



**A SMART CARD ALLIANCE TRANSPORTATION COUNCIL WHITE PAPER DEVELOPED IN PARTNERSHIP WITH THE INTERNATIONAL PARKING INSTITUTE**

# EMV and Parking

Publication Date: June 2015
Publication Number: TC-15001

**Smart Card Alliance**
191 Clarksville Rd.
Princeton Junction, NJ 08550
www.smartcardalliance.org

# About the Smart Card Alliance

The Smart Card Alliance is a not-for-profit, multi-industry association working to stimulate the understanding, adoption, use and widespread application of smart card technology. Through specific projects such as education programs, market research, advocacy, industry relations and open forums, the Alliance keeps its members connected to industry leaders and innovative thought. The Alliance is the single industry voice for smart cards, leading industry discussion on the impact and value of smart cards in the U.S. and Latin America. For more information please visit http://www.smartcardalliance.org.

# About the International Parking Institute

The International Parking Institute (IPI) is the world's largest association of parking professionals and the parking industry. Parking is integral to transportation flow, economic development, land use, law enforcement, architectural aesthetics and overall quality of life. With the parking industry's wide-ranging impact, IPI members include professionals from cities, port authorities, civic centers, academic institutions, hospitals and healthcare facilities, airports, corporate complexes, race tracks, transit and transportation agencies, retail, hospitality, entertainment and sports centers, architects, engineers, financial consultants and urban planners, as well as the suppliers of equipment, products and services to the parking and transportation industries. www.parking.org.

# Table of Contents

# 1 Introduction

As the United States moves to an EMV payments infrastructure, parking industry stakeholders across the payments value chain recognize the need to learn about EMV in order to plan for EMV migration. With the October 2015 EMV fraud liability shifts, parking industry stakeholders need to review their current payments infrastructure and develop their strategy and plan for EMV migration.

The Smart Card Alliance and the International Parking Institute (IPI) have partnered to assist parking industry stakeholders with understanding the transition to EMV and the fraud liability shift. The purpose of this collaborative white paper, the first step in this partnership, is to inform and educate the industry about EMV in the parking industry.

This white paper covers the critical aspects of deploying EMV-compliant solutions within the parking infrastructure. The primary audiences are parking merchants and suppliers and integrators of parking equipment, software, and support services. The white paper provides the following information:

- An overview of relevant EMV chip technology features and key implementation options
- Key milestones and guidance for U.S. EMV migration, as announced by the payment networks
- Key considerations for parking industry stakeholders who want to accept and process EMV chip transactions in both attended and unattended environments
- The relationship between U.S. contactless bank card transactions and NFC-enabled mobile payments and EMV

## 1.1 History of EMV and U.S. Migration

The EMV global payment standard was developed in 1994 by three credit card brands: Europay, MasterCard, and Visa. The standard is currently managed by EMVCo.[1]

The intention of the original specification developers was to examine the vulnerability of the bank card process and consider technologies and practices that could diminish or eliminate fraud in the card-present environment. Relevant information was gathered from the banking industry, card processing entities, and technology providers. This information pointed to the benefits of chip-based technology for payment processing, including standards that would ensure global interoperability and acceptance. The first version of the EMV specification was published in 1996. The production version of the EMV specifications, Version 3.1.1, was published in 1998.

The challenge with any type of global specification is to keep up with an ever-changing technological landscape and operational demands. One motivation for EMVCo was to create specifications that would encompass backwards compatibility (within reason). The intention was to protect the investments made by payment ecosystem stakeholders in infrastructure and technology and avoid prohibitive payment card processing costs.

Financial institutions in Europe, Latin America, Asia/Pacific, Canada, and the United States are already either issuing EMV chip cards for credit and debit payment or migrating to EMV. According to EMVCo, approximately 3.7 billion EMV chip cards have been issued globally, and 36.9 million point-of-sale (POS) terminals accept EMV chip cards, as of the fourth quarter of 2014.[2] EMVCo also reported that 32 percent of

[1] Information on the EMV specifications and the EMVCo organization is available at http://www.emvco.com.

[2] EMVCo, "EMVCo Reports 3.4 Billion EMV Chip Payment Cards in Global Circulation," press release, May 6, 2015, http://www.emvco.com/media_center.aspx?id=48.

all chip card-present transactions conducted between January and December 2014—both contact and contactless—used EMV chip technology. Europe Zone 1 maintained the highest percentage of EMV chip transactions, which accounted for nearly 97 percent of card-present payments.

The U.S. is now migrating to EMV chip technology. Between July 2011 and June 2012, American Express, Discover, MasterCard, and Visa announced plans to move to an EMV-based payments infrastructure within the U.S. The plans include a series of incentives and policy changes for card issuers and merchants, with a target date of October 2015 to complete implementation of EMV chip cards, terminals, and processing systems. According to the EMV Migration Forum[3], as of the end of 2014, approximately 120 million cards have been issued and 4.5 million EMV-capable terminals have been installed, accounting for approximately 10 percent of the cards in the market and 37 percent of the POS terminals. Additional growth is expected in 2015: the EMV Migration Forum estimated that 50 percent of cards issued (600 million cards) will be chip cards and 60 percent of all POS terminals (7 million terminals) will be enabled to accept chip cards by the end of the year.

## 1.2 Why EMV

Issuers around the world are issuing chip cards and merchants are moving to EMV-compliant terminals to increase security and reduce the incidence of card-present fraud resulting from the use of counterfeit cards. Additionally, other fraud types (e.g., use of lost or stolen cards) can be reduced by prompting a customer to enter a PIN, which is assumed to be known only to the cardholder to whom the card was issued.

Adopting EMV technology can both create a more secure payments environment for the parking industry and reduce parking operators' and owners' liability for fraudulent transactions. It is important to note that there is no mandate for merchants or parking owners or operators to implement EMV technology; however, the payment networks' fraud liability shifts take effect in October 2015. Lost or stolen and counterfeit card fraud rates may currently be very low in situations where fraudulent parking purchases are unlikely. The implementation decision is a business decision that should be based on current fraud rates and the potential for increased fraud for non-EMV-compliant acceptance as the rest of U.S. payments acceptance infrastructure migrates to EMV.

### 1.2.1 EMV Fraud Liability Shift Timeline

EMV migration globally has been driven by the need to reduce fraud losses, by payment network requirements and incentives, and by fraud liability shifts, which specify that liability for fraudulent transactions is, in general, born by the party with the least secure technology. In 2011 and 2012, all of the global payment networks announced plans for U.S. migration to EMV. The different payment networks all have slightly different fraud liability shift dates, but the two most important dates are the same: October 2015 is the fraud liability shift date for merchants, and October 2017 is the fraud liability shift date for automated fuel dispensers. (Additional information on fraud liability shifts can be found in an EMV Migration Forum white paper.[4])

Beginning in October 2015, global payment networks and certain U.S. debit networks plan to implement fraud liability shifts that will affect card-present counterfeit chip card transactions and lost or stolen chip card transactions. As of that date, liability for those transactions generally will shift to the merchant if the merchant does not use EMV chip-enabled devices and applications to process payment transactions. The

---

[3] The EMV Migration Forum is a cross-industry body focused on supporting the EMV chip implementation steps required for payment networks, issuers, processors, merchants, and consumers to help ensure a successful introduction of more secure chip technology in the United States. Additional information can be found at: http://www.emv-connection.com/emv-migration-forum/.

[4] EMV Migration Forum, "Understanding the 2015 U.S. Fraud Liability Shifts," May 2015, http://www.emv-connection.com.

impact of the October 2015 liability shifts to the merchant depends on two conditions:

- Whether EMV chip cards (domestic and international, including credit and debit cards) are used.
- Whether EMV chip-enabled POS card payment acceptance applications and devices are deployed. Automated teller machines (ATMs) and automated fuel dispensers are excluded, but in-person POS retail devices, unattended terminals, kiosks, vending machines, and mobile payment acceptance devices are included.

### 1.2.2 Liability Shift Applicability to Acquirers/Merchants

The liability shift for acquirers/merchants is defined as follows: after October 2015, if a merchant accepts a magnetic stripe card that was counterfeited with track data copied from an EMV chip card, and the merchant has a POS terminal that is not EMV chip-enabled, the acquirer/merchant may be liable for the fraudulent transaction. Before the shift, issuers bore the risk for counterfeit card use at physical merchant locations. American Express, Discover, and MasterCard also have a lost or stolen liability shift, which impacts lost or stolen PIN-preferring chip cards used at less secure acceptance devices.

If the acquirer/merchant implements the appropriate EMV acceptance devices on or before October 2015, the payment networks (American Express, Discover, MasterCard, and Visa) and the card-issuing banks will continue to assume the liability for fraudulent transactions resulting from use of their customers' cards.

While unrelated to EMV implementation, compliance with the Payment Card Industry Data Security Standard (PCI DSS) is also essential to securing the payments infrastructure. One of the payment network incentives to move the industry to EMV is a reduction in PCI assessment based on implementation of EMV processing. Each organization should check with the PCI Qualified Security Assessor team to determine what those reductions will entail.

## 1.3 U.S. EMV Implementation Milestones

The four major card payment networks have announced EMV implementation milestones. The following milestones apply to bank card processing in the United States:

- October 2012: PCI audit relief

  If more than 75 percent of a merchant's transactions originate from EMV chip-enabled POS terminals that support both contact and contactless transactions, the merchant can apply for relief from the audit requirement for PCI DSS compliance. The operation is still required to be PCI compliant.
- April 2013: Acquirer compliance

  Acquirers and sub-processors must be enabled to handle full EMV chip data in transactions.
- July 2015: EMV unattended liability shift

  All online-capable, chip-enabled (contact and contactless) unattended terminals (ATMs excluded) must support the processing of transactions without a cardholder verification method (CVM). (CVMs are described in Section 1.4.2.)
- October 2015: Fraud liability shift for card-present transactions, including counterfeit fraud liability shift and lost or stolen fraud liability shift (described below). This is the milestone that impacts parking industry stakeholders.
- October 2017: Fraud liability shift for automated fuel dispensers

  This fraud liability shift includes automated fuel dispensing equipment.

The October 2015 counterfeit fraud liability shift protects a party who invests in EMV deployment from financial liability for fraud losses from card-present counterfeit transactions. Today, across payment

networks, liability for card-present fraudulent transactions is generally the responsibility of card issuers. The counterfeit liability shift applies to transactions involving American Express, China UnionPay, Discover, MasterCard, Visa, and certain U.S. regional debit networks. American Express, Discover, and MasterCard also have a lost or stolen fraud liability shift. If a lost or stolen PIN-preferring chip card is used at a less secure terminal, fraud liability shifts to the acquirer/merchant.[5]

## 1.4 EMV Transaction Process[6]

Traditional credit cards encode the information required for a transaction on a magnetic stripe. The information is static; data are read when the card is swiped through a reader. The terminal then transmits the static data for processing. The card is no longer needed for the transaction

The logic behind EMV transaction processing is not radically different from the logic behind magnetic stripe transaction processing. Like magnetic stripe transaction processing, EMV transaction processing includes multiple steps, such as card authentication, risk assessment and fraud detection, and optionally, PIN or signature verification. Unlike magnetic stripe cards, however, EMV chip cards are designed to store sensitive data (such as PINs or security keys) securely. In addition, they have processing power that allows the cards to manage risk and perform cryptographic computations dynamically.

Secure chip technology allows EMV processing to incorporate features that can enhance security:

- Enhanced card authentication methods that rely on dynamic data.
- The potential to define flexible cardholder verification methods. For example, banks that manage multiple card portfolios can configure some cards to be PIN-preferring and other cards to be signature-preferring.

The EMV transaction authorization process works as follows:

1. The cardholder inserts an EMV chip card into a reader or taps the card on the reader (in the case of a contactless transaction). The contact chip card stays in the reader until the transaction is complete.
2. The POS terminal identifies what payment network's application is on the card.
3. The terminal selects the appropriate EMV application and uses the data set associated with the payment network to enforce the network's application requirements.
4. The card and terminal follow an EMV-specified protocol to conduct a dialog that allows each of them to execute their respective risk-management processes.

### 1.4.1 Card Authentication

One of the key attributes of EMV is the ability to authenticate a card to ensure that it is not a clone or counterfeit card. The EMV specification defines two card authentication methods, offline and online. While the U.S. is largely an online-only market, online vs. offline authentication is an implementation choice by issuers and merchants.

Offline card authentication uses asymmetric cryptography to allow merchants to replace physical inspection of a card with electronic card authentication before requesting authorization from the issuer.

---

[5] Ibid.

[6] Content is from the Smart Card Alliance Payments Council white paper, "Technologies for Payment Fraud Prevention: EMV, Encryption and Tokenization," October 2014, http://www.smartcardalliance.org/publications-technologies-for-payment-fraud-prevention-emv-encryption-and-tokenization/

Online card authentication is performed as part of the real-time authorization process, similar to what is done for a magnetic stripe transaction, allowing the issuer to authenticate the card and authorize the transaction. The important difference is that the card uses symmetric key technology to generate a unique application cryptogram. This cryptogram, called the authorization request cryptogram, is sent to and authenticated by the issuer as part of the authorization request.

These cryptographic processes enable EMV to protect card-present transactions from counterfeit fraud and skimming. The chip generates unique digital signatures and cryptograms by applying an algorithm to data provided by the card and the acceptance device and to transaction-specific data (e.g., card verification result, application transaction counter value, amount of the transaction, the date, and a terminal-generated unpredictable number).

### 1.4.2 Cardholder Verification Method (CVM)

An EMV transaction includes several elements that contribute to transaction validation. One of these is the CVM. The intent of the CVM is to authenticate the cardholder at the time of the transaction. The issuer prioritizes CVMs based on the risk associated with the transaction.

EMV currently supports four types of CVMs:

- Chip and signature
- Chip and online PIN
- Chip and offline PIN
- Chip with no cardholder verification method (no CVM)

Chip and signature is similar to cardholder verification used currently for magnetic-stripe card transactions. The consumer's signature is captured at every transaction.

With chip and online PIN, the terminal sends the cardholder-entered PIN to the card issuer to be validated.

For chip and offline PIN, the PIN entered by the consumer is matched to the PIN that is securely stored on the EMV chip card, rather than being sent to the issuer for verification. Chip and offline PIN functionality is exclusive to EMV card transactions.

In high volume, low-dollar transactions at merchants in low-risk categories (such as fast food, transit, parking, convenience stores, and automated kiosk locations), "no CVM" (requiring neither PIN nor signature) is often preferred for transactions (and may be required by some payment networks and merchant categories). No CVM transactions are processed without the cardholder's PIN or signature.

Many issuers in the U.S. thus far have chosen to issue signature-preferring EMV chip cards that do not support PIN transactions. For cards without a PIN, the available CVMs are typically signature and no CVM. It is important to note that depending on payment network rules and issuer preference, chip cards are usually configured to accommodate multiple types of CVMs, to ensure acceptance at a wide variety of terminal types with different CVM requirements.

U.S. EMV chip cards will be a mix of signature-preferring cards and PIN-preferring cards. To date, the majority of EMV chip credit cards issued have been signature-preferring; EMV chip debit cards using the U.S. common debit application identifier (AID) will be online PIN-preferring.

# 2 Considerations for Deploying EMV in a Parking Environment

The parking industry is seeing an increase in EMV requirements for parking payment solutions. Since EMV migration can be a lengthy and complex process, parking equipment manufacturers and operators should perform an impact analysis to understand the scope of the upgrade effort. The following sections highlight some of the key EMV migration considerations for parking equipment manufacturers, integrators, and operators.

## 2.1 Chip Card Readers and PIN Pads

EMV chip-enabled POS terminals are available in many form factors and sizes and can support both contact and contactless chip card acceptance. The choice of a terminal depends on what CVMs the merchant wants to accept and the prospective transaction location. For example, at a typical retail location with a cashier stand (such as at a retail store), the terminals shown in Figure 1 may be appropriate choices. These terminals include a slot on the right side that accommodates magnetic stripe credit cards and a slot on the bottom that accommodates chip cards.

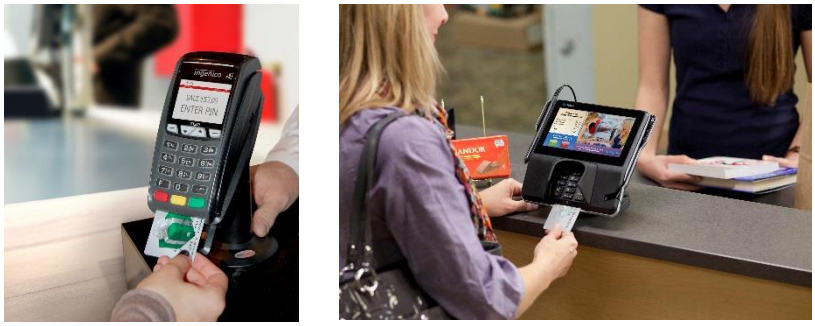

**Figure 1. Examples of Chip-Enabled POS Terminals[7]**

Installing this type of chip-enabled terminal is straightforward, in that little or no structural work is required. Implementation costs include the new terminals, any needed software, and training.

In situations where the chip-enabled terminal must be incorporated into a specific device or infrastructure, the form factor is more of a concern. Retrofitting payment kiosks such as in parking pay on foot machines, in-lane payment devices, or any other type of unattended payment device to include EMV chip-enabled terminals raises two questions:

- Whether space is available on the face of the device to accommodate the larger faceplates of the reader terminals
- Whether space is available within the actual device to accommodate the electronic and mechanical requirements of the reader terminals

Examples of terminals that can be incorporated into kiosk devices are shown in Figure 2.

[7] Photos provided by Ingenico and Verifone.

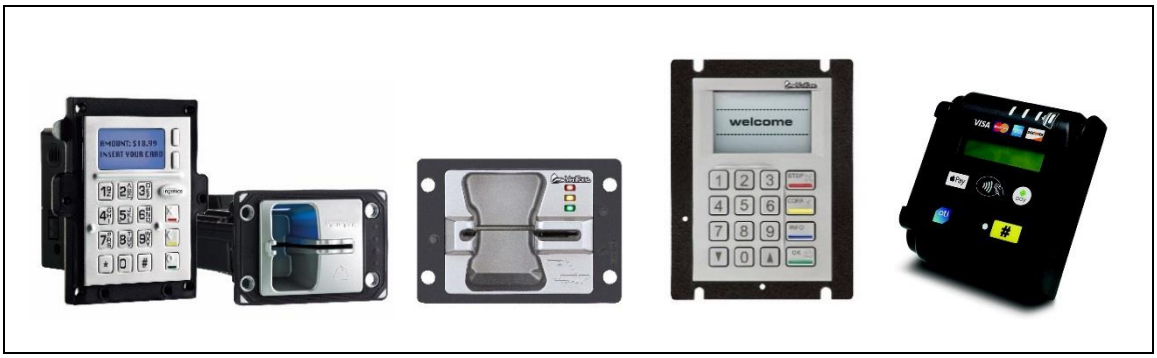


**Figure 2. Examples of Chip-Enabled Devices for Kiosks[8]**

Most parking access revenue control system (PARCS) manufacturers are including additional room in their new generations of devices to accommodate the EMV chip-enabled reader and PIN pad. In certain situations, a parking payment device may not be able to be retrofit to accommodate the appropriate EMV chip-enabled reader.

EMV transactions involve a dialog between the chip card and the chip card reader and (potentially) a PIN pad. The process by which chip card readers and PIN pads are selected should include the following:

- Identify what acceptance terminal capabilities are needed. For example, determine if there is a need to support a PIN pad or if contactless or NFC transaction acceptance is desired.
- Purchase acceptance terminals that are approved by EMVCo and the payment networks. Request EMVCo and payment network letters of approval from providers.[9]
- Purchase only PCI-approved PIN entry devices.[10]
- Consult with merchant acquirers to find out what devices they offer and what is needed to enable EMV capability on an acquirer's platform (including certification).
- Review the documentation and support provided by the chip card reader and PIN pad vendor to determine the complexity of integrating the device with other equipment.
- Consider implementing an acceptance device that also supports contactless transactions to be able to accept both contactless card and mobile NFC contactless transactions (e.g., Apple Pay, Android Pay).

It is important to note that in unattended environments such as parking, the payment networks require support for "no CVM," so a PIN pad may not be required unless the parking operator is concerned about lost or stolen card fraud.

## 2.2 EMV Messaging Impact

EMV transactions send data from the POS device to the acquirer processor and issuer. U.S. acquirers and sub-processors were required to accept full EMV chip data in transactions as of April 2013. Key interface and messaging activities include the following:

[8] Photos provided by Ingenico, OTI America and Verifone.

[9] Approved terminals are listed on the EMVCo web site, at https://www.emvco.com/approvals.aspx?id=83.

[10] Approved devices are listed on the PCI web site, at https://www.pcisecuritystandards.org/approved_companies_providers/approved_pin_transaction_security.php.

- Consult with the parking operator's acquirer to determine whether EMV is supported.
- Determine what changes are required in the parking operator's back-end host systems to support EMV processing.
- Determine which processors need to be supported and what the interface requirements are for supporting new EMV data fields and process flows.

## 2.3 Testing and Certification

EMV implementation requires that devices, software, and end-to-end implementation be certified. Key certification activities include the following:

- Parking equipment providers should work with their PARCS integrator and the acquirer processor to plan and execute the certification process.
- Locations that plan to deploy a new parking revenue control system or update their existing system should only purchase devices that are approved by EMVCo and the payment networks. Working with the PARCS integrator to plan and execute a successful end-to-end test is recommended.

The EMV certification process is more complex and structured than the current merchant–processing agent certification process. Most payment card hardware devices are currently processor and payment-software independent. The EMV certification process involves integration testing with the terminal, the software, and the acquirer. In addition, each payment network (American Express, Discover, MasterCard, and Visa) has very specific acquirer-host and EMV chip-enabled terminal testing criteria. Each has defined processes to verify functionality, ensure the integrity of the payment network infrastructure, and provide a positive payment experience for the cardholder.

## 2.4 Terminal Management System

As with any new POS terminal deployment, considerations include how terminals will be managed and updated. A terminal management system allows for efficient and timely management and deployment of updates to installed terminals.

## 2.5 Other Payment or Security Functionality

Many merchants use EMV migration as an opportunity to evaluate their payment and payment security strategy for other potential changes. For example, since the payment card acceptance infrastructure is being updated for EMV, perhaps contactless and NFC functionality should also be enabled, or other security technologies such as point-to-point encryption (P2PE), end-to-end encryption (E2EE) or tokenization should be implemented.[11] If implementing P2PE, it is important to deploy solutions validated by PCI.[12]

## 2.6 Other EMV Deployment Considerations

As part of EMV migration planning, parking operators need to consider the cardholder experience. Guidance at unattended terminals can help inexperienced cardholders understand that they must insert the chip card (as opposed to swiping a magnetic stripe card). It is also important to consider the placement of the chip

[11] For additional information on the roles of EMV, encryption and tokenization in providing transaction security, see the Smart Card Alliance Payments Council white paper, "Technologies for Payment Fraud Prevention: EMV, Encryption and Tokenization," http://www.smartcardalliance.org/publications-technologies-for-payment-fraud-prevention-emv-encryption-and-tokenization/.

[12] "Validated Point-to-Point Encryption (P2PE), PCI Security Standards Council, https://www.pcisecuritystandards.org/approved_companies_providers/validated_p2pe_solutions.php.

acceptance devices, to allow for easy cardholder access, and how the requirements for completing a chip card transaction (e.g., inserting rather than swiping the card or entering a PIN) may impact queuing.

# 3 EMV Deployment and Parking Payment

The parking industry processes card payments for a variety of products and services. A significant number of these transactions are card-not-present transactions, including parking credential or parking pass payments made online, citation payments, deposits, and towing fees. However, many transactions are still card-present transactions, in which the patron must present a payment card to a cashier or device.

Parking payments can take place in a variety of locations. From the early 1900s through the mid-1930s, payments were made with cash and required person-to-person interaction. With the introduction of the first parking meter, the Park-O-Meter, in the mid-1930s, payments could be collected from the parker without human intervention. In the early 1970s, parking payments could be made using credit cards, but processing involved the use of manual impression devices, commonly called "knuckle draggers," and still required the presence of a cashier. The 1980s saw the introduction of credit card readers that read the magnetic stripe and transmitted the information over a telephone modem. In the 1990s, credit card processing advanced to enable the parker to pay without involving a cashier, and to introduce payment processing over an Ethernet connection and increasing reliance on software.

While there are still situations in which a cashier processes payment transactions, the incidence of unattended parking payment processing is increasing significantly. In such parking transactions, as with all payment card transactions, vigilance and compliance are critical to preventing fraud.

## 3.1 Parking Payment Scenarios

Currently, parking is paid for according to different scenarios, depending on the location of the parking space and the logistics preferred by the parking operator. The deployment of EMV chip cards has different implications for the different scenarios.

### 3.1.1 Attended In-Lane Cashiering

In certain locations, parking patrons pay for parking at a cashier booth from their cars (in-lane cashiering). After processing the parking ticket, the cashier indicates the fee, and the patron pays with cash or a bank card.

The use of chip cards raises two considerations. First, the EMV chip-enabled terminal is consistent with the POS hardware that could be deployed at general retail locations. The second consideration is whether the parking operator wants to support PIN acceptance. If the transaction requires only a supporting signature or no CVM (see Section 1.4.2 for a description of CVMs), the payment process is similar to the current process. The patron hands the cashier the card, the cashier inserts the card into the EMV chip-enabled terminal, and the transaction is processed. If PIN support is desired, the PIN pad must be accessible by the parking patron who is in a vehicle outside the cashier booth. In many cases, the logistics of this type of terminal access may require significant adjustments to or replacement of the cashier booth.

### 3.1.2 Attended Central Cashiering

Parking patrons can also pay parking fees by walking up to a cashier or other payment location. As with in-lane processing, the EMV chip-enabled terminal is consistent with POS hardware that could be deployed at general retail locations. In addition, because payment is made by a patron on foot, a counter-type operation is viable and would most likely not require significant changes to the payment area.

### 3.1.3 Unattended Pay on Foot and Parking Meters

Pay on foot devices can include both the automatic pay stations normally associated with gated parking facilities and metered payment devices. Metered payment devices include both single-space meters and multispace meters, often referred to as pay-by-space or pay-and-display. In all scenarios, the payment is made by a parking patron on foot. Most pay station devices currently accept credit and debit cards. These devices currently house magnetic stripe credit card readers.

The physical attributes of an EMV chip-enabled terminal are significantly different from those of a traditional magnetic stripe credit card reader. If a PIN pad is also desired, accommodating the reader and pad can be difficult, especially in situations in which the payment device itself is small and self-contained (such as an individual parking meter and many multi-space meters).

### 3.1.4 Unattended Pay in Lane

Pay in lane devices can process parking payments made by a driver in a vehicle located in the exit lane and adjacent to the payment device. While a few devices accept either cash or bank cards, the majority of pay in lane devices are designed to accept only card payments that don't require a PIN. In addition, this method of payment processing has become increasingly popular as more parking facilities, such as at airports, deploy this option, offering sound customer service, reasonable labor savings, and increased patron throughput.

However, as is true for pay on foot devices and metered payment devices, EMV deployment can represent a challenge in terms of space limitations, especially if the parking operator implements a PIN pad. Hardware space is at a premium within the pay in lane devices; an additional consideration is the orientation of the hardware in relation to the driver and the time required for the driver to enter a PIN.

## 3.2 Parking Payment Transactions

EMV migration has an impact on payment transactions made using in-lane cashiering, pay on foot devices, and pay in lane devices. All stakeholders are affected: customers, merchants, parking equipment vendors, and processors.

This impact is partially due to a fundamental difference between how a magnetic stripe transaction is processed and how an EMV chip transaction is processed. In magnetic stripe transactions, the card is simply a data store. The terminal reads the card data, then passes the data to the payment processor for processing and verification. EMV transactions differ in that the chip can process information and communicate with the chip-enabled terminal to determine many of the payment rules (for example, which CVM will be used and whether the card is authenticated online or offline). The issuer can also set rules that will result in the chip declining the transaction when the terminal is unable to provide the services requested by the chip.

The protocol for the interaction between the chip and the terminal in an EMV transaction is defined by the EMV specifications. The protocol prescribes a series of steps (Figure 3).

### 3.2.1 Impact on Transaction Speeds

The negotiations between the card and the terminal and between the terminal and the customer can affect transaction speeds. The impact on speed is different for pay on foot transactions and pay in lane transactions. Furthermore, transaction speed is directly affected by the customer's familiarity with an EMV chip transaction and the mobility and attentiveness of the customer. If the customer is familiar with EMV chip transactions, the customer will be ready to interact with the terminal, resulting in faster transactions than when the customer is not familiar with the process. In addition, transactions at pay on foot stations may be faster than transactions that are initiated from within the vehicle.

It is also important to consider the impact of PIN-based transactions, if supported, on throughput. As discussed in Section 1.4.2, U.S.-issued EMV chip cards will be a mix of signature-preferring and PIN-preferring cards and often will support no CVM. No CVM transactions and contactless EMV transactions will provide faster throughput for parking payment.

Note that this white paper and the process described above focuses on contact EMV chip cards. Contactless EMV transactions (using a contactless card or NFC mobile device) follow a different process which is not covered in this white paper. A brief description of contactless EMV transactions can be found in Section 4.

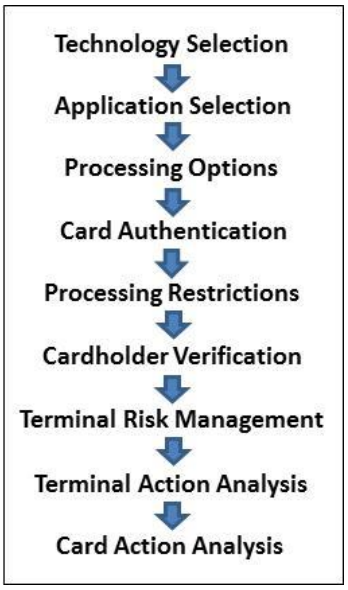


**Figure 3. Processing Steps for an EMV Contact Transaction**

### 3.2.2 Operational Impact

Implementing EMV chip technology may have impacts in addition to the potential for longer overall transaction times (particularly in the early stages of U.S. EMV migration, when cardholders are learning to use their chip cards). Such impacts can include:

- Higher maintenance costs for additional devices at pay stations to support PIN-preferring cards
- Higher full time equivalent (FTE) staffing during initial implementation to cashier services
- Potential ergonomics, safety and queueing issues for consumers who are reaching out of a car window to insert a card or enter a PIN (if required)

### 3.2.3 Implementation Requirements

To create a production EMV environment, the parking access revenue control system (PARCS) vendor must implement several interfaces:

- The physical interface in the payment station
- The interface between the payment station and the payment processor
- The physical interface in the chip-enabled terminal
- The interface between the chip-enabled terminal and the payment processor

Additional requirements include the following:

- The interface between the payment processor and the acquirer
- Certification of the interface between the payment processor and the acquirer
- End-to-end certification between the payment station and the acquirer

### 3.2.4 Staff and Customer Training

Parking operators need to consider and plan for staff training and communications with customers on the changes in the payment process. While not covered in this white paper, the customer experience is a critical part of EMV deployment planning. As a resource, the EMV Migration Forum publication, "Recommended Communications Best Practices," provides a guidance for retail merchants on developing effective messaging and education approaches before, during and after migration to EMV chip technology.[13] The GoChipCard.com web site also provides easy-to-understand resources for consumers and merchants on how and why payment transactions are changing.[14]

### 3.2.5 Cost Impact

EMV migration incurs certain costs.

Upgrades to equipment can vary for several reasons but principally due to the extent of upgrading an existing installation and the total number of hardware and software components that need to be upgraded. Additional costs incurred will typically include installation costs, certification of devices with payment processors and merchant acquirers (initial and ongoing), spare parts, signage at the POS, and staff and customer training.

The ongoing costs after EMV migration are the typical costs seen with payment acceptance.

PARCS vendors lose a certain amount of control over support because of the addition of components and the involvement of third parties. Implementation of EMV technology introduces additional vendors, who share responsibility for delivering an end-to-end solution. Ownership and accountability is no longer is the sole responsibility of the PARCS solution provider. Troubleshooting and repair becomes a responsibility that is shared between various equipment and service providers.

In addition, the PARCS solution provider is no longer solely responsible for making sure certified devices are available. Availability now becomes the responsibility of device equipment manufacturers, which needs to be coordinated with the certification process required by the payment card industry.

[13] "Recommended Communications Best Practices," EMV Migration Forum, http://www.emv-connection.com/recommended-communications-best-practices/.

[14] GoChipCard.com, http://www.gochipcard.com. This web site was developed by the EMV Migration Forum and the Payments Security Task Force to provide easy-to-use resources on chips cards for consumers, merchants and issuers.

# 4 EMV and NFC Mobile Payments

The EMV standard is defined by technical specifications and processing methodologies that are designed to secure card-present credit and debit card transactions. An EMV transaction can be implemented by inserting the chip card into an EMV reader (a contact transaction) or by holding a chip-based contactless card (or other device with an EMV payment application and an NFC interface, such as a smartphone) in close proximity to a contactless chip-enabled reader.

NFC is a technology similar to Bluetooth that enables a radio frequency connection between two electronically compatible devices located within close proximity. NFC-enabled mobile devices can support EMV chip transactions.

The increasing acceptance of NFC-enabled electronic wallet applications, such as Apple Pay and Android Pay, will encourage the adoption of POS devices capable of processing NFC payments. In addition, a magnetic stripe card can be enrolled in an electronic wallet application. When the application is presented for payment at an EMV terminal, the transaction becomes an EMV transaction, with all the associated protection, even though the payment card is actually a traditional magnetic stripe card.

Since the POS acceptance infrastructure is changing with EMV, parking operators should consider supporting contactless and mobile NFC transactions as part of the upgrade. By combining this migration, the operator may have a better return on investment and will be ready for future payment mechanisms.

The parking industry is also implementing in-app mobile payment for parking. These implementations are card-not-present transactions and are not EMV chip transactions. Additional information on the types of mobile payments can be found in Appendix A.

# 5 Conclusions

EMV is an open standard for chip-based payment cards and acceptance infrastructure that was designed to protect against card-present fraud resulting from the use of counterfeit or lost and stolen cards and to improve the security of the transaction authorization process. EMV is a worldwide standard, which ensures global acceptance and interoperability, and supports form factors besides cards.

Now is the time for parking industry stakeholders to invest the time and, where appropriate, the funds to prepare for the migration to EMV. EMV migration requires a lot of decisions and infrastructure changes and takes time. This is also an opportune time for parking operators to review their overall payments strategy and determine the functionality that is needed to support EMV and other new payment methods (e.g., contactless and mobile NFC).

After the October 2015 U.S. fraud liability shifts, if a skimmed EMV chip card is fraudulently used at a merchant who has not upgraded to EMV payment acceptance, the merchant is liable for the fraud. Parking operators should consider how much fraud occurs in a parking operation to determine the functionality they need to support and the timing for EMV migration.

Parking industry migration to an EMV solution requires input from all participating stakeholders of the payment ecosystem—parking operators, acquirers, systems integrators, PARCS providers, parking consultants. Receiving guidance from and working collaboratively with all stakeholders are critical to success.

# 6 Publication Acknowledgements

This white paper was developed by the Smart Card Alliance Transportation Council, in partnership with the International Parking Institute (IPI), to educate the parking industry stakeholders across the payments value chain about the critical aspects of deploying an EMV solution in their parking infrastructure.

Publication of this document by the Smart Card Alliance does not imply the endorsement of any of the member organizations of the Alliance.

The Smart Card Alliance wishes to thank Transportation Council and IPI members for their contributions. Participants involved in the development of this white paper included: Aberdeen Management Group, Accenture, CH2M, Creditcall, Giesecke & Devrient, HUB Parking Technology, Ingenico, LTK Engineering Services, Lumin Advisors, MasterCard, Metropolitan Transportation Authority (MTA), OTI America, Parkmobile, Sentry Control Systems, Southeastern Pennsylvania Transportation Authority (SEPTA), SMARTRAC N.V., SP Plus Corporation, T2 Systems, Texas A&M, Verifone, Visa Inc.

The Smart Card Alliance thanks **Steven Grant**, Aberdeen Management Group (formerly of LTK Engineering Services), for leading the project, and the following individuals who wrote content and participated in the project team for this document:

- **Michael Flanagan,** Sentry Control Systems
- **Steven Grant**, Aberdeen Management Group
- **Jeremy Gumbley**, Creditcall
- **Josh Martiesian**, Metropolitan Transportation Authority
- **Cathy Medich**, Smart Card Alliance
- **Brent Paxton**, Parkmobile
- **Roger Slayton**, HUB Parking Technology
- **Tom Wunk**, T2 Systems
- **Rachel Yoka**, IPI

The Smart Card Alliance also thanks members who participated in the review of the white paper including:

- **Sam Bayoumi**, Visa Inc.
- **Jennifer Dogin**, MasterCard
- **Michael Drow**, SP Plus Corporation
- **Mike Herzog**, OTI America
- **Jerry Kane**, SEPTA
- **Michele Krakowski**, Lumin Advisors
- **Peter Lange**, Texas A&M
- **Amy Linden**, MTA Metropolitan Transportation Authority
- **Oliver Manahan**, MasterCard
- **Celine Mantoux**, Giesecke & Devrient
- **Eric Schindewolf**, Visa Inc.
- **Michael Simanek**, Accenture
- **Brian Stein**, CH2M
- **Hassan Tavassoli**, SMARTRAC N.V.

The Smart Card Alliance thanks **Allen Friedman**, Ingenico, **John Rego**, OTI America, and **Erik Vlugt**, Verifone, for providing photos of EMV chip readers.

## Trademark Notice



## About the Smart Card Alliance Transportation Council

The Transportation Council is one of several Smart Card Alliance Technology and Industry Councils, focused groups within the overall structure of the Alliance. These councils have been created to foster increased

industry collaboration within a specified industry or market segment and produce tangible results, speeding smart card adoption and industry growth.

The Transportation Council is focused on promoting the adoption of interoperable contactless smart card payment systems for transit and other transportation services. The Council is engaged in projects that support applications of smart card use. The overall goal of the Transportation Council is to help accelerate the deployment of standards-based smart card payment programs within the transportation industry.

The Transportation Council includes participants from across the smart card and transportation industry and is managed by a steering committee that includes a broad spectrum of industry leaders.

Transportation Council participation is open to any Smart Card Alliance member who wishes to contribute to the Council projects. Additional information about the Transportation Council can be found at http://www.smartcardalliance.org/about_alliance/councils_tc.cfm.

# 7 References


"Chip Education for VARs, ISOs and Merchants," EMV Migration Forum and Payments Strategy Task Force resource, http://www.emv-connection.com/chip-education-for-vars-isvs-and-merchants/

EMV Connection, http://www.emv-connection.com

"EMV Frequently Asked Questions," Smart Card Alliance, http://www.emv-connection.com/?page_id=141

"EMVCo Reports 3.4 Billion EMV Chip Payment Cards in Global Circulation," press release, May 6, 2015, http://www.emvco.com/media_center.aspx?id=48

GoChipCard.com, http://www.gochipcard.com

International Parking Institute, http://www.parking.org

"Minimum EMV Chip Card and Terminal Requirements – U.S.," EMV Migration Forum resource, http://www.emv-connection.com/minimum-emv-chip-card-and-terminal-requirements-u-s/

Recommended Communications Best Practices," EMV Migration Forum, http://www.emv-connection.com/recommended-communications-best-practices/

Smart Card Alliance, http://www.smartcardalliance.org

"Technologies for Payment Fraud Prevention: EMV, Encryption and Tokenization," Smart Card Alliance Payments Council white paper, October 2014, http://www.smartcardalliance.org/publications-technologies-for-payment-fraud-prevention-emv-encryption-and-tokenization/

"Understanding the 2015 U.S. Fraud Liability Shifts," EMV Migration Forum white paper, May 2015, http://www.emv-connection.com/understanding-the-2015-u-s-fraud-liability-shifts/

# 8 Appendix: Mobile Parking Payments

According to eMarketer, 1.64 billion people worldwide had smartphones in 2014 with growth to 2.38 billion by 2017.[15] Data shows that increasing numbers of consumers rely on mobile technology to help them make important day-to-day buying decisions, from gathering information about products and services to paying for purchases. Mobile commerce (m-commerce) refers to the use of a mobile phone, smartphone, or other mobile device to support a commercial transaction. To capitalize on the proliferation of smartphones and tablets, merchants need to make their business processes more mobile-friendly. This helps businesses improve efficiencies, enhance customer satisfaction, reduce costs, and increase revenue.

M-commerce is already one of the major trends affecting small business owners. People increasingly use mobile devices to shop, research products, recommend products to friends on social network sites, and compare online product prices to the prices in brick-and-mortar stores. That is, m-commerce is not restricted to selling and paying for products; it encompasses many of the activities involved in buying and in establishing relationships between businesses and customers.

As consumers become more technology savvy and reliant on mobile devices, businesses must begin looking for solutions that leverage industry-best practices for mobile payments, incorporate all of the latest security features, and use technology that will endure. Therefore, it is important to implement the right solution in the beginning, to avoid investing a substantial amount of money in one technology only to replace it the next year.

Increasingly, the challenge lies in finding a mobile parking strategy that is not only cost-effective, positioned for EMV, and progressive, but is also quick and easy to implement. Luckily, mobile payment solutions are starting to emerge that provide businesses with the tools they need to stay ahead of the curve.

Mobile parking payments are typically account-based payments that customers initiate and track using a mobile device. These payments can be made in a variety of ways, depending upon the particular parking configuration served. But all payments fall into one of two categories:

- In-app mobile payments
- Proximity mobile payments

## 8.1 In-App Mobile Payments

To make an in-app mobile payment, the customer uses a mobile application to authorize the purchase of parking. The customer does not transmit payment data by interacting directly with a physical POS device or system. Payment approvals and authorizations take place entirely between web services.

### 8.1.1 Types of In-App Mobile Payments

Examples of these types of payments include the following:

- Mobile applications that pay for on-street parking services
- Mobile applications that pay for gated parking using a ticket number or license plate number (LPN)
- Mobile applications that prepay for event or gated parking

[15] "2 Billion Consumers Worldwide to Get Smart(phones) by 2016 - See more at: http://www.emarketer.com/Article/2-Billion-Consumers-Worldwide-Smartphones-by-2016/1011694#sthash.VH1HD8z3.dpuf," eMarketer, December 11, 2014

When a mobile app is used to pay for on-street parking, the app communicates the paid amount or paid time associated with a vehicle LPN or parking space or zone number.

When a mobile app is used to pay for gated parking, the app communicates the paid amount or paid time associated with a gated parking ticket or vehicle LPN. The customer inputs or scans a ticket number or LPN. Then, when the vehicle enters the exit lane, the ticket is inserted or the license plate is read, and the parking system recognizes that parking has been fully or partially paid for by the mobile application.

When a mobile app is used to prepay parking, the app communicates the paid amount or paid time associated with a barcode or vehicle LPN. When the vehicle arrives, either the license plate on the vehicle or the barcode on the mobile application is read and the parking system opens the gate for the motorist.

In each of these cases, the mobile application communicates the payment amount or paid status of the customer's account; secure credit or debit account information is not communicated to the parking system. In addition to the payment amount or paid status, the mobile application sends a unique identifier associated with the customer's payment or paid status. These unique identifiers include but are not limited to LPNs, parking ticket numbers, parking space or zone numbers, barcodes, or other applicable data.

### 8.1.2 Transmitting Payment Information

Because no protected payment information is transmitted between the mobile application web service and the parking system, secure payment information must be transmitted elsewhere in the transaction. The mobile application web service funds or authorizes a customer's account either through a card-not-present transaction or a third-party wallet or payment authorization aggregator.

#### 8.1.2.1 Card-Not-Present Transaction

To provide funding through a card-not-present transaction, the customer inputs card information directly into the mobile application or applicable web service. Typically, the mobile application web service will store the card data securely, so that the customer is only required to input the data once for each applicable card.

#### 8.1.2.2 Third Party Wallet or Payment Authorization Aggregator

When funding is provided through a third-party wallet or payment authorization aggregator, a customer need not input secure card data. Instead, the customer links the mobile application to a third party, such as Apple Pay, PayPal®, Visa Checkout, MasterPass™, or Amazon Payments. A key benefit of this approach is that if card data is invalidated, due either to fraud or expiration, secure payment information must be managed in only one or a limited number of third-party web locations. The benefit to the mobile application web service is higher user adoption rates, as customers may stop using a mobile application web service if they have to update information in the app every time the secure payment account data changes.

### 8.1.3 Risk of Fraudulent Transactions

The primary purpose of EMV is to reduce the possibility of card-present fraud, and since none of the cases outlined above incorporate secure EMV chip transactions, merchants bear the liability for fraudulent transactions. While this sounds disconcerting, instances of card-not-present fraud may be infrequent in the parking industry, especially for mobile applications.

Typically, mobile application web services in the parking industry require vehicle LPN data. There is no benefit to providing an alternate LPN; the LPN identifies the customer's account and validates a payment. Since a customer LPN can easily be traced, card fraud is very unlikely in mobile application web services where a customer is required to enter a valid LPN.

In addition, mobile application web services are able to require that location services be used. If the use of fraudulent card data increases, requiring location services to use the mobile application would discourage card fraud, since the precise location of the fraudster could be determined.

Finally, in gated parking facilities, where barcodes and parking tickets can be used in lieu of vehicle LPNs, parking and security cameras are becoming more common. Such camera systems make it easier to catch fraudsters and should discourage fraudulent parking payment transactions.

## 8.2 Proximity Mobile Payments

Proximity mobile payments are payments in which a customer's mobile phone interacts with a physical POS device or system to authorize a payment transaction. NFC-enabled proximity mobile payments may use an EMV-compliant application and store the payment account information securely on the mobile device, resulting in a contactless EMV chip transaction.

Proximity mobile payment transactions require that the mobile device be able to transmit the required secure information. In addition, the parking POS system must have the hardware and software needed to accept contactless EMV chip payments. Mobile phone hardware and operating system providers have been promoting this technology, and adoption for proximity mobile payments is increasing.

These payment methods and systems may generate a valid contactless EMV chip transaction, in which the transaction data is the same as a contactless EMV chip card transaction data. The merchant's POS system can thus conduct an EMV transaction.

Accepting proximity mobile payments requires physical hardware upgrades. It is advisable for merchants to evaluate their options and requirements before making such upgrades. Many merchant facilities have decided to implement POS solutions that are both mobile-enabled and also contactless EMV-enabled. This approach can involve the addition of contactless readers to entrance and exit lanes. Since these devices use radio frequencies (RF) to communicate with contactless chip cards, they also allow for NFC-enabled proximity mobile payments, making merchant POS systems NFC-payment ready.

Industry analysts predict that NFC mobile payment acceptance will grow in the U.S. as merchants migrate to EMV chip-enabled terminals that also support NFC and as the popularity of NFC mobile payments grows (e.g., with Apple Pay, Android Pay and Samsung Pay).