EMV Credit Card Parking Technology
Stakeholder obligations to ensure its proper implementation in Parking Systems
(Revised April 2014)

Introduction

This article is an update of a presentation prepared for the Parking Association of Australia in November 2011. In the past 2 ½ years some key changes have taken place with regards to EMV compliance and PCI Security Standards.

This document serves as a guide only and parking operators and owners seeking to update their credit card payment systems should consult their preferred banking institution.

Background to Fraud 1980 – Present

Credit card fraud losses to Visa and MasterCard alone have increased from $110 million in 1980 to an estimated $1.63 billion in 1995 around the world. The Australian Institute of Criminology has revealed the percentage of revenue lost to fraud increased by 55% from 2006 to 2009. The Australian Crime Commission 2011 report found that a total of 593,819 fraudulent credit card transactions occurred in 2010. 10% of Australians say they have been a victim of credit card fraud over the past 5 years, which is relatively low compared to some other countries (America and UK - 27%, China and Singapore – 15%, Germany – 8%, Dubai - 7%).

As internet security is making it increasingly harder for criminals to commit fraud, they are now moving into new vulnerable territory such as the unattended credit card payment environment which includes all vending machines, parking meters and petrol pumps that authorise card transactions. This area has seen a sharp increase in fraudulent activity in recent years. The image below shows a card skimming device on a petrol pump.
What is EMV?

EMV is an acronym for Europay – MasterCard - Visa and is a global standard for credit and debit payment cards based on chip card technology. As of the end of 2010, there were more than 1.24 billion EMV compliant chip-based payment cards in use worldwide.

EMV chip-based payment cards, also known as smart cards, contain an embedded microprocessor. The microprocessor chip contains the information needed to use the card for payment, and is protected by various security features. Chip cards are a more secure alternative to traditional magnetic stripe payment cards.

EMVCo\(^1\) is an organisation that manages, maintains and enhances the EMV Integrated Circuit Card Specifications for chip-based payment cards and acceptance devices, including point of sale (POS) terminals and ATMs. EMVCo also establishes and administers testing and approval processes to evaluate compliance with the EMV Specifications.

Key advantages of EMV

- EMV works with the embedded chip in the card (visible in the top left corner); therefore it is more secure than encoded magnetic stripe technology. Each new transaction generates a unique digital signature in the chip proving authenticity in an offline mode and prevents use of fraudulent cards.
- Superior levels of security are achieved by employing Public Key Cryptography. This is a key issued to the card reader provider that allows for an open source method of encrypting data. Asymmetric key encryption is employed where a public key is used for the encryption process and a private key used for the decryption process.
- EMV supports enhanced cardholder verification methods.
- Configuration of the card after it has been issued. This includes changing floor limits that allow transactions below a certain amount to be approved without querying the bank online. It also allows for the cancellation of stolen or void cards, etc.
- Contactless (Tap & Go) solution can be added at a later stage.
- Offline transactions are supported by EMV. Quite often a card holder is preauthorized for transactions up to $100 without any online verification needed.

The card scheme providers (MasterCard and Visa) have tried to encourage the adoption of EMV by emphasizing the lower financial risk associated with EMV credit card payments, via what they have coined as the “Liability Shift”.

The Liability Shift applies to the party (Issuer or Bank) responsible for all losses related to fraud resulting from non-EMV compliant card payment transactions. For example: “A merchant operating a magstripe-only terminal will be liable for any counterfeit fraud that is conducted at that terminal using a counterfeit card that was originally issued with a chip. The principle is that the fraud would have been prevented if the terminal had been chip-capable”\(^2\).

---

\(^1\) EMVCo - www.emvco.com
\(^2\) MasterCard – An introduction to chip
Evolution of Parking Payment Solutions

Parking meters and car parking systems have progressively adopted more complex payment methods to match current industry trends while also defending against fraudulent activity. This has required ongoing research and development as well as capital costs in upgrading equipment. The following flowchart shows the typical evolution experienced within the industry.

Payment Card Industry – Data Security Standards (PCI –DSS)

PCI security standards are technical and operational requirements set by the PCI Security Standards Council (PCI SSC) to protect cardholder data. The standards apply to all entities that store, process or transmit cardholder data – with guidance for software developers and manufacturers of applications and devices used in those transactions.

PCI DSS applies to all entities that store, process, and/or transmit cardholder data. It covers technical and operational system components included in or connected to cardholder data. If you are a merchant who accepts or processes payment cards, you must comply with the PCI DSS (the organisation).
PCI PA-DSS is for software developers and integrators of payment applications that store, process or transmit cardholder data as part of authorization or settlement when these applications are sold, distributed or licensed to third parties.

Although PA-DSS compliance is not required for software supplied by a service provider, it is still important to ensure that all software provided has undergone a PCI PA-DSS certification process by the software developer. In any event the software should include the following protections (as referenced from the PCI Security Standards website):

- Do not retain full magnetic stripe, card validation, code or value, or PIN block data.
- Protect stored cardholder data.
- Provide secure authentication features.
- Log payment application activity.
- Develop secure payment applications.
- Protect wireless transmissions.
- Test payment applications to address vulnerabilities.
- Facilitate secure network implementation.
- Cardholder data must never be stored on a server connected to the internet.
- Facilitate secure remote software updates.
- Facilitate secure remote access to payment application.

PCI PTS (PTS= PIN Transaction Security) is a set of security requirements focused on characteristics and management of devices used in the protection of cardholder PINs and other payment processing related activities. These requirements generally apply to the Card Acceptance Terminal (CAT Device). The requirements are for manufacturers to follow in the design, manufacture and transport of a device to the entity that implements it.

In June 2013 The PCI Security Standards Council released version 4 of the PCI PTS standard. This document supports the submission of products under the following categories:

- “PIN Entry Devices” or “Unattended Payment Terminal – Point of Interaction”
- Non-PIN acceptance Point of Interaction devices evaluated for account data protection
- Encrypting PIN pads that require integration into POS terminals or ATMs.
- Secure components for POS terminals

The standard can be referenced at the following link:
https://www.pcisecuritystandards.org/documents/PCI_PTS_POI_SRs_v4_Final.pdf

Parking Equipment suppliers may believe that as a service provider, they do not require any certification in this regard. In any case, it is understood that they have likely acquired the card reader from a third party vendor and therefore any relevant PCI certification (i.e. relating to the CAT device itself) should be available.

Contactless Card Payments

Any new parking equipment installations require a fully compliant EMV credit card solution that includes both a contact reader and a contactless card reader. At this stage the contactless reader should interface with PayPass and PayWave as a minimum. In the future it is anticipated that the contactless card reader will interface with NFC enabled mobile devices.

Some key considerations when installing a contactless solution include:
• Customer workflow – how does a customer purchase a ticket and how is the contactless reader activated during a transaction (i.e. powered up to process a card transaction). The contactless reader cannot drain the battery excessively if the device is not mains powered (i.e. a parking meter).
• Is the contactless reader a separate unit attached to the outside of the meter/equipment housing - or is it integrated within the front fascia?

**How PCI differs from EMV**

**EMV by itself does not protect the confidentiality of, or inappropriate access to sensitive cardholder data.**

Current EMV acceptance and processing environments may process both EMV and non-EMV transactions, (such as magnetic stripe). These non-EMV transactions do not have the same fraud-reduction capabilities of EMV transactions and, consequently, require additional protection which is outlined in the PCI data security standards.

In addition, it is important to note that in EMV environments, the PAN is not kept confidential at any point in the transaction, indeed, it is necessary for the PAN to be processed by the point-of-sale terminal unencrypted in order to complete critical steps in the EMV transaction process. The expiry date and other cardholder data are also transmitted in clear-text.

The potential for these transaction types and/or data elements to be exposed and used fraudulently within both the face-to-face channel and the card-not-present channel are the reasons why it is necessary to implement PCI DSS in today’s EMV acceptance environment(s).

By design, PCI DSS does not distinguish between underlying transaction security mechanisms, but instead seeks to protect the PAN and other sensitive authentication data. Both PCI and EMV are essential elements in the fight against fraud and data exposure. Together they provide the greatest level of security for cardholder data throughout the entire transaction process.

**Key Dates for Implementation**

According to a media release from CBA³, EMV should have already been implemented in any parking systems currently in operation. The date CBA originally prescribed for final implementation of EMV was 1st April 2014. As the date has now lapsed, parking operators that are not currently EMV compliant should consult with their preferred bank on which steps they need to take. The following are the key items from the CBA media release:

- **EMV Compliance Mandate:**
  - Visa and MasterCard have mandated that all terminals that accept their cards must be able to process the more secure EMV chip cards.
  - Compliance is already required for any new devices being deployed to the market.
- **Visa Chip and Pin Mandate:**
  - Visa has issued a mandate requiring all chip card transactions to be approved with a PIN. Unattended devices (i.e. parking machines) are exempt from this mandate.
- **PayPass functionality for Merchant categories:**
  - MasterCard have issued a mandate that requires that all merchants within certain merchant category codes (MCCs) must be able to accept and process PayPass cards via a contactless reader.

---

³ *CBA Unattended EMV/PayPass Compliance FAQ - 2013*
Key Issues in Implementing EMV

The following issues are common for most merchants at present:
- Parking Equipment upgrade costs
- What are the penalties for non-compliance?
- Does the bank have a say in regards to the merchant’s choice of equipment supplier?
- In light of the recent announcements from Visa and MC, if a merchant has recently bought equipment that is not EMV enabled – but the upgrade costs are high – what can they do legally?
- Contactless must be included in all new equipment installations, thereby increasing capital outlay.
- Transactions under $100 do not require PIN authentications
- Will there be reductions in merchant fees as an incentive to change?

How can your bank help you through the EMV process?

Your bank should provide written advice regarding the changes to EMV transactions including:
- Timeframes
- Fines
- Liability shifts
- Technical direction for the long term
- Provide advice on PCI and EMV standards
- Review current credit card payment solutions from suppliers
- Project manage the EMV certification process with the gateway providers, suppliers and independent certification agencies (e.g. Witham Labs and FIME)

EMV Certification Process

The process of obtaining EMV certification is usually an initiative of the parking equipment supplier – however requires close coordination and project management between all parties (refer to figure on next page).

There are 2 formal levels of certification for EMV:

EMV Level 1 Certification: This includes the certification of the hardware itself and includes the Card acceptance terminal.

EMV Level 2 Certification: This includes the software kernel that manages the EMV process with the Card Acceptance Terminal.

There is also a third and final certification process that includes the interface to the financial institutions. The way EMV works is through close integration to the banking environment. This can only be achieved through a complex process involving several organisations. A central independent certifying body (e.g. FIME) verifies that the EMV solution has completed what is termed as an “End to End” EMV transaction. This involves testing individual credit card transactions through a complete banking environment – from the card reader through various gateways and onto the card issuer itself. Organisations such as FIME specialise in this type of certification.
Please note that EMV certified hardware/software (i.e. EMV level 1 and 2) alone, does not constitute a complete EMV solution. The end-to-end process must be tested and certified for EMV compliance. For example, the following certifications are provided by your preferred supplier if they are interfacing with the MIGS payment gateway:

- Visa ADVT
- Visa VCPS (Contactless)
- MasterCard M-TIP
- MasterCard M-TIP - PayPass

A supplier using a non-MIGS gateway will require similar documentation from the gateway provider that verifies that their product is an EMV end-to-end solution.
Conclusion

- Any EMV solution deployed in an unattended environment (such as a parking meter or pay stations) must be “end to end” compliant between the device and the financial institution.
- A device that is EMV level 1 or EMV level 2 compliant is not necessarily “end to end” compliant.
- Suppliers must provide technical diagrams and specifications verified by the merchant’s bank.
- The bank is expected to have a clear vision and roadmap for EMV and contactless in the unattended space – including liability rules, fines and technical aspects of EMV for both MasterCard and Visa.
- The merchant (Council, car park owners) must be given a chance to upgrade their current facilities with sufficient time to allow for budgeting, procurement and implementation.

For more information or assistance with EMV, contact us on +612 8920 0800 or pci@parkingconsultants.com

Glenn Caldwell, Consultant