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

EMV and Parking

Version 2.0
Publication Date: May 2016
Publication Number: TC-16002

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

With the United States moving 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 now in place, 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 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 EMV, U.S. contactless payment card transactions and NFC-enabled mobile payments.

The reader is encouraged to review the references in Section 7 for additional educational resources and the Standardization of Terminology[1] document from the EMV Migration Forum.

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.[2] EMVCo now has six member organizations—American Express, Discover, JCB, MasterCard, UnionPay, and Visa—and is supported by dozens of banks, merchants, processors, vendors and other industry stakeholders who participate as EMVCo Associates.

The intention of the original specification developers was to examine the vulnerability of the payment 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.

---

[1] The "Standardization of Terminology" glossary is available at http://www.emv-connection.com/standardization-of-terminology/.

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

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 3.4 billion EMV chip cards have been issued globally, and 36.9 million point-of-sale (POS) terminals accepted EMV chip cards, as of the fourth quarter of 2014.[3] EMVCo also reported that one in three of all chip card-present transactions conducted between July 2014 and June 2015—both contact and contactless—used EMV chip technology (i.e., were chip-on-chip transactions).[4] Europe Zone 1 maintained the highest percentage of EMV chip transactions, with nearly 97 percent of card-present payments using EMV chip.

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: October 2015 was established as the date when fraud liability would shift to the party using the least secure technology in a payment transaction.

As of the end of 2015, the EMV Migration Forum[5] estimates that approximately 400 million cards have been issued to U.S. cardholders, with Visa reporting that 7 in 10 Americans have at least one chip card in their wallet.[6] First Annapolis is forecasting that substantially all U.S. credit and debit cards with be converted to EMV in the next one to two years.[7]

Merchant acceptance of EMV chip cards is also growing. MasterCard has reported that over 1.2 million merchant locations were EMV-enabled as of March 2016, with approximately one million local and regional merchant locations accepting chip cards.[8] Visa has estimated that 50% of merchant locations will be enabled

---

[3] 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.

[4] EMVCo, "One Third of All Card-Present Transactions Globally Use EMV Chip Technology," press release, December 21, 2015, https://www.emvco.com/media_center.aspx?id=48.

[5] 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/.

[6] Visa, "Visa Chip Technology: Adoption Accelerates in U.S. Market," February 2016, https://usa.visa.com/dam/VCOM/download/visa-everywhere/security/visa-us-chip-adoption.pdf.

[7] First Annapolis Navigator, "EMV Activity Rising Slowly but Steadily in the U.S.," January 2016, http://www.firstannapolis.com/articles/emv-activity-rising-slowly-but-steadily-in-the-u-s.

[8] MasterCard, "MasterCard Sees Continued Momentum in U.S. EMV Adoption," March 31, 2016, http://newsroom.mastercard.com/press-releases/mastercard-sees-continued-momentum-in-u-s-emv-adoption/.

by the end of 2016.[9] Issuers and merchants are seeing steady growth in EMV chip-on-chip transactions; First Annapolis estimates that five to ten percent of card-present transactions were EMV at the end of 2015.[10]

1.2 Why EMV

Issuers around the world are issuing chip cards and merchants are moving to EMV-compliant POS 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 parking owners or operators to implement EMV technology; however, the payment networks' fraud liability shifts took effect in October 2015, which transfers liability for fraudulent card-present transactions to the party with the least secure technology. (See additional details in Section 1.2.1.) 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, the potential for increased fraud for non-EMV-compliant acceptance as the rest of U.S. payments acceptance infrastructure migrates to EMV, and the operational impact of EMV in the parking environment (see Section 3).

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. The different payment networks all have slightly different fraud liability shift dates, but the two most important dates were the same: October 2015 was 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 the EMV Migration Forum white paper "Understanding the 2015 U.S. Fraud Liability Shifts."[11])

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

---

[9] Visa, Ibid.

[10] First Annapolis, Ibid.

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

1.2.2 Liability Shift Applicability to Acquirers/Merchants

The October 2015 counterfeit fraud liability shift protects a party who invests in EMV deployment from financial liability for fraud losses from counterfeit magnetic stripe cards with track data copied from a chip card (see reference in footnote 11). The counterfeit liability shift applies to transactions involving American Express, China UnionPay, Discover, MasterCard, Visa, and certain U.S. regional debit networks.

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 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.[12]

If the acquirer/merchant implements the appropriate EMV acceptance devices, the payment networks 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[13] (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 their PCI Qualified Security Assessor team to determine what those reductions will entail.

1.3 EMV Transaction Process[14]

Traditional payment cards feature a magnetic stripe on which cardholder and account information is encoded and stored. 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:

---

[12] Ibid.

[13] The PCI DSS is a standard meant to ensure the protection of sensitive cardholder data throughout the data transmission and storage process, while EMV is intended to prevent the fraudulent use of counterfeit, lost and stolen payment cards. Additional information about PCI DSS can be found at https://www.pcisecuritystandards.org/pci_security/.

[14] 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/

- EMV chip cards and terminals support enhanced card authentication methods that rely on dynamic data.
- Issuers have 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.
- Counterfeit reproduction of EMV chip cards is virtually impossible.

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.

1.3.1 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, issuers and merchants may choose to implement online card authentication only or both online and offline card authentication.

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.

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, date, and terminal-generated unpredictable number).

1.3.2 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)

Signature with chip is processed identically as signature used currently for magnetic stripe card transactions. The consumer's signature is captured for most transactions.

Online PIN with chip is processed identically as with PIN-based magnetic stripe card transactions. 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 many transactions in fast food, transit, parking, convenience stores, and automated kiosk locations), "no CVM" is often preferred for transactions. No CVM transactions are processed without the cardholder's PIN or signature.

No CVM is especially relevant to the parking industry. As of July 1, 2015, all newly-deployed chip-enabled (contact and contactless) unattended terminals must support the processing of transactions without a CVM.[15,16] Payment networks have also issued guidance that unattended payment terminals are not required to support PIN acceptance if the terminal does not have a PIN pad, even if the chip card is PIN-preferring.[17] If the unattended terminal has a PIN pad and the EMV chip card presented is PIN-preferring, then the transaction must be processed with a PIN.

U.S. EMV chip card issuance has been a mix of signature-preferring 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) have been online PIN-preferring. 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.

1.4 EMV and U.S. Debit

The U.S. has unique requirements for debit card transactions. Regulation II of the Durbin Amendment to the Dodd-Frank Wall Street Reform and Consumer Protection Act of 2010 ("Reg II") requires that there must be merchant choice between at least two unaffiliated debit networks when routing point-of-sale debit transactions. While such routing choice is not unique to merchants processing EMV transactions, for parking owners that upgrade to EMV, the debit routing implementation[18] can introduce additional technical and customer experience (e.g., display prompts) factors that may need to be considered prior to deployment.

---

[15] See reference for Visa: "Chip Payment Acceptance: Putting It into Perspective for Small-Ticket Unattended Merchants, https://www.visa.com/chip/merchants/grow-your-business/payment-technologies/credit-card-chip/docs/Chip_Payment_Acceptance_Putting_it_Into_Perspective_for_Small_Ticket_Unattended_Merchants.pdf.

[16] Note that different payment networks have different policies for the use of "no CVM" at unattended POS terminals. Parking owners are advised to consult with their acquirers for more information on the network-specific requirements.

[17] Visa, op.cit.

[18] Additional information on EMV debit implementation can be found in the EMV Migration Forum white, "U.S. Debit EMV Technical Proposal," April 2015, http://www.emv-connection.com/u-s-debit-emv-technical-proposal/.

1.5 EMV and Contactless Transactions

At the same time as the U.S. is moving to EMV chip card payments, contactless payments using Apple Pay, Android Pay and Samsung Pay with NFC-enabled mobile devices are becoming more common. In addition, the payments industry is anticipating more dual-interface (contact and contactless) EMV chip card issuance in the next wave of EMV chip card issuance.[19]

As parking merchants upgrade their terminals to accept EMV-compliant chip cards, adding support for contactless payment is straightforward (particularly as many new POS devices come equipped with the option to support contactless payments) and would enable contactless acceptance using mobile NFC devices and contactless and dual interface chip cards. Since EMV contact chip card payments and contactless payments made using mobile NFC devices or dual-interface cards use the same transaction data, implementing them simultaneously rather than separately can help to minimize implementation time and complexity, including the time to test, certify, and deploy.[20] Contactless payments can also deliver faster transaction speed, especially when coupled with no CVM transactions.

[19] Digital Transactions, "Payment Card Manufacturer Sees Growing Interest in Dual-Interface Cards," February 26, 2016, http://www.digitaltransactions.net/news/story/Payment-Card-Manufacturer-Sees-Growing-Interest-in-Dual-Interface-Cards.

[20] Additional information can be found in the Smart Card Alliance white paper, "EMV and NFC: Complementary Technologies Enabling Secure Contactless Payments," published in November 2015, http://www.smartcardalliance.org/smart-card-alliance-white-paper-explores-contactless-payments-and-the-role-of-nfc-technology-in-u-s-emv-migration/

2 Considerations for Deploying EMV in a Parking Environment

The parking industry has seen an increase in EMV requirements for new parking payment solutions as well as retrofits for EMV to existing solutions. Since EMV migration can be a lengthy and complex process, parking equipment manufacturers and owners 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 all parking stakeholders.

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 primarily on the prospective transaction location, as well as on what CVMs the merchant wants to accept.

For example, at a location with a cashier stand, a terminal similar to one used in a retail store (shown in Figure 1) may be an appropriate choice. These terminals include a slot on the right side that accommodates magnetic stripe cards and a slot on the bottom that accommodates chip cards. For those implementations that already have a form of electronic payments, installing this type of chip-enabled POS terminal in a parking environment can be straightforward, requiring little or no structural work.

Figure 1. Example of a Chip-Enabled POS Terminal

However, parking owners and operators need to consider the parking patron experience for different types of parking payment scenarios. For example, how does the parking patron interact with the cashier and POS terminal when exiting a gated parking facility? Implementation costs would include the new terminals, any needed software, and training.

The devices shown in Figure 2 are examples of EMV-enabled parking kiosks.

Figure 2. Examples of Chip-Enabled Parking Kiosks

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 three 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
- Whether the cashier booth operates in both attended and unattended modes. With an EMV POS terminal installed outside a booth that typically operates in an unattended mode, the POS terminal must also be able to work while the booth is attended. This requires the parking access revenue control system (PARCS) to allow for the solution outside of the booth to operate while the booth is attended.

Examples of terminals that can be incorporated into kiosk devices are shown in Figure 3.

Figure 3. Examples of Chip-Enabled Devices for Kiosks[21]

Most 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, older PARCS parking payment devices may not be able to be readily retrofitted to accommodate the appropriate EMV chip-enabled reader due to physical space limitations.

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.[22]

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

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

- Purchase only PCI-approved PIN entry devices.[23]
- 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 contactless payments from both contactless cards and NFC-enabled mobile devices (e.g., Apple Pay, Android Pay, Samsung Pay).

It is important to note that in unattended environments such as parking, the payment networks may require support for "no CVM,"[24] and a PIN pad may not be needed unless the parking owner believes the cost of lost or stolen card fraud will outweigh the operational costs of a PIN pad.

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:

- Consult with the parking owner/operator's acquirer to determine whether EMV is supported.
- Determine what changes are required in the parking owner'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

All global payment networks have acquirer host and EMV chip terminal testing processes to help maintain and ensure the integrity of the payment network infrastructure and an optimized cardholder acceptance experience. The American Express, Discover, MasterCard and Visa EMV testing requirements are globally accepted and therefore relevant to the U.S. market in order to reduce any potential interoperability issues in production.

These testing and certification processes follow the EMV specification and each global payment network's application specification, with an objective of ensuring interoperability among all host systems, payment terminals, and cardholder devices. With the benefit of global knowledge and experience, the global payment networks have developed, and continually strive to improve, their testing processes and requirements, in order to help minimize potential deployment and production risks.

---

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

[24] Note that different payment networks have different policies for the use of "no CVM" at unattended POS terminals. Parking owners are advised to consult with their acquirers for more information on the network-specific requirements.

This section summarizes the different types of testing and certification performed. Detailed global payment network certification information is available in the EMV Migration Forum white paper, "EMV Testing and Certification White Paper: Current Global Payment Network Requirements for the U.S. Acquiring Community."[25] If more functional detail is needed about specific certification processes, parking owners and operators should consult with their acquirer/processor.

Testing and certification covers EMVCo terminal type approval for both chip hardware and software, acquirer host testing and POS terminal testing.

2.3.1 EMVCo Terminal Type Approval

EMVCo terminal type approval includes two levels of testing.

Level 1 testing measures the conformance of the hardware chip-reading components, or interface modules (IFM), to the EMV-defined set of electrical, mechanical, and communication protocol characteristics. (Interface modules support communication between the device and the chip card, and are commonly known as "chip readers.")

Level 2 testing measures the conformance of the terminal-resident application software that supports specified EMV functionality, both required and optional. The EMV-compliant application software is commonly known as the "EMV kernel." Further information about these approvals can be found on www.emvco.com.

Typically, the EMVCo Level 1 and Level 2 approvals are obtained by vendors prior to selling the devices. The parking payment service provider should be able to provide EMVCo letters of approval (LoAs) to demonstrate that equipment and software has been tested to be compliant to EMV standards.

2.3.2 Acquirer Host Testing

The acquirer host testing process is performed by the global payment networks, and is designed to test the capability of the acquirer/acquiring processor to carry full chip data correctly in the messages sent to the global payment networks for EMV contact chip and contactless transactions. Acquirers, acquirer processors, and merchants directly connected to the global payment networks will need to undergo this testing. This testing will already have been completed by acquiring processors, and this phase should not affect parking merchants.

2.3.3 Terminal Testing

Terminal testing is typically managed by the acquirer. Required terminal testing does not focus solely on the terminal; it also examines anything that sits between the card and the payment network.

Terminal testing has two phases. In phase 1, the acquiring processor will certify that the terminal communicates properly with the acquiring processor's host and that the terminal sends full chip data correctly in the messages sent to the acquiring processor for EMV contact chip and contactless transactions. Because the terminal may be just one component in a card payment acceptance solution, this testing can be

[25] For specific information about testing and certification, please see the EMV Migration Forum white paper, "EMV Testing and Certification White Paper: Current Global Payment Network Requirements for the U.S. Acquiring Community," http://www.emv-connection.com/emv-testing-and-certification-white-paper-current-global-payment-network-requirements-for-the-u-s-acquiring-community/.

performed by the terminal vendor, but more often is performed by the system integrator or the provider of the parking payment solution (working in conjunction with the acquiring processor). Where the parking owner has unique requirements, it is likely that this testing will need to be performed on the specific payment configuration deployed in the parking environment.

Phase 2 of terminal testing is an integration regression test required by the global payment networks, often referred to as "Level 3" testing. Again, this testing is most likely to be performed by the provider of the parking payment solution in conjunction with the acquiring processor.

This global payment network terminal testing takes place after both EMVCo Level 1 and Level 2 terminal approval, as well as the acquirer terminal certification, and precedes terminal deployment.

Figure 4 illustrates the areas that are covered by terminal testing, namely the interaction and communication between merchant and the acquirer.

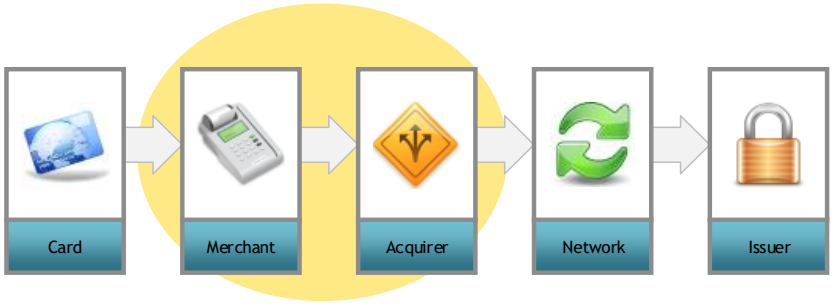

Figure 4. Areas Covered by Terminal Testing

Currently, global payment network terminal testing is required in the following situations:

- New hardware, a new EMV-approved kernel, or new payment application software is introduced, or payment-related configuration changes are made. Any time there are changes to the payment application affecting chip processing or the kernel by terminal configuration, retesting with the payment network is required.[26]
- Changes are made to the chip payment application processing on the terminal or within the infrastructure.[27]
- Hardware or software is modified significantly or an EMVCo-approved kernel is changed on a deployed terminal. Refer to EMVCo Type Approval Bulletin No. 11 for more details on minor and major changes.
- Hardware, software, or parameter settings are changed and the change impacts the payment application.
- Terminal-to-acquirer messaging is changed affecting chip processing.

[26] Ibid.
[27] Ibid.

Some of the global payment networks require tests in addition to those described in Section 2.3.2 and Section 2.3.3, such as live environment end-to-end testing.

While Level 3 testing may not typically be performed by the merchant, the merchant should consider the time needed for this testing in their EMV implementation and rollout planning.

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 EMV Offline Functionality[28]

Just as they do today with the magnetic stripe environment, merchants are able to process EMV transactions when communications are offline. The U.S., however, is an online-preferring environment.[29] For example, if both an EMV card and terminal are offline-capable, they are likely only to engage in requesting and receiving offline authorization if the terminal was unsuccessful in receiving an online response from the issuer host.

When a merchant has a communications disruption, several options exist for continuing to process EMV transactions so as not to impede commerce. These options carry varying risks to the merchant, and require different systematic implementations. The three offline processing options discussed below include: EMV offline authorization; deferred authorization of an EMV card transaction; force post of an EMV card transaction.

- Offline Authorization Decision. An offline EMV authorization is a transaction resulting from a request by the terminal to the chip card for approval of a transaction without requesting a real-time online authorization of the transaction from the issuer host. The card and merchant terminal must support (and be certified for) offline authorization in order for an offline authorization of an EMV payment transaction to occur.
- Deferred Authorization. A deferred authorization is an authorization request or financial request which occurs when a merchant captures transaction information while connectivity is interrupted; the merchant holds the transaction until connectivity is restored. After connectivity is restored, the merchant sends transactions for an online authorization request, and receives an authorization response from the issuer.
- Forced Post (Merchant Stand-In). Forced post is when a merchant approves a transaction and processes the transaction into settlement without obtaining any issuer authorization.

For deferred authorization, force post or offline approvals above the network floor limits, in order to mitigate risk, the merchant should consider the transaction amount, and could evaluate the Terminal Verification Result (TVR), if supported by the payment application on both the card and the terminal. This could, for example, help the merchant mitigate risk of accepting expired cards, CVM failures, or counterfeit cards. It is

[28] Additional information can be found in the EMV Migration Forum white paper, "Merchant Processing during Communications Disruptions," available at http://www.emv-connection.com/merchant-processing-during-communications-disruption/.

[29] The U.S. is an online-preferring market and this section only addresses online-preferring terminals.

also important to note that EMV supports Offline Card Authentication (see section 1.3.1) which, if supported by both the card and the terminal, can help mitigate risk of accepting counterfeit cards.

Parking merchants should discuss requirements for transaction processing when communications are offline with their acquirer to determine the most appropriate approach for their parking environment.

2.6 Other Payment or Security Functionality

Many merchants use EMV migration as an opportunity to evaluate their payment functionality and security strategy for other potential changes that can have positive impacts on the overall parking payments acceptance environment. 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.[30] If implementing P2PE, it is important to deploy solutions validated by PCI.[31]

2.7 Other EMV Deployment Considerations

As part of the EMV migration planning process, parking stakeholders need to consider the cardholder experience at entry and, in particular, at exit. Guidance for the customer at unattended terminals and for the cashier in an attended lane is crucial to avoid confusion at exit and reduce queuing.

Providing the customer with pictorial and/or written instructions at the parking facility and media outlets that illustrate proper insertion of the card can help inexperienced cardholders understand that they must insert the chip card and leave it in the reader. Some solutions may clamp the card in the chip reader if it is not a motorized reader.

Instructions should also remind the cardholder to remove the chip card before leaving. To prevent cardholders from leaving their card, some best practices can include:

- Not raising the parking barrier gate until the chip card is removed
- Producing an audible sound or tone to remind the cardholder to remove the card

Terminals with displays should prompt the cardholder to insert the card, to allow the card to remain in the reader while processing, and to remove the card when processing is complete, similar to the retail customer experience. Terminals without displays should use auditory or visual cues (e.g., red/green LEDs), in conjunction with signage, to indicate the appropriate cardholder action.

It is also important to consider where chip acceptance devices are placed to allow for easy cardholder access, and how the requirements for completing a chip card transaction (i.e., inserting rather than swiping the card or entering a PIN) may impact queuing. This is especially relevant for high- and low-profile vehicles that are challenged by the height and distance from the driver to the EMV terminal location.

---

[30] 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/.

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

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, such as using a parking credential, paying for parking online, or paying for citations, 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 busters," 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 many 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 owner. The deployment of EMV chip cards has different implications for the different scenarios. The use of chip cards raises two considerations. First is whether EMV chip-enabled POS terminals similar those deployed at general retail locations are suitable for parking environments. The second consideration is whether to support only chip and signature or accept chip and PIN transactions. These considerations have different implications for attended and unattended environments. In this discussion, "attended" refers to situations where a cashier is directly handling the payment process; "unattended" is where payment processing occurs solely between the cardholder and the payment device, without assistance (regardless of the proximity of an attendant).

In addition, as discussed in Section 3.2.1, the introduction of EMV processing can potentially have a negative impact on payment transaction time, particularly with poorly planned implementations. Parking owners and operators should work closely with their payment solution providers to ensure that there is minimal disruption to the payment flow.

3.1.1 Attended In-Lane Cashiering

In certain locations, parking patrons pay for parking at a cashier booth from their cars. After processing the parking ticket, the cashier displays the fee, and the patron pays with cash, check or a payment card.

Generally speaking, the EMV hardware and software used for general retail can be readily integrated into the attended parking environment where the cashier is directly facilitating the payment.

If the transaction requires only a supporting signature or no CVM (see Section 1.3.2 for a description of CVMs), the payment process is similar to the current process for magnetic stripe cards. The patron hands the card to the cashier, the cashier inserts the card into the EMV chip-enabled terminal, and the transaction is processed. If the parking owner decides not to support PIN on magnetic stripe and chooses not to support PIN for chip, there will be no change to current signature/no CVM processing.[32]

If PIN support is desired, the PIN pad must be accessible to the parking patron who will be in a vehicle outside the cashier booth. To facilitate PIN entry, the terminal may need to be handed through the booth and car window to the patron – an operation fraught with many potential challenges including dropping the device and causing damage to terminal and/or the vehicle or exposing it to precipitation. Another option may be to mount an outdoor-suitable PIN pad on the booth face for access through the car window (typically called a booth transaction panel). In such a system, however, it is important to consider the ergonomics for customers entering their PINs, the overall time for the payment interaction, and the cashier's role (other than assisting the customer with instructions). These considerations, as well as the additional ongoing costs of PIN support, must be weighed against any anticipated exposure to lost-and-stolen card fraud.

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 POS terminal deployed at an attended central cashiering station will be similar to those typically deployed at general retail locations. (The experience is similar to other retail environments and drive-through merchants.) 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 multi-space 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 card readers.

The physical attributes of an EMV chip-enabled reader may be significantly different from the magnetic stripe card reader it replaces (if it is not an additional reader). (It must be determined if an EMV reader can also read magnetic stripe cards, or if the EMV reader is to be installed in addition to the existing magnetic stripe reader.)

If a PIN pad is 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). The parking owner should work with their acquiring processor to determine their exposure to lost-and-stolen fraud, and to weigh those costs against the cost of implementing PIN support. Note that this exposure may change over time, so fraud costs should be regularly monitored.

Note also that even if the payment terminal supports PIN, a PIN will only be prompted if the card has been personalized by the issuer to be PIN-preferring.

---

[32] The parking owner must evaluate their potential exposure to lost-and-stolen fraud.

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. This method of payment acceptance has become increasingly popular as more parking facilities deploy this option, since it offers sound customer service, reasonable labor and overhead savings, and increased patron throughput. While a few devices accept either cash or payment cards, the majority of pay-in-lane devices are currently designed to accept only card payments that do not require a PIN.

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 a parking facility implements a PIN pad. Hardware space is at a premium within the pay-in-lane devices; additional considerations are the orientation of the hardware in relation to the height and distance of the driver from the EMV hardware and the time required for the driver to enter a PIN. Again, the parking owner or operator should work with their acquiring processor to determine their exposure to lost-and-stolen fraud, and to weigh those costs against the cost of implementing PIN support.

3.1.5 Ticketless "Credit Card In-Out"

Ticketless "credit card in-out" (CCIO) systems need to consider how implementations will be impacted by EMV chip transactions. When using magnetic stripe technology, the card is swiped or ingested upon entry and certain sectors of the data read are used as a non-ambiguous, secure identifier. Upon exit, a match is made with the entry data, a fee is computed, and the card is charged. While CCIO is not implemented in a majority of pay-parking locations, certain locations use it extensively; at least one major U.S. airport transacts more than 80%[33] of its parking fees using CCIO.

In an EMV environment, technical considerations regarding CCIO include:

- Processing requirements. Obtaining an identifier via EMV processing will require different processing than for magnetic stripe transactions. Since an EMV chip card read includes magnetic-stripe-equivalent data (in addition to other data), CCIO support for both entry and exit terminals will be technically feasible.
- PCI scope. Will the data exchange between the EMV terminal and the PARCS application software compromise the reduction in PCI scope that EMV would otherwise provide? If the full PAN is used as a component of the identifier, it must be protected under PCI DSS, unless some means of encryption or masking is used.

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, parking 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

[33] "Parking Upgrades," Carol Ward, http://web.archive.org/web/20160104145526/http://www.parking.org/media/334807/arnparkingnow2014.pdf

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 5).

Figure 5. Processing Steps for an EMV Contact Transaction

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. Parking operators need to work with their payment solution provider to ensure transaction speeds are acceptable.

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. An operational consideration is adding signage during the chip migration to notify the customer that chip support has been implemented, and that (for contact chip readers) they need to leave their card in the reader until prompted to remove it.

It is also important to consider the impact of PIN-based transactions, if supported, on throughput. As discussed in Section 1.3.2, 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 the process described above focuses on contact EMV chip cards. A brief description of contactless EMV transactions can be found in Section 4.

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 (e.g., PIN pads) at pay stations to support PIN-preferring cards
- Higher full time equivalent (FTE) staffing, or parking ambassadors, during initial roll-out to address customer issues
- Potential ergonomics, safety and queuing 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 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

PARCS vendors benefit from simplifying both their implementation and certification requirements by using fully certified pre-validated solutions with the acquiring host. This type of solution allows the parking solution to request a payment from the unattended solution which then processes the payment directly with the acquiring host and provides the approved or declined message back with the required data for receipt generation. In this scenario no card data passes through PARCS which can reduce the PCI certification requirements.

The implementer must also consider how to communicate the change in processing flow to the cardholder. Particularly in the early phases of the U.S. migration to chip support, the cardholder must be instructed to insert the chip card, leave it in the reader while processing, and then remove the card when processing is complete. This can be accomplished through terminal displays or other cues, in conjunction with appropriate signage.

For several years after the initial migration to chip, there will be a mix of magnetic stripe cards and chip cards in circulation.

EMV terminals must first read the card to determine the presence of a chip. For parking environments that use EMV terminals that are similar to retail POS terminals, the customer will follow the terminal prompts to either insert the chip card or swipe the magnetic stripe. If a chip card is first swiped, the customer will be prompted to insert the card and to leave the card in the reader for the duration of the transaction.

Kiosks or other self-service devices may support a different interface for customer interaction—using readers similar to the ones that are used for ATMs (either ones that require the cardholder to insert and remove a card (also called dip readers) or ones that are motorized and ingest the card). Where a dip reader is used and a chip is detected, the customer must be instructed to leave the card in the reader for the duration of the transaction. If no chip is detected, the customer is instructed to immediately remove the card and the transaction is processed from the magnetic stripe. In some cases, a reader may implement a "double-dip" process to address the customer's habit of quickly inserting and removing payment cards. Under "double-dip," the terminal will attempt to read the chip. If the card is removed before this can complete, the terminal reads the magnetic stripe as the card is being removed. If the magnetic stripe contains a chip indicator, the cardholder is prompted to reinsert the card and to leave it in the reader. This behavior may be reinforced by introducing mechanical clamps to restrict removal of the card on the second insertion. While the "double-dip" process does result initially in an additional insertion, it quickly trains the cardholder to leave the card in the terminal.

3.2.4 Staff and Customer Training

Parking owners and operators need to consider and plan for staff training and communications with customers on the changes in the payment process, particularly during the early phases of EMV migration. 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 merchants on developing effective messaging and education approaches before, during and after migration to EMV chip technology.[34] For example, customer-facing signage and FAQs on EMV for cashiers can help during the migration. The GoChipCard.com web site also provides easy-to-understand resources for consumers and merchants on how and why payment transactions are changing.[35]

3.2.5 Cost Impact

EMV implementation incurs certain costs which can be significant during migration. Costs include:

- Equipment upgrades. 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.
- Installation costs
- Certification of devices with payment processors and merchant acquirers (initial and ongoing)
- Spare parts
- Signage at the POS
- Staff and customer training
- Additional staffing support during the migration

---

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

[35] 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.

The ongoing costs after EMV migration are the normal costs seen with payment acceptance including the typical per transaction fee.

PARCS vendors may lose a certain amount of control over support because of the addition of components and the involvement of new third parties. Implementation of EMV technology introduces additional vendors, who share responsibility for delivering an end-to-end solution. Ownership and accountability may no longer be the sole responsibility of the PARCS solution provider. Troubleshooting and repair can become a responsibility that is shared among 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 testing processes required by the payment card industry.

4 EMV Contactless Payments and NFC-Enabled Mobile Devices

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 a Near Field Communication (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 (RF) communication between two electronically compatible devices located within close proximity. NFC-enabled mobile payment may use an EMV-compliant application and store the payment account information securely on the mobile device, resulting in a contactless EMV chip transaction. Industry analysts predict[36] that NFC-enabled 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-enabled mobile payment methods grow (e.g., with Apple Pay, Android Pay and Samsung Pay).

Regardless of whether a chip card or a magnetic stripe card is enrolled in an electronic wallet application, NFC-enabled mobile payment methods and systems will 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 a standard contactless EMV transaction.[37]

To implement contactless payments from NFC-enabled mobile devices, the parking POS system must have the hardware and software needed to accept contactless EMV chip payments. 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 contactless/NFC-enabled and contact EMV-enabled. This approach can involve the addition of contactless readers to entrance and exit lanes. When planning an upgrade, parking owners should request devices that can communicate with both contactless chip cards and NFC-enabled mobile devices.

Since the POS acceptance infrastructure is changing with EMV, parking owners should consider supporting contactless transactions from contactless EMV chip cards and NFC-enabled mobile devices as part of the upgrade. By combining this migration, the owner may have a better return on investment and be ready for future payment mechanisms such those using NFC-enabled wearables.

---

[36] "How Chip Cards Could Pave the Way for Apple Pay," Inc., Oct. 23, 2015, http://www.inc.com/jeremy-quittner/chip-card-roll-out-will-also-push-digital-wallets-to-the-forefront.html

[37] It is important to note that contactless transactions from NFC-enabled mobile phones use tokenized data so that the primary account number (PAN) may not look like the PAN from the original card. Additional information on how NFC-enabled mobile devices support EMV contactless payments can be found in the Smart Card Alliance white paper, "EMV and NFC: Complementary Technologies Enabling Secure Contactless Payments," http://www.smartcardalliance.org/publications-emv-and-nfc-complementary-technologies-enabling-secure-contactless-payments/.

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 owners to review their overall payments strategy and determine the functionality that is needed to support EMV and other new payment methods (e.g., contactless payments from EMV chip cards or NFC-enabled mobile devices).

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

Many resources are available from the EMV Migration Forum and other payments industry stakeholders to assist merchants with migration. Key resources are listed in Section 7 and additional resources can be found on the EMV Migration Forum's EMV Connection and GoChipCard.com web sites.

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. The initial white paper was published in June 2015, with an update in May 2016.

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 to the May 2016 update of this white paper. Participants involved in the development of the May 2016 white paper update included: 20/20 Parking Consultants; Aberdeen Management Group; CH2M; CPI Card Group; Cubic Transportation Systems; Dallas Area Rapid Transit (DART); GO Systems & Solutions; Lumin Advisors; MasterCard; Metropolitan Transportation Authority (MTA); Metropolitan Transportation Commission (MTC); Moneris Solutions; Quadagno & Associates; Southeastern Pennsylvania Transportation Authority (SEPTA); Visa Inc.; Walker Parking Consultants.

The Smart Card Alliance thanks the following individuals who wrote content and participated in the project team for this document:

- **Sam Bayoumi**, Visa
- **Charl Botes**, MasterCard
- **Marc Cleven**, Visa
- **Jennifer Dogin**, MasterCard
- **Steven Grant**, Aberdeen Management Group
- **Michele Krakowski**, Lumin Advisors
- **Jerry Kane**, SEPTA
- **Joshua Martiesian**, MTA
- **James Maglothin**, 20/20 Parking Consultants
- **Brian McGann**, Walker Parking Consultants
- **Cathy Medich**, Smart Card Alliance
- **Brian Stein**, CH2M
- **Mike Strock**, Smart Card Alliance
- **Jeff Stroud**, MasterCard
- **David Weinshel**, Visa

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

- **Troy Bernard**, CPI Card Group
- **David Blue**, Cubic Transportation Systems
- **Doug Hatton**, Moneris Solutions
- **Mike Hughes**, Moneris Solutions
- **Carol Kuester**, MTC
- **Tina Morch-Pierre**, DART
- **Polly Okunieff**, GO Systems & Solutions
- **Peter Quadagno**, Quadagno & Associates
- **Jason Weinstein**, MTC

The Smart Card Alliance also thanks the IPI and Smart Card Alliance members who contributed to the June 2015 publication, including: 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 Technology Group, SP Plus Corporation, T2 Systems, Texas A&M, Verifone, Visa Inc.

The Smart Card Alliance thanks **Amano**, **Ingenico, OTI America, Skidata, Verifone,** and **Walker Parking Consultants** for providing photos of EMV-enabled POS terminals, chip readers and parking kiosks in Figures 1, 2 and 3.

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 Appendix A: In-App Mobile Parking Payments

While not relevant to EMV migration, 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. This section provides an overview of in-app mobile parking payments to highlight other options that parking owners may want to consider when developing their long-term payment strategies.

7.1 Market Trends

According to eMarketer, 1.64 billion people worldwide had smartphones in 2014 with growth to 2.38 billion by 2017.[38] 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, builds on EMV functionality, and progressive, but is also quick and easy to implement. Mobile payment solutions are starting to emerge that provide businesses with the tools they need to stay ahead of the curve.

7.2 In-App Mobile Payments

In-app mobile parking payments are typically account-based payments that customers initiate and track payment using a mobile device.

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

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.

7.2.1 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

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, 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.

7.2.2 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.

7.2.2.1 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.

7.2.2.2 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.

7.2.3 Risk of Fraudulent Transactions

Instances of card-not-present fraud may be infrequent in the parking industry, especially for mobile applications. In-app payment functions can take advantage of mobile services, such as location data, to further minimize risk. Third party payment functionality, such as Apple Pay or other mobile payment approaches, may also offer security features such as biometrics.

In addition, mobile application web services in the parking industry typically 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.

Mobile application web services are also 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.

7.3 Conclusion

While in-app mobile payment functionality is not yet as fully developed as contactless payments using EMV contactless chip cards or NFC-enabled mobile devices, there is rapidly growing interest in offering this functionality, particularly as it offers opportunities to tie in with marketing and loyalty programs.

8 Appendix B: References

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

"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/

"Chip Payment Acceptance: Putting It into Perspective for Small-Ticket Unattended Merchants," Visa publication, https://www.visa.com/chip/merchants/grow-your-business/payment-technologies/credit-card-chip/docs/Chip_Payment_Acceptance_Putting_it_Into_Perspective_for_Small_Ticket_Unattended_Merchants.pdf

"EMV Activity Rising Slowly but Steadily in the U.S.," January 2016, First Annapolis, http://www.firstannapolis.com/articles/emv-activity-rising-slowly-but-steadily-in-the-u-s

"EMV and NFC: Complementary Technologies Enabling Secure Contactless Payments," Smart Card Alliance, November 2015, http://www.smartcardalliance.org/smart-card-alliance-white-paper-explores-contactless-payments-and-the-role-of-nfc-technology-in-u-s-emv-migration/

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

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

EMV Migration Forum, http://www.emv-connection.com/emv-migration-forum/

"EMV Testing and Certification White Paper: Current Global Payment Network Requirements for the U.S. Acquiring Community," EMV Migration Forum, April 2016, http://www.emv-connection.com/emv-testing-and-certification-white-paper-current-global-payment-network-requirements-for-the-u-s-acquiring-community/

EMVCo, http://www.emvco.com

"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

"How Chip Cards Could Pave the Way for Apple Pay," Inc., Oct. 23, 2015, http://www.inc.com/jeremy-quittner/chip-card-roll-out-will-also-push-digital-wallets-to-the-forefront.html

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

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

"Merchant Processing during Communications Disruptions," EMV Migration Forum white paper, April 2016, http://www.emv-connection.com/merchant-processing-during-communications-disruption/

"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/

"One Third of All Card-Present Transactions Globally Use EMV Chip Technology," EMVCo press release, December 21, 2015, https://www.emvco.com/media_center.aspx?id=48

"Parking Upgrades," Carol Ward, http://web.archive.org/web/20160104145526/http://www.parking.org/media/334807/arnparkingnow2014.pdf

"Payment Card Manufacturer Sees Growing Interest in Dual-Interface Cards," Digital Transactions, February 26, 2016, http://www.digitaltransactions.net/news/story/Payment-Card-Manufacturer-Sees-Growing-Interest-in-Dual-Interface-Cards

PCI Security Standards Council, https://www.pcisecuritystandards.org/pci_security/

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

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

"Standardization of Terminology," EMV Migration Forum, http://www.emv-connection.com/standardization-of-terminology/

"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/

"U.S. Debit EMV Technical Proposal," EMV Migration Forum, April 2015, http://www.emv-connection.com/u-s-debit-emv-technical-proposal/

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

"Visa Chip Technology: Adoption Accelerates in U.S. Market," February 2016, Visa publication, https://usa.visa.com/dam/VCOM/download/visa-everywhere/security/visa-us-chip-adoption.pdf