WHITE PAPER

Smart Card Alliance

A SMART CARD ALLIANCE MOBILE AND NFC COUNCIL AND PAYMENTS COUNCIL WHITE PAPER

EMV and NFC: Complementary Technologies Enabling Secure Contactless Payments

Publication Date: November 2015
Publication Number: PC-15002

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.

Table of Contents

1 Introduction

EMV is a global standard for secure debit or credit payments made using chip cards at a merchant who has an EMV chip-acceptance infrastructure. EMV-compliant chip card payments protect against the use of counterfeit, lost, or stolen cards and skimming. Issuers, merchants, consumers, and acquirers/processors can all benefit from EMV. As a result of the EMV fraud liability shift in October 2015, merchants, issuers, and processors in the United States are in the final stages of upgrading their infrastructures.

EMV is a payments technology.

NFC is a communications technology that enables contactless EMV.

Simultaneously with the U.S. move to EMV chip card payments, Near Field Communication (NFC) technology is emerging as a useful accessory for consumer transactions. NFC is not a payment technology; it is a set of standards that enables proximity-based communication between consumer electronic devices such as mobile phones, tablets, and personal computers. NFC supports an extremely simple man-machine interface, facilitating its use for a number of functions, including mobile payment. NFC technology is compatible with the current contactless payment acceptance infrastructure—an NFC-compliant mobile device can communicate with a point-of-sale (POS) system that currently accepts contactless payment cards.

NFC and EMV are companion technologies. NFC applies to how devices communicate; EMV applies to payments made with contact and contactless chip cards or with a mobile NFC device emulating a contactless chip card. Contactless payment transactions made using mobile NFC devices use the same infrastructure as contact and contactless EMV chip card transactions. This white paper clarifies how EMV chip payment and NFC communications technologies are used together.

1.1 Key Terms and Definitions

One common misunderstanding is that NFC is a payments technology rather than a communications technology. A common question is "Why do we need EMV? Can't we just leapfrog to NFC?" Payment participants are confused about whether to prepare to process payments made using EMV contact chip cards, EMV contactless chip cards, mobile NFC devices, or all three.

To resolve such confusion and benefit from the discussion in this white paper, it is important to understand the following terms:

Contactless chip card: A chip card that communicates with the reader through radio frequency (RF), using an ISO/IEC 14443-compliant interface.

Contactless payment: A payment transaction that does not require physical contact between the consumer's payment device and a physical terminal. The consumer holds the payment device (such as a contactless or dual interface chip card or mobile NFC device) in close proximity (less than approximately 1-2 inches) to the terminal, and payment account information is transmitted wirelessly, over RF.

Contactless POS terminal: A terminal with contactless functionality, enabling it to accept contactless payments, including payments from contactless and dual interface chip cards and mobile NFC devices that are provisioned with payment applications and credentials.

Dual interface card: A chip card with both contact and contactless interfaces. Payment transactions can use either interface.

Dual interface POS terminal: A terminal with both contact and contactless functionality. Payment transactions can use either interface.

Mobile NFC device: An NFC-enabled mobile device, such as a mobile phone. A mobile NFC device can support contactless payment when it has a compatible payment application in the device and is provisioned with payment account credentials.

1.2 Background

Although contactless payments were introduced to the U.S. payment ecosystem in the mid-2000s, adoption did not achieve critical mass. Major initiatives encouraged the use of mobile NFC devices to make contactless payments, starting with the introduction of Google Wallet in 2011 and followed by Softcard in 2012. The launch of Apple Pay™ in 2014 and the launch of Android Pay and Samsung Pay™ in 2015 have reignited interest in contactless payments using mobile NFC devices, cards and other form factors.

As merchants upgrade their terminals to accept EMV-compliant contact chip cards, one option is also to include support for contactless payment using mobile NFC devices and contactless and dual interface chip cards (particularly as many new POS devices come equipped to support contactless payments). EMV chip card acceptance addresses card-present fraud and is being driven by the fraud liability shift dates. Support for NFC can add value in retail locations where improving the speed of payment or leveraging other services associated with mobile device payments that can drive business. The Smart Card Alliance Payments and Mobile and NFC Councils collaborated on this white paper to clarify what NFC and EMV mean to merchants and issuers and to provide answers to questions about migration strategy. This white paper also describes the issuance and acceptance infrastructure and identifies impacts, benefits and key considerations for migration.

2 EMV Chip Migration and NFC in the U.S.

Card payment options for consumers have changed radically since the 1960s–1970s, when the only choices were magnetic-stripe plastic cards and relatively simple merchant terminals and ATMs. Figure 1 illustrates the numerous payment options now available.

Figure 1. Current Payment Options for Consumers

2.1 Current Status of EMV Chip Migration in the U.S.

To encourage adoption of EMV chip technology in the U.S., throughout 2011 and 2012 the global payment networks announced that beginning in October 2015, liability for counterfeit and, for some payment networks, lost or stolen card transactions at most POS locations would shift to the party that was not chip-enabled.[1] For example, if a cardholder presents a chip card and the merchant cannot process chip cards, liability potentially shifts from the issuer to the merchant. Announcement of these liability shift dates prompted a flurry of activity in the U.S. market, and currently the market is well on its way to implementing chip cards and EMV chip-enabled POS terminals successfully.

Initial card issuance efforts focused primarily on consumer and commercial credit cards, with debit cards now following quickly. Although the early adopters were mainly large issuers, many of the 10,000-plus financial institutions in the U.S. have either begun issuing chip cards or have active issuance projects underway. Some of the most recent projections of the estimated number of EMV chip cards and acceptance locations or devices that will be in the market are below.

- ✓ As of September 2015, the U.S. has over 200 million EMV cards issued.[2] (Smart Card Alliance webinar, October 2015)
- ✓ The Payments Security Task Force (PST) eight financial institution members (representing approximately 50 percent of U.S. payment card volume) reported that 60 percent of their U.S. consumer credit and debit

[1] "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/.

[2] "The Evolution of Payments Specifications and Tokenization," Smart Card Alliance and EMVCo webinar, October 1, 2015, http://www.smartcardalliance.org/activities-events-the-evolution-of-payment-specifications-and-tokenization-webinar-series/.

cards will contain EMV chips by the end of 2015, expanding to 98 percent by the end of 2017.[3] (PST, September 2015)

- ✓ Approximately 57 percent of consumers have at least one chip card in their wallet. (Visa media briefing, September 2015)

The merchant community has been somewhat slow to adopt EMV, due primarily to two factors:

1. Residual uncertainty regarding the U.S debit solution (merchants want to avoid multiple terminal or software upgrades). Although specifications for the U.S. debit solution have been published, some industry participants are still in the process of debit testing and certification.
2. The number and variety of merchant terminals and the fragmentation of the merchant community.

However, progress has been made, and the following are recent estimates of merchant adoption:

- ✓ MasterCard has reported that more than 350,000 national merchant locations accept chip cards and 26 percent of national and regional merchants have started to accept chip cards as of September 2015.[4] (MasterCard, September 2015)
- ✓ Visa has reported that SMB retailers account for 50 percent of Visa's U.S. chip payment volume.[5] (Visa, September 2015)
- ✓ The PST acquirer members estimate that about 40 percent of their terminals will be capable of accepting chip cards by the end of 2015.[6] (PST, September 2015)
- ✓ The Strawhecker Group estimated that 27 percent of merchants will be EMV-ready by October 2015, with EMV-readiness varying widely based on merchant category.[7] (Strawhecker Group, September 2015)

New ways of doing business typically involve challenges, and consumer and merchant education are critical to a successful merchant EMV adoption effort. Educational websites, such as the EMV Migration Forum's GoChipCard.com, aid this effort. In addition, consumers have expressed a desire to make payments in a more secure manner, and certain people are always willing to adopt new technologies.

The U.S. has also benefitted from observing trends in other countries that have rolled out chip cards. The U.S. market recognizes that while counterfeit fraud will be reduced, card-not-present fraud may increase. Efforts are underway to identify and implement processes that hopefully can address this concern in the U.S.[8]

Issuers must address several strategic questions as part of their chip card rollout. U.S. issuers are free to issue either PIN-preferring or signature-preferring cards (a "chip and choice" environment). Some issuers have decided to issue both, depending upon their product portfolio (e.g., corporate credit cards, consumer credit cards, debit cards). A second consideration for both issuers and merchants is what payment interfaces to support: both contactless and contact EMV payments, or contact payments only.

---

[3] http://newsroom.mastercard.com/press-releases/u-s-move-to-chip-cards-on-track/

[4] http://newsroom.mastercard.com/press-releases/mastercard-u-s-consumers-and-merchants-benefit-from-security-of-chip-cards/

[5] http://visacorporate.tumblr.com/post/130209237023/fact-sheet-emv-chip-adoption-in-the-us

[6] http://newsroom.mastercard.com/press-releases/u-s-move-to-chip-cards-on-track/

[7] http://files.ctctcdn.com/347071db201/08274512-6cce-4608-bec6-6e696cb57cb9.pdf, http://www.businesswire.com/news/home/20150917006071/en/Ready-U.S.-Merchants-EMV#.Vg1YoRFVhBc, http://www.businesswire.com/news/home/20150929006599/en/Types-Retail-Merchants-EMV-Ready#.Vg1ZLBFVhBd, http://files.ctctcdn.com/347071db201/540c1afb-61ac-4255-bb6e-5192093e2050.pdf

[8] A number of white papers have been published concerning this topic. See the EMV Migration Forum white paper, "Near-Term Solutions to Address the Growing Threat of Card-Not-Present Fraud," at http://www.emv-connection.com/near-term-solutions-to-address-the-growing-threat-of-card-not-present-fraud/, and the Smart Card Alliance white paper, "Card-Not-Present Fraud: A Primer on Trends and Transaction Authentication Processes," at http://www.emv-connection.com/card-not-present-fraud-a-primer-on-trends-and-transaction-authentication-processes/.

2.2 Current Status of Contactless Payments

Contactless chip cards were first issued in the U.S. in 2004. However, a combination of factors, including the convenience of magnetic stripe transactions with no signature required, minimal incremental spend, and modest merchant uptake, led to sluggish adoption rates in comparison with the rates in countries implementing contactless payment after EMV chip migration.

Contactless payments using mobile NFC devices started with Google Wallet in 2011, followed by Softcard in 2012. Again, adoption was slow due to limited merchant acceptance and mobile NFC device availability. The U.S. launch of Apple Pay in October 2014 gave mobile NFC an exciting new face, added a "coolness" factor, and reignited interest in contactless payments. Although adoption numbers remain relatively low, momentum appears to be building for payment using contactless chip cards and mobile NFC devices.

While focused on contact chip card issuance in the initial EMV chip card roll-out, issuers are now considering both rolling out dual interface cards and implementing new mobile strategies. Terminals that support both contactless and contact payments are readily available, with many supporting both interfaces as standard features. Many in the industry believe that as merchants and acquirers replace terminals to support contact EMV chip cards, merchants may also choose to support contactless payments.

Rolling out contactless payment using mobile NFC devices in the U.S. has both advantages and challenges. Since EMV chip card payments and contactless payments made using mobile NFC devices use the same transaction data, implementing them simultaneously rather than separately minimizes implementation time and complexity, including the time to test, certify, and deploy. Both issuers and merchants therefore have a perfect opportunity to position themselves to support EMV contact chip card, EMV contactless chip card, and mobile NFC device contactless payments. In addition, there are increasing numbers of mobile payment offerings in the U.S. that incorporate NFC technology (with examples shown in Table 1).

The primary challenge, other than the cost to issuers of dual interface cards, is the level of merchant acceptance. However, as noted above, merchant acceptance is expected to increase substantially in the next 1–2 years.

Table 1. Examples of U.S. Contactless Payment Offerings (Current and Announced) Using NFC

Offering	Technology Used in U.S. Contactless Payment[9]
Dual-interface chip card	EMV chip card with both contact and contactless interfaces
Apple Pay™	NFC, secure element, tokenization
Android Pay	NFC, Host Card Emulation, tokenization
Samsung Pay™	NFC, Host Card Emulation, Magnetic Secure Transmission, tokenization

[9] Additional information on the technology used for contactless payments can be found in the Smart Card Alliance white paper, "Host Card Emulation (HCE) 101," available at http://www.smartcardalliance.org/publications-host-card-emulation-101/.

3 The Intersection of EMV Chip, Contactless, and NFC

The intersection of EMV chip, contactless and NFC for contactless payments requires an understanding of the process for provisioning and using EMV chip cards and mobile NFC devices for payment. This section describes the following:

- How EMV chip cards are provisioned
- How EMV chip cards are used at the merchant point-of-sale
- How payment account credentials are provisioned into mobile NFC devices
- How mobile NFC devices are used for contactless payments

In the processes shown, it is important to remember the EMV chip payment transaction is more secure than a magnetic stripe transaction, resulting in strong fraud prevention, and the same security features are used with a mobile NFC device provisioned for contactless payments. Contact and contactless payment transactions incorporate data security techniques to ensure that the payment card and credentials are not counterfeit. In addition, chip cards and mobile NFC devices can also support multiple approaches to cardholder verification (e.g., signature, PIN, and no cardholder verification method required).

3.1 Provisioning and Using EMV Chip Cards

Figure 2 illustrates the process by which EMV contact and contactless chip cards are provisioned and used for payment transactions. The following describes the process; the numbered paragraphs describe the numbered box in the flow diagram.

1) The process starts with the card issuer. The EMV chip contains a secure microcontroller, which stores data safely and also provides support for multiple applications (e.g., debit, credit). The issuer or issuer's card personalization (perso) bureau provisions the card with one or more application identifiers (AIDs), based on what product type the EMV cards support, and configures the card for specific transaction rules (e.g., the cardholder verification method priorities, online/offline authorization and authentication). The issuer also encodes the magnetic stripe on the back of the EMV chip card.

2) Card perso bureaus send personalization commands to the card, conveying customer-specific data received from the issuer. The information includes both customer card information and additional security information that can be used while processing a payment transaction through an EMV chip-enabled terminal. Only entities that have the appropriate security keys are able to write data to the EMV chip.

3) The card is sent to the consumer. The customer activates the EMV chip card using the method provided by the issuer, and the card is ready for use.

4) The consumer uses the chip card at an EMV chip-enabled terminal. EMV chip transactions require interaction between the chip and an EMV terminal (using a protocol defined by the EMV specifications). EMV terminals are similar to magnetic stripe POS terminals but also accept EMV chip cards through insertion of a contact chip card or tap of a contactless chip card. If an EMV chip card is swiped at an EMV POS terminal, the terminal will prompt the cardholder to insert the card. EMV chip cards also support payment transactions initiated using the magnetic stripe at terminals that are not chip enabled.

   During a chip transaction, the chip must communicate with a chip reader in the terminal. The terminal helps enforce any rules set by the issuer on the chip. These rules can include enforcing services, such as offline data authentication, cardholder identity verification with a PIN or signature, and online

authorization. The issuer typically defines the rules to determine what payment transaction steps are required. Issuers can also set rules that require the chip to decline a transaction if the terminal is unable to perform the requested services.

5) As part of the transaction, the EMV chip generates an authorization request cryptogram (ARQC), which is then sent to the issuer host in an online authorization request. The ARQC can be verified by the issuer host, thus confirming that the chip card is not counterfeit.

6) The acquirer sends the authorization request through the payment network to the issuer or issuer processor. The issuer/issuer processor validates the transaction data and the ARQC and sends a response approving or declining the transaction. Authorization and clearing and settlement messages resulting from chip card transactions at the POS will carry the chip information through the transaction process.

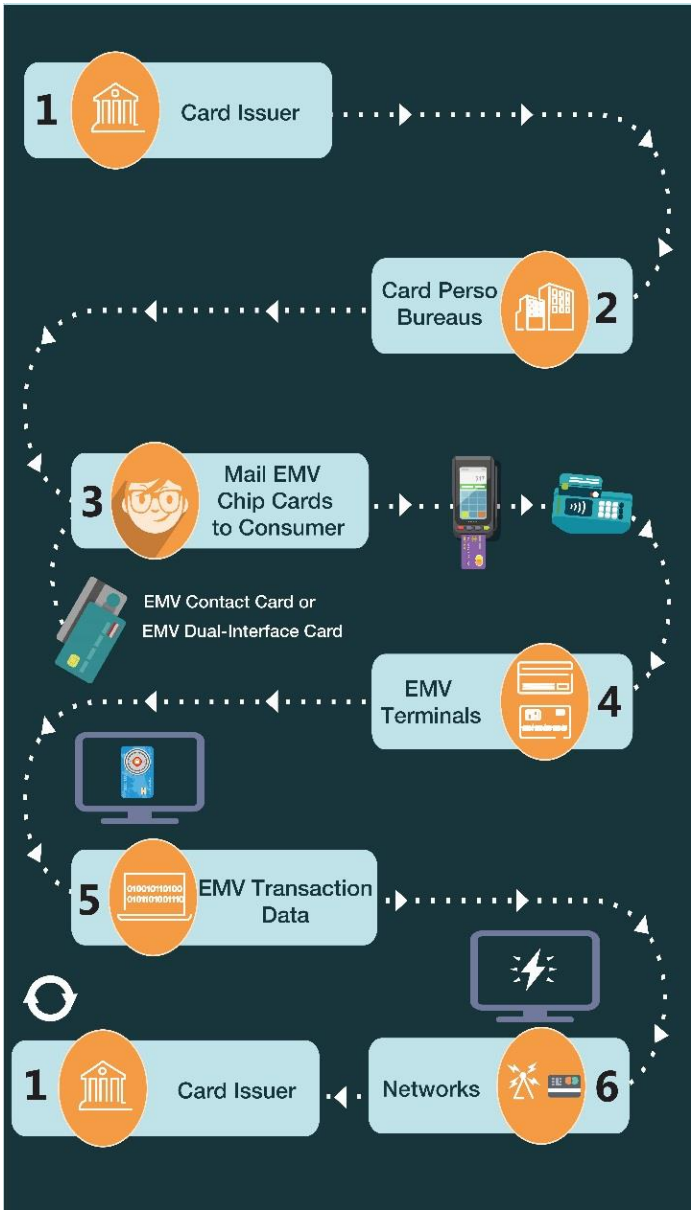

Figure 2. EMV Chip Card Provisioning and Transaction Flow

3.2 Provisioning and Using EMV Chip Cards and Mobile NFC Devices

Figure 2 illustrates the process by which EMV chip cards and mobile NFC devices are provisioned and used for transactions.

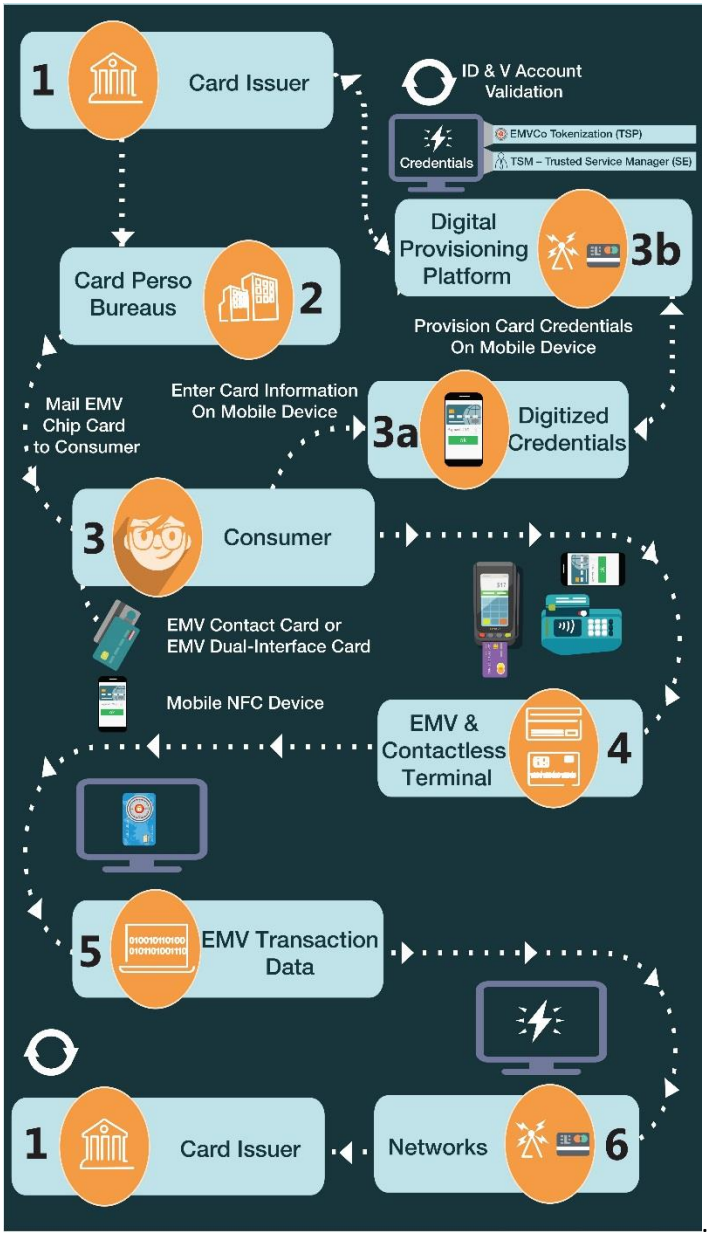

Figure 3. EMV Chip Card and Mobile NFC Provisioning and Transaction Flow

Similar to the process described in "Provisioning and Using EMV Chip Cards" above, the process to provision and use a mobile NFC device is also shown with six steps. Process steps 1, 2 and 3 are the same since these are provisioning the EMV chip card and delivering it to the consumer. The following describes the process; the numbered paragraphs describe the numbered box in the flow diagram.

1) The process starts with the card issuer. The EMV chip contains a secure microcontroller, which stores data safely and also provides support for multiple applications (debit, credit). The issuer or issuer's card personalization bureau provisions the card with one or more application identifiers (AIDs), based on what

product type the EMV cards support, and configures the card for specific transaction rules (e.g., the cardholder verification method priorities, online/offline authorization and authentication). The issuer also encodes the magnetic stripe on the back of the EMV chip card.

2) Card perso bureaus send personalization commands to the card, conveying customer-specific data received from the issuer. The information includes both customer card information and additional security information that can be used while processing a payment transaction through an EMV chip-enabled terminal. Only entities that have the appropriate security keys are able to write data to the EMV chip.

3) The card is sent to the consumer. The EMV chip cards store card information more securely than magnetic stripe cards. The customer activates the EMV chip card using the method provided by the issuer, and the card is ready for use.

   3a) To use the card for payment with a mobile NFC device, cardholders must first enter the card information into a mobile wallet application on the device. The issuer then verifies the cardholder's identity before provisioning the actual payment credentials to the mobile device.

   3b) For contactless payment using mobile NFC devices, the trend is to tokenize payment credentials for added security.[10] The digital provisioning platform provisions the payment information to the mobile device as digital credentials, which may involve a token service provider (TSP) to create a token from the payment card information. The token is what is provisioned to the device. The trusted service manager (TSM) provisions the credentials to the mobile device. The mobile device can then be used for contactless payment transactions using NFC technology.

4) EMV-enabled POS terminals can, if so configured, process both contact and contactless payment transactions initiated using chip cards and contactless payment transactions using mobile NFC devices. If an EMV chip card is swiped at a chip-enabled POS terminal (to read the magnetic stripe), the terminal will prompt the cardholder to insert the card (to read the chip).

5) The contactless payment transaction flow looks the same to a merchant regardless of whether a chip card or a mobile NFC device is being used. However, during an EMV transaction initiated from a mobile NFC device, a payment token may replace the card number and expiration date with numeric codes of the same length. Separate ranges of numeric codes are allocated so that no payment token can be confused with a card number. The TSP maintains the mapping between card numbers (coupled with their expiration dates) and payment tokens (coupled with their expiration dates).

   As in the previous flow, the EMV chip or the mobile NFC device payment application generates an ARQC, which is sent in an online authorization request to the issuer host for verification. For a mobile NFC device, the authorization request sends the token from the consumer's device to the merchant's terminal, acquirer, payment network and issuer.

6) The payment network sends a detokenization request to the TSP, who can translate token data to card data (and back) on request. The TSP returns the card data, which the payment network adds to the authorization request before forwarding the request to the issuer. The response from the issuer includes an authorization response cryptogram (ARPC) and card data but no token data. The response goes first to the payment network, which replaces the card data with token data obtained from the TSP before resending the response to the acquirer, the merchant, and the consumer's device.

[10] Additional information on tokenization can be found in the Smart Card Alliance white paper, "Technologies for Payment Fraud Prevention: EMV, Encryption and Tokenization," available at http://www.smartcardalliance.org/publications-technologies-for-payment-fraud-prevention-emv-encryption-and-tokenization/.

4 Key Considerations for Contactless Payment Implementations

Implementing contactless payment with EMV chip cards and mobile NFC devices poses additional considerations for merchants and issuers. These considerations include:

- How to migrate POS systems from contactless magnetic stripe data (MSD) to contactless EMV
- What types of transactions to accept
- What cardholder verification method (CVM) to implement
- Whether to allow offline transactions
- How to ensure a satisfactory consumer experience
- What costs will be incurred
- How contactless payment adoption is affected by mobile NFC device availability and other usability factors

4.1 POS Migration from Contactless MSD to Contactless EMV

Contactless payment applications currently reside in a POS terminal as multiple application kernels, one for each supported payment network. The kernels are developed and certified by the vendor who provides the terminal. The integration of a contactless payment terminal requires specific end-to-end certification that must be completed by the merchant or acquirer before deployment, similar to what is currently required for contact EMV chip implementation. The terminal's capabilities (contact, contactless, or both) determine the testing that must be performed for a given deployment.[11]

A contactless application kernel can be configured to support two types of transactions: contactless magnetic stripe data (MSD) transactions and contactless EMV chip transactions.

The contactless MSD transaction path was developed to streamline the acceptance of chip transactions over a contactless interface by minimizing the changes needed at the POS. To support a contactless MSD transaction, the contactless card reader and the card assembles Track 1 and Track 2 data in a format very similar to a magnetic stripe transaction. This enables the POS payment application to process authorizations and settlements without any network messaging changes other than those already in place for a magnetic stripe transaction.

The contactless EMV chip transaction path leverages the cryptographic functions normally associated with a contact EMV chip transaction and uses the same authorization and settlement fields as a contact chip transaction.[12] The contactless EMV chip transaction also supports enhanced features and functions such as the consumer device CVM (e.g., biometric factors or a pass code).

Like the contactless payment terminals, contactless chip cards and mobile NFC handsets supporting contactless payment can be configured to support either or both transaction types.

Merchants should check with their acquirers on the ability of their terminals to support MSD contactless and EMV contactless and various configuration options.

---

[11] "EMV Testing and Certification White Paper: Current U.S. Payment Brand Requirements for the Acquiring Community," EMV Migration Forum white paper, July 2013, http://www.emv-connection.com/downloads/2013/05/EMV_Testing_Certification_V1.0-080213.pdf.

[12] See EMV specifications, "Book 2 – Security and Key Management," Version 4.3, November, 2011, http://www.emvco.com/specifications.aspx?id=223.

4.2 Transaction Type Selection

Contactless payment acceptance is typically added to traditional card payment acceptance solutions, although there are some markets (e.g., transit, vending) in which contactless acceptance may be deployed without supporting a magnetic stripe or contact chip reader. Three contactless acceptance configuration options are possible:

- Option 1: Contactless only
- Option 2: Contactless and traditional magnetic stripe
- Option 3: Contactless, traditional magnetic stripe, and contact EMV chip

With Option 1, contactless payment is the only way payment is accepted, using either a mobile NFC device or contactless card. The contactless POS terminal is configured to support one or both of the contactless transaction paths (i.e., MSD or EMV) described in Section 4.1. This option may be used by transit to speed up payment at turnstiles and on buses.

When Option 2 is implemented, a contactless POS terminal is connected to the POS as a peripheral.[13] The contactless terminal is configured to support one or both of the contactless transaction paths described in Section 4.1. This option was common to initial U.S. deployments, where the contactless peripheral was configured to support the contactless MSD path only; this option may persist for merchants choosing not to adopt contact EMV.

For Option 3, the contactless reader is connected to (or integrated into) a POS terminal supporting traditional magnetic stripe and contact EMV chip transactions. The reader is configured to support one or both of the contactless transaction paths described in Section 4.1. Because the merchant POS infrastructure and acquirer host must be upgraded to carry contact EMV chip data, it is recommended that contactless EMV chip transactions also be supported.

As described in Section 4.1, the industry currently supports both contactless EMV chip transactions and contactless MSD transactions. Removing the MSD transaction path greatly simplifies integration, reduces the scope of testing, and removes the potential for MSD interoperability issues. Long-term merchant acceptance is expected to migrate to contactless EMV chip transactions, both for cards and mobile devices, as terminals are replaced. Industry stakeholders should check with the payment networks for additional information; migration requirements may vary by payment network.

4.3 Contactless Transactions and Cardholder Verification Method

Issuers and merchants should consider the CVM that will be used for contactless payment transactions.

Contactless payment technology can support PIN transactions. However, contactless payment is often used for small value transactions, where speed and convenience are critical and no cardholder verification is required.

Mobile payment devices can support new CVMs, such as consumer device CVM (CD-CVM), that further enhance security and are more convenient for the cardholder. CD-CVM is a user authentication function that is completed before the mobile phone is presented for payment. Examples of CD-CVMs include pass codes and biometric factors.

4.4 Offline Transactions

Offline contactless payment transaction authorization and data authentication may be permitted based on payment network rules. Offline data authentication can be a key risk management tool for certain industries, such as transit; offline data authentication is implemented independently from offline authorization.

[13] NFC peripheral readers are typically classed as intelligent readers.

4.5 Consumer Experience at the POS

The consumer experience at the POS is a critical consideration.

A contact EMV chip transaction requires that the consumer insert a card into an EMV chip-enabled terminal. The card remains in the terminal until the authorization response is received. Early removal of the card can cause the transaction to be restarted and possibly not receive any issuer scripting (i.e., commands and data sent by the issuer to the card).

In a contactless payment transaction, the consumer holds the contactless card or mobile NFC device within 1-2 inches of the contactless terminal; a visible or audible signal indicates when the transaction is complete. The contactless payment experience (often termed "tap-and-go") is fast and convenient for consumers. A mobile NFC device may require additional consumer input (e.g., a passcode entry or biometric), but the payment is still tap-and-go.

4.6 Contactless Implementation Cost Considerations

Contactless acceptance solutions are not cost free. The most obvious cost is for the additional hardware—a contactless-enabled terminal or peripheral. The terminal upgrades required for EMV chip acceptance often combine contact and contactless functionality, which may reduce or offset the cost of upgrading to accept contactless payment transactions.

There are also development costs associated with the integration of contactless applications, though these costs can be defrayed when designing the solution for contact and contactless chip transactions. Finally, there are costs associated with contactless terminal integration testing and configuration maintenance of three applications (magnetic stripe, contact EMV, and contactless).

Introducing contactless acceptance at a particular POS incurs incremental costs and complexity. A merchant decision on what capabilities to enable on their POS terminal may impact liability for card fraud. However, the value-added services that mobile NFC devices offer to both consumers and merchants could be seen as a significant driver for such adoption.

Likewise, costs are associated with issuing contactless chip cards. Contactless chip cards are more expensive than magnetic stripe cards or EMV chip cards with a contact interface only. The higher cost is driven by multiple factors, including the addition of an antenna to the chip, the costs of integrating the antenna into the card during fabrication, and higher card personalization costs. Issuers also need to factor in the cost of provisioning payment credentials to mobile NFC devices. Transaction authorization systems may require enhancements to validate contactless transactions (e.g., to handle the additional types of dynamic data used for contactless transactions). Finally, additional costs may be associated with testing and certifying contactless chip cards and payment applications used with mobile NFC devices.

4.7 Contactless Payment Acceptance, Device Availability and Usability

Both mobile NFC devices and contactless chip cards rely on the same contactless payment transaction acceptance technology. As a result, the adoption and popularity of using mobile NFC devices for contactless payments should increase contactless acceptance. Adoption will depend, however, on widespread availability of mobile devices that include NFC technology.

In the U.S., interest in contactless card issuance had waned in recent years, in part because perceptible advantages in the speed of cardholder presentment were negligible, compared with the traditional swipe once the payment networks adopted the "no signature required" rule. However, many countries that have migrated to EMV have seen an increase in dual-interface card issuance following an increase in contactless payment acceptance. In particular, the acceptance of contactless payments for transit has been a driver for both contactless card issuance and overall use of contactless payment by consumers.

4.8 Summary of Key Considerations for Contactless Implementation

There is no “one size fits all” recommendation about whether and when to implement contactless payment; different market segments have different requirements. The introduction of Apple Pay, Samsung Pay, and Android Pay has renewed focus on the use of mobile NFC devices to make contactless payments. This development and the EMV liability shift have motivated many merchants to consider how to best future-proof their solutions. However, contactless payment using mobile NFC devices is best regarded as a companion solution rather than a replacement for the card form factor.

5 Conclusion

The U.S. EMV migration is well on its way. Millions of EMV chip cards have been issued to consumers and both large and small merchants are upgrading their POS infrastructure to accept EMV chip transactions. In parallel with this mass migration, new mobile NFC devices have been introduced in the U.S. market that support contactless payment and that can be used at the same POS systems that accept contactless payment cards.

NFC and EMV are companion technologies. NFC applies to how devices communicate; EMV applies to payments made with contact and contactless chip cards or with a mobile NFC device emulating a contactless chip card. The launch of multiple, prominent mobile NFC devices supporting payments has fueled interest in contactless payments using not only mobile NFC devices, but also cards and other form factors.

While EMV chip migration is driven by the need to reduce payment card fraud, the use of mobile NFC devices is motivated by their ability to support value-added services beyond payment. A mobile NFC device can be used to conveniently pay with a tap, but can also deliver promotions, offers and/or loyalty programs to the consumer. These services can provide significant value and can be the business driver for contactless acceptance.

6 Publication Acknowledgements

This white paper was developed by the Smart Card Alliance Mobile and NFC Council and Payments Council to explain how EMV and NFC are companion technologies and clarify how they work together to enable secure payments.

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 Council members for their contributions. Participants involved in the development of this white paper included: ABnote; Advanced Card Systems; American Express; Booz Allen Hamilton; Capgemini; CH2M; Consult Hyperion; CPI Card Group; Cubic; Discover Financial Services; Exponent, Inc.; First Data Corporation; FIS; Fiserv; Gemalto; Giesecke & Devrient; GlobalPlatform; Heartland Payment Systems; Hewlett Packard Enterprise; Infineon Technologies; Initiative for Open Authentication (OATH); Ingenico; IQ Devices; JPMorgan Chase; MasterCard; Metropolitan Transportation Authority (MTA); Mozido CorFire; NBS Technologies; NXP Semiconductors; Oberthur Technologies; Quadagno & Associates; SHAZAM; STMicroelectronics; Thales e-Security; TSYS; Valid USA; Vantiv; Verifone; Visa Inc.; Wells Fargo; Xerox.

The Smart Card Alliance thanks the Council members who participated in the project team to write the document, including:

- **Andreas Aabye**, Visa Inc.
- **Christian Aabye**, Visa Inc.
- **Philip Andreae**, Oberthur Technologies
- **Deborah Baxley**, Capgemini
- **Aron Clark**, Visa Inc.
- **Jose Correa**, NXP Semiconductors
- **Fred Csaky**, FIS
- **Brady Cullimore**, American Express
- **David deKozan**, Cubic
- **Michael DeVitto**, MTA
- **Ana Egan**, Discover Financial Services
- **Frazier Evans**, Booz Allen Hamilton
- **Allen Friedman**, Ingenico
- **Scott Hagstrom**, ABnote
- **Sarah Hartman**, TSYS
- **Ian Hermon**, Thales e-Security
- **Margaret Heuer**, Wells Fargo
- **Simon Hurry**, Visa Inc.
- **Jack Jania**, Gemalto
- **Christine Lopez**, Vantiv
- **Joshua Martiesian**, MTA
- **Cathy Medich**, Smart Card Alliance
- **Bob Merkert**, Advanced Card Systems
- **Sadiq Mohammed**, MasterCard
- **Arnaud Moser**, Infineon Technologies
- **Manish Nathwani**, SHAZAM
- **Nick Pisarev**, Giesecke & Devrient
- **Peter Quadagno**, Quadagno & Associates
- **Lokesh Rachuri**, Capgemini
- **JC Raynon**, Verifone
- **Gerald Schoenecker**, Ingenico
- **Brian Stein**, CH2M
- **Mike Strock**, Smart Card Alliance
- **Lawrence Sutton**, CH2M
- **Sridher Swaminathan**, First Data
- **Jamie Topolski**, Fiserv
- **Sastry Yeleswarapu**, Capgemini
- **Tom Zalewski**, Mozido CorFire

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

- **Elle Archer**, American Express
- **Suresh Bachu**, Capgemini
- **Brent Bowen**, Valid USA
- **Hank Chavers**, GlobalPlatform
- **Deana Cook**, Chase Paymentech
- **Terry Dooley**, SHAZAM
- **Mike English**, Heartland Payment Systems
- **Don Malloy**, OATH
- **Oliver Manahan**, MasterCard
- **Pedro Martinez**, Gemalto
- **Brad McGoran**, Exponent, Inc.
- **Ken Mealey**, American Express
- **Jean Pare**, Xerox
- **Greg Proehl**, STMicroelectronics

- **Alan Fontella**, NBS Technologies
- **Tracey Harrington,** Discover Financial Services
- **Shane Irvin**, TSYS
- **Russ Kent**, Hewlett Packard Enterprise
- **Simon Laker**, Consult Hyperion
- **Akif Qazi**, Discover Financial Services
- **Steve Rogers**, IQ Devices
- **Tony Sabetti**, CPI Card Group
- **Paul Simon**, JPMorgan Chase
- **Adam Smitherman**, TSYS

The Smart Card Alliance also thanks **Lokesh Rachuri** and **Capgemini** for creating the graphics in Figures 2 and 3, and **Sarah Hartman** and **TSYS** for creating the graphic in Figure 1.

Trademark Notice

About the Smart Card Alliance Mobile & NFC Council

The Smart Card Alliance Mobile and NFC Council was formed to raise awareness and accelerate the adoption of payments, loyalty, marketing, promotion/coupons/offers, peer-to-peer, identity, and access control applications using NFC. The Council focuses on activities that will help to accelerate the practical application of the technology, providing a bridge between technology development/specification and the applications that can deliver business benefits to industry stakeholders.

The Council takes a broad industry view and brings together industry stakeholders in the different vertical markets that can benefit from mobile and NFC applications. The Council collaborates on: educating the market on the technology and the value of mobile and NFC applications; developing best practices for implementation; and working on identifying and overcoming issues inhibiting the industry.

About the Smart Card Alliance Payments Council

The Smart Card Alliance Payments Council focuses on facilitating the adoption of chip-enabled payments and payment applications in the U.S. through education programs for consumers, merchants, issuers, acquirers/processors, government regulators, mobile telecommunications providers and payments service providers. The group is bringing together payments industry stakeholders, including payments industry leaders, merchants and suppliers, and is working on projects related to implementing EMV, contactless payments, NFC-enabled payments and applications, mobile payments, and chip-enabled e-commerce. The Council's primary goal is to inform and educate the market about the value of chip-enabled payments in improving the security of the payments infrastructure and in enhancing the value of payments and payment-related applications for industry stakeholders. Council participation is open to any Smart Card Alliance member who wishes to contribute to the Council projects.

7 References

“Card-Not-Present Fraud: A Primer on Trends and Transaction Authentication Processes,” Smart Card Alliance Payments Council white paper, February 2014, http://www.emv-connection.com/card-not-present-fraud-a-primer-on-trends-and-transaction-authentication-processes/

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

”EMV Testing and Certification White Paper: Current U.S. Payment Brand Requirements for the Acquiring Community,” EMV Migration Forum white paper, July 2013, http://www.emv-connection.com/downloads/2013/05/EMV_Testing_Certification_V1.0-080213.pdf

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

“Host Card Emulation (HCE) 101,” Smart Card Alliance Mobile and NFC Council white paper, August 2014, http://www.smartcardalliance.org/publications-host-card-emulation-101/

“Near-Term Solutions to Address the Growing Threat of Card-Not-Present Fraud,” EMV Migration Forum white paper, April 2014, http://www.emv-connection.com/near-term-solutions-to-address-the-growing-threat-of-card-not-present-fraud/

Smart Card Alliance Mobile and NFC Council, http://www.smartcardalliance.org/activities-councils-mobile-and-nfc-council/

Smart Card Alliance Payments Council, http://www.smartcardalliance.org/activities-councils-payments/

Smart Card Alliance web site, 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/