/unbanked commuter, and securely spent without fraudulent transactions being injected within the NPS, the stock standard payment medium has a gap that needs to be filled. A "*flat-fare*" structure can easily be accommodated on a pre-authorized debit payment media that is smart card based at the point of entry or exit within a public transport journey, with the exception that there will be no access control infrastructure at the end of the journey. A differentiated fare structure and/or access control infrastructure at the end of the journey, however, requires additional information, that either needs to be:

- transmitted to the end of the journey of a commuter; or
- available on the smart card for the POS device to determine the accurate fare.

As indicated earlier, a differentiated fare structure requires the following possible information sets to be available:

- Position - the start and end position of the commuter's journey.
- Time - the start and end time of the commuter's journey.
- Route - the route the commuter came from (promoting certain route usage for different routes).
- Transit product - if the smart card carries the proof of payment for a transit product, no monetary value deduction is required or only a small part of the monetary or product value needs to be deducted.
- Commuter classification - it is a well-respected fact that certain commuter classes require discounted fares.

For fixed facilities such as train and bus stations, the possibility exists that information could be transmitted to all possible nodes of journey exit for the commuter. However, this "*shotgun*" approach is inefficient and as it is indicated that public transport networks do operate on a loss.

3.1 Automated Fare Collection as part of EMV

According to Kotze (2009), the following proposed access flow diagram correctly indicates the process of how the proposed data structure might be accessed. This process is indicated in Figure 2 and will be explained briefly.

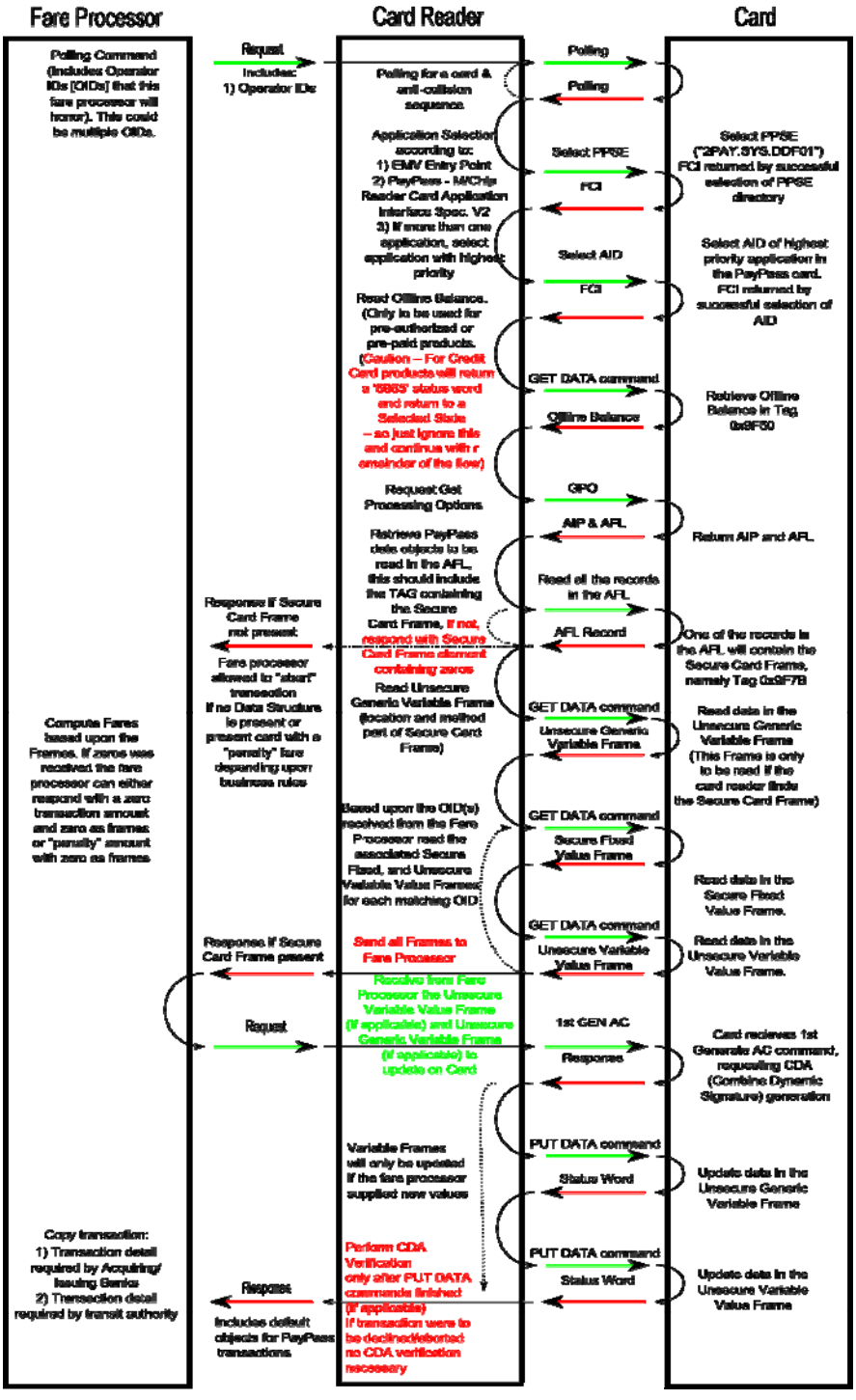

Figure 2: The Transaction Flow of Accessing the Public Transport Data

The difference between Figure 1 and Figure 2 seems quite substantial. To add to the complexity, additional fare media calculations have been added. The following is a description of the flow found in Figure 2,starting at the top left corner of the figure:

- The fare processor will initiate all communications to the card reader by indicating which operators' products it currently honours, or currently has an agreement to honour. This will start the normal transaction as indicated in Figure 1.

- After the correct contactless application has been selected, the card reader will then try to read the “Offline Balance". If it is unsuccessful, it will have to consider other business rules for the transaction. As the smart card is not a pre-authorized debit application, these business rules may include increased fare.

- According to Robberts (2009),the data structure will be accessed most easily when the Secure Card Block is part of the AFL list, hence will always be read by a card reader even if the card reader is a retail POS device. Thus as part of the AFL record retrieval process, the terminal will automatically read the Secure Card Block within the AFL records at the point when the terminal request the GPO command.

- If the smart card has a Secure Card Block within the AFL, it will continue the transaction, or else it will reply to the fare processor that it does not have a data structure, in which case the fare processor can either abort the transaction or try to execute a punitive fare amount.

- If the smart card has a Data Structure by having the Secure Card Block, it will read the Generic Variable Block either through a GET DATA or a READ RECORD command. This decision is indicated within the Secure Card Block, through the SFI Map data element within the relevant data block.

- Depending upon the Operator IDs that the Fare Processor provided to the Card Reader, the Card Reader will identify if any of the three products were assigned with any one of the Operator IDs within the Secure Card Block. The data elements “Value Block 1 Operator ID", “Value Block 2 Operator ID", and “Value Block 3 Operator ID" indicate the “ownership" of the respective Value Blocks. The “Secure" and “Unsecure" pairs of the Value Blocks will be read from the data structure and be given to the fare processor for calculating the fare due.

- It should be noted that a Fare Test Bench will be created for the evaluation criteria to see if the proposed data structure met the needs in question.

- The fare processor will then calculate any fare due, and return to the card reader the amount due (which could be zero), the Unsecure Generic Value Block and the Unsecure Variable Value Block.

- The card reader will then request the GEN AC command to authorize the financial transaction - see Figure 1as well as its discussion.

- Finally, the card reader will update any Unsecure Blocks if any changes were required. This step is left to the last because the GEN AC command could fail, in which case the Unsecure Data Blocks should not be updated.

4 CONCLUSION

The article focused on the possible convergence of fare and payment media technology applications. As a proposal, this article selected the EMV specification, selected by the South African banking community as its “de facto” smart card payment standard. The article used a previous implementation from MasterCard Worldwide based upon the EMV specification to propose a public transport data structure that can be used within the EMV transaction flow to facilitate fare media requirements.

The proposed public transport data access flow has not yet been fully tested within a live environment and therefore might lack certain aspects with regard to practical implementation requirements. It is however envisaged that these implementation requirements can be accommodated within the current solution, without considerate change to the access mechanism.

5 REFERENCES

ABOU-RHAME, N. 2009. A shift in perspective In: Thinking Highways 4.1 (Mar. 2009), 21{24.

BEGHIN, D., HIGGS, N., NAPIER, M. & POWELL, R. (Ed.) 2008. The number of people banked in South Africa has increased by 20 percent but use of products remains limited[Online]. Available from: http://www.finscope.co.za/documents/2008/PR_SA07_ banked.pdf[Accessed: 2008/12/04].

DEWE, C. 2009. National Department of Transport's Public Transport Data Structure - Stakeholder Requirements for Surepaw (Product Supplier). Interview:Pretoria:NDoT Public Transport Data Structure.

HENDRY, M 2007. Multi-application Smart Cards - Technology and Applications. New York: Cambridge University Press.

KOTZE, P. 2009. National Department of Transport's Public Transport Data Structure - Card, Terminal, and IFM transaction flows. Interview:Stellenbosch:NDoT Public Transport Data Structure.

MASTERCARD WORLDWIDE. 2009. A Generic EMV Transaction Flow. Interview:Johannesburg:MasterCard Workshop.

MORGAN, C. 2009. National Department of Transport's Public Transport Data Structure - Stakeholder Requirements for TMT (Product Supplier). Interview:Pretoria:NDoT Public Transport Data Structure.

PRETORIUS, C. 2009. National Department of Transport's Public Transport Data Structure - Stakeholder Requirements for Questek (Product Supplier). Interview:Pretoria:NDoT Public Transport Data Structure.

RADU, C. 2003. Implementing Electronic Card Payment Systems. 1st Edition. Norwood: Artech House.

ROBBERTS, D. 2009. National Department of Transport's Public Transport Data Structure - Stakeholder Requirements for the Europay, MasterCard, and Visa standard requirements. Interview:Pretoria:NDoT Public Transport Data Structure.

SMART CARD ALLIANCE. 2008. Serving Unbanked Consumers in the Transit Industry with Prepaid Cards - A Smart Card Alliance Transportation Council White Paper [On-line]. Available from: http://www.smartcardalliance.org/download/pdf/Serving_ Unbanked_Transit_Riders_White_Paper.pdf[Accessed: 2008/12/04].

SMITH, K. 2008a. Interview: Pre-Authorised Debit. Interview:Pretoria:National Department of Transport Project: Electronic Fare Collection and Integrated Fare Management Report: Final Report Document.

SMITH, K. 2008b. The Current South African Banking Industry Status Quo. Interview:Pretoria:National Department of Transport Project: Electronic Fare Collection and Integrated Fare Management Report: Final Report Document.

SOUTH AFRICA. 2001. Financial Intelligence Centre Act, No 38 of 2001. Government Gazette 22886.