INFORMATION SECURITY VULNERABILITIES WITHIN EMV AUTOMATED FARE COLLECTION, THEIR CONSEQUENCE, AND POSSIBLE REMEDIES

D JOUBERT

Royal HaskoningDHV (Pty) Ltd, PO Box 25302, Monument Park, 0105, Pretoria,

Tel: 012 367-5889; Email: Dawie.Joubert@rhdhv.com

ABSTRACT

South Africa embarked on a world first when it promulgated legislation to ensure that it future proofed fare revenue collection for its public transport system. The legislation did not get promulgated without resistance from local and international fare collection product suppliers. The promulgation is technology agnostic, and only refers to a bank issued fare medium that must be based on the Europay MasterCard Visa (EMV) standard that should contain the Automated Fare Collection (AFC) Data Structure (DS). The AFC DS in turn is defined as electronic tags that are used for recording and retrieving public transport-related data.

Herein lays the vulnerability of the legislation. Card Associations (CAs), such as MasterCard, Visa, and American Express to name but a few, create bank issued media implementations that authenticate financial transactions that comply with the strict EMV specification. These CAs also provide AFC DS mechanisms that provide access to the electronic tags that are referenced within the legislation. These AFC DS access mechanisms are not governed by EMV. These mechanisms are not governed, reviewed, or audited for "fit-for-purpose" within the public transport domain either. They are provided as is and do not come with any warranty and/or guarantee that "fare-calculations" will be secure, reliable, and consistent. How could they, they are not part of the calculation process.

If the AFC DS electronic tags can be compromised, meaning the manipulation of the public transport data on the fare medium, then the CA have a direct impact to the correct and/or incorrect calculation of the fares.

All the provided AFC data structure mechanisms provided to date can be compromised to some extent. Additional legislation that was promulgated also inhibits the use of the AFC Data Structure to its full extent as originally envisaged. This paper will briefly provide detail on some of these issues, their impact, mitigation measures, and a recommendation for a more secure implementation.

1 INTRODUCTION

South African National Department of Transport (NDoT) selected the EMV platform to assist in standardising the electronic fare collection and electronic fare integration initiatives. This was done as the potential smart cards are able to be a more secure mechanism for collecting fares and/or validation of a commuter's credentials (Trepanier et al, 2004). Smart cards also provide the ability to introduce more complex fare rules, reduce driver interaction, and increase the ridership data quality generated (Dempsey, 2008). Data generated, stored, and transmitted through the smart card can assist an Implementation Authority with Strategic, Tactical, and Operational decisions with regard to their public transport services offered (Pelletier et al, 2011).

Pelletier et al (2011) illustrates, through several case studies, how information on the smart card is validated when entering the public transport service. The validation checks for several fit for purpose characteristics before that card is accepted. The information on the smart card is always considered to be in an asynchronous state to that of the information contained in the back office. This means that the last known and trusted state of the smart card is not immediately available to all the entry and exit points of the public transport system when it is presented for validation.

There is a time delay for the information to be processed, and transmitted from the presented point to the back office and then to the remaining points, if it is done at all. Due to the asynchronous nature of the system and the existence of multiple different Implementing Authorities, validation of the smart card contents can be complex from any one point in the system.

2 STATUS QUO

In June 2011 the regulations requiring automated/electronic fare collection systems to use a fare medium based upon the EMV standard as issued by a "participating bank" was promulgated (South Africa, 2011). The fare medium, as stipulated in the regulations, should also contain the Automated Fare Collection (AFC) Data Structure (DS) which would allow public transit information to be written and read from the fare medium (Joubert & Biermann, 2010). This was one of the first steps towards an integrated fare policy for South Africa, with the implementation to follow.

The AFC Data Structure's main focus was to have a shared "scratch pad" to implement, generate, and share public transport information, in a standardised way between different electronic fare collection systems (Joubert, 2010). The initial accepted and promoted approach by the National Department of Transport was to adopt the approach of: "as fast as the fastest bank" (Smith, 2008). This meant that the first bank supporting the first CA's AFC DS mechanism will be used first.

The initial proposed AFC DS used within the EMV framework did have technical limitations. These limitations for the public transport industry however were to the security benefit of the payments industry. One such benefit was the inability to write monetary value back to a pre-authorised debit application during an offline transaction (Kotze, 2009). These limitations did not allow a limited amount of previously discussed public transport fare collection business rules. One such business rule as per example was the ability to deduct the maximum amount of fare at the start of the journey and paying the remainder back, immediately, at the end of a journey (Joubert, 2010).

Although EMV was not initially capable of being used within a high demand throughput system such as public transport, it was designed around the paradigm of being part of a multi-application domain. Not just a banking application, but loyalty, identification, and public transport applications were envisaged. Their term was the “multi-application-wallet”, “because a physical wallet does not just carry cash and payment cards” (Andreae, 2011). This has since changed with technology advances that have increased in the microchip, banking, internet, and public transport industries. These advances occurred to such a variety of components that EMV transactions can now be executed under 500 milliseconds (Visa International, 2013). This is arguably well suited for most public transport systems, although still disputed by many that indicate that 300 milliseconds should be the benchmark. EMV was not the only payment solution and during the same time that the first EMV standard was released (1996), Seoul introduced the Mifare Classic (contactless smartcard) within its Public Transport system. Mifare was developed by Mikron and stands for *MI*kron *FARE*-collection System.

Mifare soon became the de facto standard within public transport fare collection but suffered several noticeable security vulnerabilities. The Mifare Classic smart card by Dutch students (De Koning Gans et al, 2008) and the newer Mifare Ultralight compromise (Intrepidus, 2012) illustrates a continuous battle to ensure that electronic information is protected, reliable, and from a reputable source. Information security is no longer an optional extra but a requirement from regulators and customers alike.

Today’s systems will also be tested by a variety of entities on a day to day basis as can be seen from the examples above. Confidentiality, Integrity, Availability, and Non-repudiation requirements are domain agnostic and it is a battle fought by all sectors such as transport, banking, etc.

One substantial benefit from a security viewpoint is that selecting the EMV standard as an AFC platform is that EMV keeps on being updated to accommodate changes and challenges continuously. The current South African AFC Data Structure approach is that of handling the AFC Data Structure within a normal EMV transaction to expedite the transaction and use available data “tags” within the banking application (Joubert & Biermann, 2010). Should the specification have required that the transportation information be housed within its own smart card application (one application for EMV, another for transport, and both of the applications needed to be utilized), the execution duration of a single transportation transaction would have made it currently not feasible for use within a high throughput environment.

Having to rely on another application (public transport reliant on EMV), several information security aspects were made a given, and others a consequence. The following section will briefly highlight some Information Security aspects before the information security aspects will be discussed as they relate to EMV and AFC Data Structure.

3 INFORMATION SECURITY

Attoh-Okine and Shen (1995) indicated that a successful smart card initiative within public transport ensures that the following information security aspects are prevented:

- Card cloning;
- Card forgery;
- Card tampering; and
- Repudiation.

Confidentiality, Integrity, Availability, and Non-repudiation are considered in the information security industry to be the primary four corner stones of information security (McCumber, 1991). Confidentiality refers to the fact that the information is not disclosed to a party forbidden to view the information. Integrity refers to the original information being delivered to the recipient without having been modified. Availability refers to the information being available at the correct time and state as required. Non-repudiation refers to the fact that the sender of the information cannot deny the sending of information that they originated.

The following sections will briefly cover the AFC Data Structure's CIA and Non-repudiation aspects.

4 AFC DATA STRUCTURE COMPLIANCE

Although the National Department of Transport (NDoT) would like every implementer to utilize the AFC Data Structure it is not legislated that one needs to use the AFC Data Structure on the bank issued fare medium, only that when a bank issue a fare medium, that it has the AFC Data Structure.

It is not required that the implementer has to comply with the AFC Data Structure as calculation mechanism for Tap-On and/or Tap-Off calculations (or for any other storage). However, that does not mean it is not an appropriate mechanism to use. It just means that the current legislated wording does not require an implementer to use it.

The mechanisms provided by the CAs to date are not yet where they should be based on the following observations:

Two four-party-mode CAs that provided tags mechanisms for the AFC Data Structure within South Africa have replication vulnerabilities that need to be addressed. This is not a new fact, it was present the day the first AFC Data Structure version was released (South Africa, 2009). The AFC Data Structure clearly identifies the replicable tags that can be compromised. The AFC Data Structure refers to these tags as unsecure.

The "*secure*" and "*unsecure"* keywords identify the mechanism required to write to the identified "*tag". "Secure"* "*tags*" can only be written to through bank issuer scripting as described by the EMV standard and implemented by the CA compliant applications on the card. This write mechanism is usually referred to as the "*online"* mechanism. The "*unsecure"* "*tags*" can be written to by anyone with a compliant ISO 7816 smart card reader writer. This means that any laptop, microcontroller, and/or device with an ISO 7816 interface (hence referred to as a "*cheap device*") can change the data within the "*unsecure*" "*tags*". The later mechanism is usually referred to as the "*offline"* mechanism. EMV work on the principle that most of the information on the bank issued media can be read (it is not confidential information). The confidential elements within the issued media are the secret keys of the card. The secret keys of the smart card are unique thus if a reverse engineer discovers the card's unique secret key, the entire payments system is not compromised, but only a single card (Robberts, 2009).

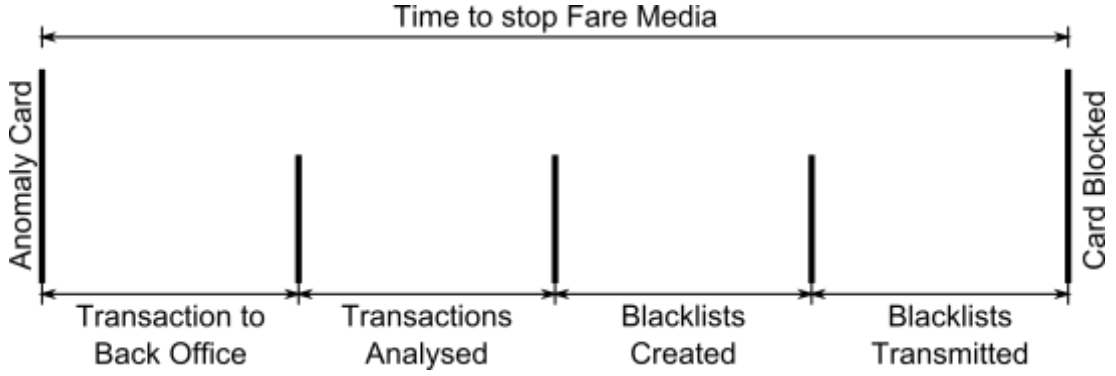
Both "*secure*" and "*unsecure*" "*tags*" can be read via a "*cheap device*". No access restrictions exist. Thus Confidentiality of the information within the AFC Data Structure is not covered. The Confidentiality aspect is twofold, the information is stored in a readable state, and it is also transmitted in a readable state, meaning, one can "*listen-in"* on the transaction and find out any information.

Integrity of the data within the "*unsecure" "tag"* is as per definition, in question. Data from these "*unsecure*" "*tags"* can be changed by a "*cheap device*". To counter the integrity of the data, a keyed-Hash Message Authentication Code (HMAC) was suggested within each of the "*unsecure*" "*tags*" to ensure that the data contained therein was at some point in time a legitimate representation of the information. Thus Integrity was able to be ensured to an acceptable degree.

Availability of data is in question because the "*unsecure" "tags"* can be written to. Thus rendering the data unavailable at the point where it was required. "*Unsecure" "tags"* contain information about boarding, alighting, and usage. Lombard (2010) indicated that copying of the "*unsecure" "tags"* to a temporary storage, using the bank issued fare media, and then restoring the "*unsecure" "tag"* state can effectively compromise the Availability of the data, because although the data integrity is maintained, it is from a previous state, hence the current data state, that is required, is not available.

Some approaches have been considered to mitigate the vulnerability of restoring a previous state by implementing an unchangeable counter that increments every time access is given to the "*unsecure" "tags".* This "*unsecure*" "*tags*" counter will then be used as part of the HMAC process to ensure that the HMAC signature is unique. However, the counter is currently allowed to "*roll-over*". "*Roll-over*" refers to computer behaviour that once you reach the maximum number a variable can store, that it will start from zero again (which assumes unsigned behaviour).
EMV caters for this in their specification, but only for the payment applications, not for the discretionary "*tags*". For instance, if EMV incurs "*roll-overs"* in certain critical aspects, such as counters, it can kill the payment application. But the mechanisms provided to access the AFC Data Structure "*tags"* do not fall under the EMV specification. Thus to currently bypass this counter, one would save the "*unsecure*" "*tags*" of the bank issued fare media to a "*cheap device*". One can then use the fare media, for whatever period of time and then restore the fare media from the "*cheap device"* by accessing the "*tags"* several times until the "*unsecure*" "*tags*" counter is as it was initially because the counter will have "*rolled-over*".
Currently, unless a "*pay-as-you-go*" scheme (also only in certain configurations) is used, a bank issued fare media can be compromised for the period when the "*unsecure" "tags"* are bypassed until the time the back office software has identified the anomaly and has updated the remote terminals to block further access to the public transport service (see Figure 1). Blacklisting of cards should be made compulsory for any future NDoT certification.

Figure 1: Time to stop Fare Media



Manufacturers may complain about implementing blacklisting, due to a possible complaint about additional overhead/time required for finding a card number within the list stored on the fare calculation/access terminal. This argument has been found to be irrelevant due to the fact that a binary search will only take $\log_2(N)$ "*checks*". This means that in a database of 40 million entries, it will take a maximum time of 26 "*if statements*" to find if the card number was blacklisted by the transport authority. These "*if statements"* are measured today in microseconds and not milliseconds.

The final vulnerability aspect of the AFC Data Structure that needs to be considered is that of Non-repudiation. Non-repudiation refers to the fact that the transaction cannot be refuted and/or challenged afterwards. EMV's Non-repudiation mechanisms that are executed when a financial transaction executes are sufficient to indicate where that card was at a certain point in time. It is for this reason that implementing authorities that plan to apportion fare between themselves always execute the financial transactions of EMV, even if the value is zero rand.

This non-repudiation mechanism does however not cover the AFC Data Structure's content at that point in time, thus although the financial transaction cannot be refuted, the data that was used to calculate the financial transaction can be refuted. It is therefore important to use a mechanism, such as asynchronous signatures, to ensure that data coming from the card is legitimate. This approach however assumes that the terminals are trusted between different parties, and that data elements used to calculate the HMAC are able to be mapped between the EMV application transaction and the information used to calculate the transaction.

5 POPI COMPLIANCE

In December 2013, the President of South Africa signed the Protection of Personal Information (POPI) Bill into law (South Africa, 2013). Irrespective the views of the bill's appropriateness and/or enforceability, the POPI Act has some consequences on EMV, the AFC Data Structure, and the information stored, generated, and reported via these mechanisms, especially within the Public Transport domain (Swart, 2014).

Because there are no Confidentiality mechanisms associated within most of the EMV "*tags"* and all of the AFC Data Structure "*tags",* measures need to be taken to protect an implementing authority. Any personal information that is made public, or is publically available will constitute a contravention of the mentioned Act. Personal information is defined very broadly, and can include, but is not limited to all of the elements defined within the AFC Data Structure.

The Act according to Swart (2014) requires some of the following aspects:

- That an entity only collect information for a specific purpose of business;
- That an entity applies reasonable security measures to protect the information collected;
- That the entity collecting the data clearly inform the subject the reason for the collection and what will happen with the information;
- That the entity ensure that its information is relevant and up to date;
- That information collected is only held for as long as necessary; and
- The subject of the information must be able to see the information upon request.

Of all the items that the Act requires, the single critical one that the current EMV and AFC Data Structure environment do not currently cater for is that of point two, which requires that "*That entity applies reasonable security measures to protect the information collected*". Reasonable security is not tied to any specific standard but available international standards such as ISO 27001 or PCI DSS will in all probability be viewed as acceptable. The public transport and/or banking implementing authority can utilize information security measures to safeguard generated information within their own Information Systems to a certain degree (See next section entitled PCI Compliance), however that leaves open the aspect that the AFC Data Structure can be read while not part of a public transport and/or banking infrastructure facility.

Although this fact can be made known to the commuter in advance, the expectation of the Act is that "*reasonable security measures"* be in place. Is it reasonable to expect that one needs a R20 microcontroller to read the personal information? This question remains unanswered, and can only be answered by the yet to be appointed information privacy regulator with certainty. Storing the AFC Data Structures in clear text should receive considerable review since it can be argued that clear text will not meet reasonable security measures. Contravening the Act can have a maximum penalty consequence of 10 years imprisonment and/or R 10 million. The Act gives a 1 year grace period before it will start with enforcement from date of commencement when it is announced.

6 PCI COMPLIANCE

The banking industry promotes and requires standards from the Payments Card Industry (PCI) standards body. This body started in 2006 to dictate controls around cardholder data to reduce credit card fraud via its exposure. For the EMV and AFC Data Structure type networks that Transport Authorities will require and operate, they specifically identify the PCI Digital Security Standard (DSS).

The PCI DSS standards' aim is to:

- Build and Maintain a Secure Network;
- Protect Cardholder Data;
- Maintain a Vulnerability Management Program;
- Implement Strong Access Control Measures;
- Regularly Monitor and Test Networks; and
- Maintain an Information Security Policy.

Although only 6 objectives, their standard goes into a 100 plus page document to explain how to achieve these objectives correctly. To be PCI-DSS compliant, one has to complete an annual assessment through an external assessor. Their definition of personally identifiable information differs from the POPI Act but there is still ample focus on the protection of such data. The current EMV system is not perfect with significant clear text transmissions between merchant to acquiring bank infrastructure in a clear text form, thus also hindering Confidentiality of the information. There is however a significant investment made on securing the networks and storage mediums the data are transmitted over and reside on via PCI.

The aim of PCI compliance is aligned with POPI, as long as one includes any personal information of the commuters as part of the information that needs to be secured and not just the payment card information.

7 CONCLUSION AND FUTURE WORK

South Africa took a step in the right direction when it published the AFC regulations in 2011. However, as indicated within this paper, the potential for misuse is real. The current method of AFC Data Structure implementation is not secure and a solution is required.

The author recognises that not all CA "*tag*" mechanisms are designed/made equal and that some, with minimal effort, can be made "***secure****"* with regard to Integrity and Availability aspects of information security. Confidentially aspects will have to be addressed on an EMV and CA standardisation level. This aspect needs further investigation and/or an official stance from the yet to be appointed information privacy regulator.

The following is recommended to ensure that AFC implementing authorities and private entities adhere to the vision of an integrated secure fare management system:

- The AFC Legislation needs to be amended to indicate that a minimum of tap-on information must be written to the AFC Data Structure;
- The AFC Legislation needs to be amended to require the bank issued fare media to have an independent counter for accessing "*unsecure*" "*tags*" which, upon the discretion of the issuer, will kill the payment application when "*roll-over*" occurs; and
- The AFC Legislation needs to be amended to require that only PCI-DSS compliant banks and transport authority networks should transmit EMV transactions.

Being on the "*bleeding edge*" unfortunately means some cuts will have to be endured, and remedied as they occur. It is this author's opinion that the current legislation leaves implementing authorities and the National Department of Transport at the mercy of the card association's "***tag****"* access mechanisms. The NDoT, without knowing, relinquished control of the access mechanisms and without remedial aspects will be facing revenue and reputational loss.

8 REFERENCES

ABE, C. 2010. 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.

ANDREAE, P. The History of EMV: An EMV Forefather Explains Why Chip is the Future. 2011. Online Interview: http://www.bankinfosecurity.com/interviews/history-emv-i-933

ATTOH-OKINE, N.O.; SHEN, L.D. 1995. "Security issues of emerging smart cards fare collection application in mass transit," Vehicle Navigation and Information Systems Conference, 1995. Proceedings. In conjunction with the Pacific Rim TransTech Conference. 6th International VNIS. 'A Ride into the Future' , vol., no., pp.523,526, 30 Jul-2Aug 1995

DE KONING GANS, G., HOEPMAN, J., GARCIA, F.D. 2008. A Practical Attack on the MIFARE Classic. In G. Grimaud and F.-X. Standaert, editors, 8th Smart Card Research and Advanced Application Conference (CARDIS 2008). Lecture Notes in Computer Science, Vol. 5189, pages 267-282, 2008. Springer Verlag.

DEMPSEY, S.P., 2008. Privacy Issues with the Use of Smart Cards. Legal Research Digest, p. 25.

Intrepidus. 2012. NFC For Free Rides and Rooms (on your phone). EUSecWest 2012. Conference: 20th September 2012

JOUBERT, D.J. 2010. Electronic Fare Collection: Convergence of Payment and Fare Media in South Africa. Masters Degree: Tshwane University of Technology

JOUBERT, D.J., BIERMANN, E. 2010. EMV Specification usage within Public Transport Automated Fare Collection. South African Transport Conference 2010.

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.

LOMBARD, J.A. 2010. Copying and restoring of unsecure data. Interview:Pretoria: NDoT Public Transport AFC Data Structure.

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

MCCUMBER, J. 1991, October. Information systems security: A comprehensive model. In Proceedings of the 14th National Computer Security Conference.

PELLETIER, M., TRÉPANIER, M., MORENCY, C. 2011. Smart card data use in public transit: A literature review, Transportation Research Part C: Emerging Technologies, Volume 19, Issue 4, August 2011, Pages 557-568, ISSN 0968-090X,

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.

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

SOUTH AFRICA. 2009. Official Release of Revision 1 of the Automated Fare Collection Data/File Structure. Open Letter.

SOUTH AFRICA. 2011. National Land Transport Act, 2009, Regulations Relating To Integrated Fare Systems, No 511 of 2011. Government Gazette 34363.

SOUTH AFRICA. 2013. Protection of Personal Information Act, No 4 of 2013. Government Gazette 37067.

SWART, I.P. 2014. Protection of Personal Information Act. Interview:Pretoria:POPI and the AFC Data Structure.

TRÉPANIER, M., BARJ, S., DUFOUR, C., POILPRÉ, R. 2004. Examination of the Potential Use of Smart Card Fare Collection System in Urban Transportation. Congrès annuel de 2004 de l'Association des transports du Canada, Québec.

VISA International. 2013. Transaction Acceptance Device Guide (TADG). Online: https://technologypartner.visa.com/Download.aspx?id=32