EMV and NFC: Complementary Technologies that Deliver Secure Payments and Value-Added Functionality

A Smart Card Alliance Payments Council White Paper

Publication Date: October 2012

Publication Number: PC-12002

Smart Card Alliance
191 Clarksville Rd.
Princeton Junction, NJ08550
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.

Copyright © 2012 Smart Card Alliance, Inc. All rights reserved. Reproduction or distribution of this publication in any form is forbidden without prior permission from the Smart Card Alliance. The Smart Card Alliance has used best efforts to ensure, but cannot guarantee, that the information described in this report is accurate as of the publication date. The Smart Card Alliance disclaims all warranties as to the accuracy, completeness or adequacy of information in this report.

TABLE OF CONTENTS

1 INTRODUCTION 4

2 OVERVIEW OF EMV AND NFC 5

2.1 EMV 5
2.2 FRAUD AND SECURITY 5
2.3 NEAR FIELD COMMUNICATION 7

3 EMV IMPLEMENTATION IN AN NFC MOBILE DEVICE 8

3.1 EMV SPECIFICATIONS AND THE RELATIONSHIP TO NFC 8
3.2 EMV FOR MOBILE DEVICES 8
3.3 MOBILE CONTACTLESS ENHANCED PROCESSING 9
3.4 NFC MOBILE DEVICE ARCHITECTURE AND EMV 10
3.5 CERTIFICATION IN A MULTI-APPLICATION ENVIRONMENT 10
3.6 MOBILE WALLETS 11
3.7 PROVISIONING ACCOUNTS 12
3.8 OTHER USES OF EMV AND NFC 13

4 CONCLUSIONS 14

5 PUBLICATION ACKNOWLEDGEMENTS 15

1 Introduction

EMV® (Europay, MasterCard®, Visa®) is a global standard for secure and convenient payment using bank cards and the EMV payments infrastructure. EMV provides protection against the use of counterfeit, lost, or stolen cards for payment and against skimming. Issuers, merchants, consumers, and acquirers/processors all benefit from EMV.

The United States is the last market to migrate to EMV. Acquirer processors must support EMV transactions by April 2013. Beginning in 2015, card issuers and merchants accepting credit and debit cards will be affected by the fraud liability shift established by the payment brands.[1]

While the U.S. payment market is now moving to EMV, Near Field Communication (NFC) technology is emerging as a useful vehicle for consumer transactions. NFC is a communications technology that enables proximity-based communication between applications on mobile devices, tablets, personal computers, and other consumer electronic devices. The technology supports an extremely simple man-machine interface, facilitating the use of NFC for a number of functions, including smart posters, identity validation, mobile coupons, mobile advertising, ticketing, mobile payments, access control, information exchange, person-to-person payment, and social networking.

According to Gartner, smartphones will constitute over 90 percent of the overall installed handset base by 2014.[2] The Mobile Movement Study of 2011 found that 70 percent of shoppers use a smartphone while shopping in a store, and 74 percent made a purchase as a result of using a smartphone. The smartphone is becoming the platform of choice for shopping and represents a unique opportunity for retailers to engage with customers. Consumers today are using smartphones to complete financial transactions, evaluate products and services, and participate in merchant loyalty programs. NFC enables consumers to take this interaction to the next level. NFC can improve the consumer experience and the merchant's ability to reach prospective customers, and build loyalty with current customers.

The *NFC Times* found that there were less than 40 million NFC handsets worldwide in 2011.[3] However, according to iSuppli's August 2011 forecast544.7 million NFC handsets will be in use by 2015 (31 percent of all mobile phones)[4]; Informa Telecoms & Media predicts that by 2015, 630 million handsets will ship with NFC, representing 40 percent of all mobile phones.[5]

These developments raise some important questions. Are EMV and NFC complementary? Will one impede the progress and acceptance of the other? How do they fit together? Is it possible to "leapfrog" EMV payments and head straight to NFC mobile payments?

This Smart Card Alliance white paper is intended to answer these questions for merchants, issuers, acquirers/processors, and the mobile and NFC community in general. Its objectives are to:

- Provide a high-level description of EMV and NFC technology and their relationship to each other
- Describe how contactless EMV works with an NFC mobile device
- Describe how EMV and NFC technologies complement each other to deliver secure payment transactions
- Describe an overview of the ecosystem supporting NFC mobile EMV contactless payment provisioning and transaction processing

[1] Additional information on the payment brands' timelines, incentives and mandates for EMV migration can be found on the Smart Card Alliance EMV Connection web site, http://www.emv-connection.com.

[2] Gartner Inc., *A New Age of Mobile Services, Oct*. 29, 2010.

[3] "NFC Phone Shipments for 2011 Expected to Come in Below Projections," NFC Times, September 29, 2011, http://nfctimes.com/news/nfc-phone-shipments-2011-expected-below-projections

[4] "NFC Could Revolutionize Daily Consumer Activities," iSuppli, September 20, 2011, http://www.isuppli.com/Mobile-and-Wireless-Communications/MarketWatch/Pages/NFC-Could-Revolutionize-Daily-Consumer-Activities.aspx

[5] "630 Million NFC handsets to drive transactions worth US$71 billion by 2015," Informa Telecoms and Media press release, September 29, 2011, http://blogs.informatandm.com/3171/press-release-630-million-nfc-handsets-to-drive-transactions-worth-us71-billion-by-2015/

2 Overview of EMV and NFC

The terms *EMV* and *NFC* are used frequently in the payment world. EMV is a global standard for the interoperation of credit and debit payment cards, point of sale (POS) terminals, and ATMs that are based on smart card technology (chip-based cards).[6] All EMV-compliant cards can be accepted by all EMV-compliant acceptance devices irrespective of the issuing bank, acquirer, or manufacturer of the card or POS terminal, assuming the merchant device is set up to accept the brand on the card. NFC is a set of standards for mobile devices that enables them to establish radio communication by touching them together or bringing them into close proximity.

2.1 EMV[7]

Initially, EMV was a joint effort between Europay, MasterCard, and Visa to ensure payment security and global interoperability and enable MasterCard and Visa cards to be accepted everywhere. EMV provides the basis for the payments infrastructure that has been operating in many different parts of the world since the 1990s.

EMVCo – owned by American Express, MasterCard,[8] Visa, and JCB – manages, maintains and further develops the EMV specifications. EMVCo also manages the type approval processes for payment terminals, the security evaluation process for all EMV-compliant payment forms, and the type approval process for compliance with the EMVCo specifications for the Common Core Definition (CCD) and the Common Payment Application (CPA). These specifications are reviewed regularly to thwart potential and evolving security threats. EMVCo has also created specifications that define the protocol that contactless cards use to communicate with merchant payment terminals and the method for selecting which contactless application to use. Version 2.2 of the EMV specifications for payment terminals that support all payment brand contactless applications was published in June, 2012.

The use of EMV contact and contactless cards for secure payments offers multiple benefits:

- The cards offer better authentication of cardholder data and better protection against credit card fraud than magnetic stripe cards.
- A transaction-unique cryptogram secures payment transactions and protects cardholders, merchants, and issuers against fraud risks by authenticating during online transactions.
- A transaction-unique digital seal or signature stored in the card's chip proves authenticity of the card for offline transactions and prevents criminals from creating and using fraudulent payment cards.
- A common certified standard for processing transactions ensures global interoperability.

2.2 Fraud and Security

Chip-based payment cards were first introduced in Europe to combat high rates of fraud. By comparison, average U.S. fraud rates are one-third of the rates in European countries prior to the introduction of EMV.[9] Because EMV is increasingly used in Europe, Asia, Latin America, and Canada, card fraud for in-person payments has shifted to magnetic stripe cards, and much of that fraud is occurring in the United

[6] Chip-based cards contain an embedded microprocessor, essentially a small computer, that provides strong security features and other capabilities that cannot be implemented using traditional magnetic stripe cards.

[7] Detailed discussion of EMV technology and U.S. migration considerations is available in the Smart Card Alliance white paper, "Card Payments Roadmap in the U.S.: How Will EMV Impact the Future Payments Infrastructure?," available at http://www.smartcardalliance.org/pages/publications-card-payments-roadmap-in-the-us.

[8] Europay was absorbed by MasterCard in 2002.

[9] "Chip-and-Pin: Success and Challenges in Reducing Fraud," Retail Payments Risk Forum Working Paper, Federal Reserve Bank of Atlanta, Douglas King, January 2012, http://www.frbatlanta.org/documents/rprf/rprf_pubs/120111_wp.pdf.

States, which is one of the last countries to migrate to EMV. The Federal Reserve estimates that bank card fraud in the U.S. has increased by 70 percent since 2004.[10]

According to EMVCo, approximately 1.5 billion EMV cards have been issued globally and 21.9 million POS terminals accept EMV cards as of the end of 2011. This represents 44.7% of the total payment cards in circulation and 76.4% of the POS terminals installed globally, excluding the U.S.[11] Most countries implement EMV with PIN-based cardholder verification (commonly referred to as "chip and PIN"), which is a reliable means of verification that, when combined with dynamic data authentication, increases transaction security and reduces the risk of counterfeit and lost and stolen card fraud. In addition, EMV-compliant cards that implement dynamic data authentication (DDA) or combined data authentication (CDA) can guard against copying and capturing data from a card, another type of skimming attack.

While most EMV card issuance and acceptance has been outside of the United States, contactless payment is more common within the United States, where more than 80 million contactless payment cards are in circulation. These contactless cards are typically not EMV-compliant, but use the magnetic stripe data in the transaction combined with a dynamic value or cryptogram. Payments made using contactless EMV cards are faster and even more secure. After migrating initially to contact EMV cards, many countries are now moving to dual-interface cards that offer both contact and contactless payment options. This development allows bank cards to be used in additional contactless scenarios, such as for paying fares directly on trains and buses or for identification, such as on college campuses. Such transactions are often conducted offline to improve speed.

The landscape is still changing. American Express, Discover, MasterCard and Visa have announced their plans for moving to an EMV-based payments infrastructure in the U.S. In August 2011, Visa announced plans to accelerate chip migration and adoption of mobile payments in the United States,[12] through retailer incentives, processing infrastructure acceptance requirements and counterfeit card liability shift. In January 2012, MasterCard announced their U.S. roadmap to enable the next generation of electronic payments, with EMV the foundational technology.[13] Discover announced a roadmap that aligns EMV migration dates with MasterCard and Visa in March 2012.[14] In June 2012, American Express announced their U.S. EMV roadmap, which aligns migration dates with the other payment brands and states that issuance of EMV-compliant cards in the U.S. will start in the latter half of 2012.[15]

The brands' support for adoption of both EMV contact and contactless technology will help prepare for the arrival of NFC-based mobile contactless payments by encouraging the U.S. payment infrastructure to accept and process both contact and contactless payment transactions at the POS.

With the U.S. market coming onboard, the future of EMV is bright. Two upcoming milestones are significant:

- Effective October 1, 2012, Visa expanded its Technology Innovation Program (TIP) to waive the annual PCI data security audit requirement for merchants to the United States. To qualify, terminals must be enabled to accept both contact and contactless transactions, including mobile contactless payments based on NFC technology.
- All four payment brands require U.S. acquirer processors and subprocessor service providers to support merchant acceptance of chip transactions no later than April, 2013.

[10] Ibid.
[11] http://www.emvco.com/documents/EMVCo_2011_EMV_Deployment_Stats.pdf
[12] http://www.smartcardalliance.org/articles/2011/08/09/visa-announces-plans-to-accelerate-chip-migration-and-adoption-of-mobile-payments
[13] http://www.mastercard.us/mchip-emv.html
[14] http://discovernetworknews.com/stories/discover-implements-emv-mandate-for-u-s-canada-and-mexico/
[15] http://about.americanexpress.com/news/pr/2012/emv_roadmap.aspx

Additional information on milestones for EMV migration in the United States can be found on the Smart Card Alliance EMV Connection Web site.[16]

2.3 Near Field Communication

Developed jointly by Philips (now NXP Semiconductors) and Sony, NFC is a set of short-range wireless technologies, usually operating over a short distance, typically less than 4 cm. NFC operates at 13.56 MHz on an ISO/IEC 18000-3-compliant interface at rates ranging from 106 kbits per second to 424 kbits per second.

NFC-enabled devices can operate in three modes:

- Reader/writer mode, in which information is read to or written from a passive NFC-enabled target. NFC targets are usually packaged in simple form factors, such as tags or key fobs, which do not require batteries.
- Peer-to-peer mode, which allows bidirectional communication between two powered NFC-enabled devices.
- Card emulation mode, which allows an NFC-enabled mobile device to emulate a contactless smart card (e.g., an NFC mobile device can present secure card credentials to a reader, to pay at the merchant POS, to access a building, or to pay transit fares).

Various NFC applications, such as credit/debit payments, transit payments, ticketing, access control, and secure identity credential verification, need a very secure environment in which to store data and perform contactless transactions. The secure element (SE) within a mobile device provides a tamper-proof environment for storing data, performing cryptographic functions, and ensuring transaction security. Because of the SE, NFC offers strong cryptographic options, enabling financial or other secure transactions. Typical applications for secure NFC transactions are access control, financial or payment transactions, and transit payment and ticketing.

Consumers and businesses can benefit from NFC in several ways:

- Interactions are initiated by a simple tap of the device.
- NFC is flexible; it is suitable for a broad range of uses in different industries and environments.
- NFC technology follows universally implemented ISO, ECMA, and ETSI standards.
- Transmissions are short range.
- NFC works with current contactless card and reader technologies.
- Built-in capabilities support secure applications.

The outlook for NFC is promising. In the United States, Google launched Google Wallet for NFC mobile contactless payments in 2011, and the Isis is targeting the second half of 2012 for the launch of its mobile wallet.

[16] http://www.emv-connection.com.

3 EMV Implementation in an NFC Mobile Device

The implementation of EMV within an NFC mobile device is defined here as the use of an NFC-enabled mobile device in contactless card emulation mode. (Section 2.3 describes the NFC modes.) Operating in this mode, a mobile device can present EMV data over the contactless interface from an EMV-compliant payment application that is stored in the mobile device.

3.1 EMV Specifications and the Relationship to NFC

EMVCo has defined multiple specifications to support contactless payments:

- Application level data functionality
- The physical security of the devices in which EMV payment applications reside
- The EMV contactless interface

The EMV specifications define which contactless communications interfaces are supported for payment transactions. Both EMV and NFC support the same ISO/IEC 14443 standard contactless protocol.

3.2 EMV for Mobile Devices

EMVCo has published a number of documents to define how an NFC-enabled mobile device should implement an EMV-compliant payment application. These documents include:

- A common set of basic functional requirements for mobile devices[17]
- The common user interface functions for EMV mobile contactless applications[18]
- Requirements for product type approval[19]

These documents reference GlobalPlatform standards that define the platform for the SE and the management of applications within the SE. The payment brands define the mobile contactless payment application functionality offered by their own contactless scheme.[20] (The different schemes are listed in Table 1.)

Table 1. Payment Brand Contactless Brand Name

Payment Brand	**Contactless Brand**
American Express	ExpressPay
Discover	Zip
Interac	Flash
MasterCard	PayPass
Visa	payWave

American Express, MasterCard, and Visa each have two contactless payment application implementations (Table 2). One implementation defines contactless authorization data carried by a

[17] EMVco, *EMVCo Handset Requirements for Contactless Mobile Payment*, June 2010.
[18] EMVco, *EMV Contactless Mobile Payment - Application Activation User Interface*, December 2010. This specification states that NFC mobile contactless applications must adhere to the EMV Entry Point specification.
[19] EMVco, *CMP Product Type Approval Administrative Process*, February 2012.
[20] EMVCo has defined a contactless payment kernel that brands can base their implementations on; however, the implementations may use brand-configurable options.

magnetic stripe-like online authorization message. The other contactless implementation uses extended EMV-based authorization and authentication data elements.

Table 2. Payment Application Specification by Contactless Scheme

Scheme	**Magnetic Stripe Authorization**	**EMV Authorization**
American ExpressPay	ExpressPay1	ExpressPay2
MasterCard PayPass	MagStripe	M/Chip
Visa payWave	MSD	qVSDC
Interac	-	Flash
Discover	Zip	TBA

3.3 Mobile Contactless Enhanced Processing

Using a mobile device can facilitate contactless transactions. The application is now hosted in a device with features and functionality that a traditional chip card lacks, such as a keyboard and a communications channel for application management.

The transaction flow between a contactless reader and a mobile contactless payment application is defined by the EMVCo or the payment brand. Mobile contactless transactions that follow the current contactless transaction flow would offer the same cardholder verification methods: PIN, signature, or no cardholder verification (for low value transactions).

Mobile devices also provide additional capabilities for cardholder verification, including the ability to add an offline passcode that is verified by the application on the mobile device. The EMVCo contactless specifications for mobile devices allow cardholder verification to be done either by a POS terminal or by a cardholder device (e.g., a mobile phone).[21] The Association Européene Payez Mobile (AEPM)[22] has also defined a new cardholder verification method for mobile NFC applications: the consumer device cardholder verification method (CDCVM). This functionality illustrates one of the advantages of using a mobile device for payment.

In addition, even when the offline passcode is not required and the payment could therefore be performed with a mobile device with no or low battery, most mobile payment initiatives require the mobile device to be powered on and active for the payment to be conducted. This ensures that the appropriate messages can be passed to the user through the mobile device's user interface and prevents the mobile device transaction information from being read without the user knowledge or consent.

Similar to an EMV dual-interface card form factor, a mobile NFC-enabled device offers not only an NFC interface to perform a contactless transaction but is also accessible over the air by the payment credential issuer. Unlike a chip card which can only be accessed by the issuer at the time of an EMV transaction, a mobile device is continuously connected to a mobile network and allows issuers to better serve their customers. It is now possible to enhance the traditional interaction between consumer and merchant with value-add services such coupons/promotional offering and real-time account management.

[21] *EMVCo Contactless Specifications for Payment Systems*, Version 2.2, http://www.emvco.com/specifications.aspx?id=21
[22] http://www.aepm.com/uk-index.php

3.4 NFC Mobile Device Architecture and EMV

In an NFC mobile device, payment functionality is divided between the user interface and the payment brand's mobile contactless payment application. The user interface functionality may be specifically developed for each particular mobile device and operating system but should follow the same functional principles. The user interface facilitates application management, application selection and cardholder verification. Payment transaction processing is a responsibility of the payment application itself.

The payment application and the consumer's payment account information are stored in the SE. The SE in an NFC-enabled handset can be in one of three locations: in an embedded device; in a removable SIM/UICC or as a separate device (e.g., a microSD card) (Figure 1).[23]

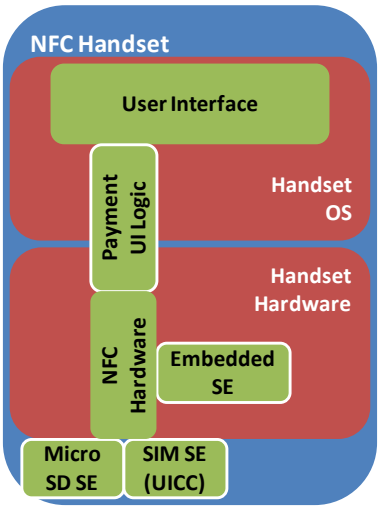

Figure 1. Simplified NFC Mobile Device Schematic

NFC-enabled devices that have their own antennas and SEs (for example, the iCarte device, microSD solutions, and SIM aerial adaptors) can also be attached to or inserted in a mobile device as a bridging technology. These devices interact directly with the mobile user interface. Because a contactless sticker is unable to interact directly with the mobile user interface, it constitutes another type of contactless card, not an NFC device.

All of the SE technology described above employs the same security and functional architecture, following standards established by EMVCo and GlobalPlatform. The payment application residing on the secure element is in fact in many cases an enhanced version of a market-proven payment application residing on millions of EMV cards today.

3.5 Certification in a Multi-Application Environment

In the current mobile payment models, the consumer will be able to load multiple payment cards onto the mobile payment device. Therefore, it is likely that the SE will host payment applications that belong to multiple payment brands. In addition, depending on the mobile device and payment model, the secure element may either be hosted in an embedded device, in a removable SIM/UICC or in a separate device (e.g., a microSD card). Considering the number of combinations of SE and payment applications, certification of mobile payment cards could be a challenge. Fortunately, EMVCo together with GlobalPlatform envision a system of modular certification.

[23] A discussion of these different approaches can be found in the Smart Card Alliance white paper, *The Mobile Payments and NFC Landscape: A U.S. Perspective*, http://www.smartcardalliance.org/pages/publications-the-mobile-payments-and-nfc-landscape-a-us-perspective.

To minimize the introduction of additional vulnerability (security or functional) and to achieve interoperability and consistent behavior among the different mobile products, EMVCo has defined a certification process[24] that applies to the components involved in the contactless mobile payment applications (i.e., the SE and the mobile platform).

The EMVCo contactless mobile platform product type approval process creates a mechanism to test component compliance with the EMV specifications (Figure 2).[25] The EMV certification requirements include a security evaluation for the secure element holding the payment application, requirements for the identification of EMV applications on a device, and conformance to a reference application activation user interface (AAUI) on the device. EMVCo does not evaluate the contactless antenna and module in the mobile device, applications external to the secure element, or the mobile device's user interface application. EMVCo also does not evaluate the operating system and transmission protocol.

In addition to the EMVCo approval process, the payment brands have their own type approval processes for their specific payment applications.

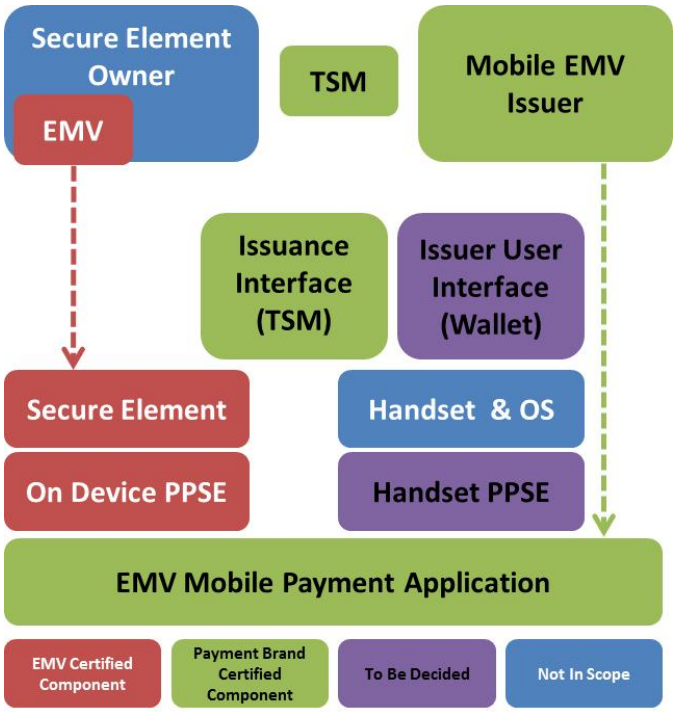

Figure 2. EMV Certification Requirements

3.6 Mobile Wallets

Consumers will be able to view and manage mobile payment cards and other applications (e.g., coupons, loyalty programs) through the mobile wallet graphical user interface. Mobile wallets may be developed by the banks, but other organizations will develop their own wallet applications as well.

A mobile wallet application will typically let the end-user activate or deactivate a mobile payment card and may let the user rearrange the cards in a preferred order. EMVCo has been formalizing the card management and the card's presentation to the end-user in the Application Activation User Interface specification (AAUI)[26]. AAUI defines a framework of minimum functional requirements of a mobile wallet,

[24]

[25] EMVco, *CMP Product Type Approval Administrative Process*, February 2012.

[26] EMV Contactless Mobile Payment - Application Activation User Interface, v1.0 December 2010

which will likely be refined through business agreements. For example, in the European model defined by AEPM, only one card may be active at a time, but other models may be adopted.

In particular, AAUI defines new requirements for the Proximity Payment Systems Environment (PPSE) application, which is a standard application that is used by contactless terminals to determine which of the active applications should be used for payment. So far, the approval of the mobile wallet applications is defined by the payment brands.

3.7 Provisioning Accounts

When the consumer requests a mobile payment service, the service provider must check that the consumer is eligible for the service – that is, that the consumer's mobile environment is compatible with the service (e.g., mobile network, mobile device type, secure element capability).

Once the eligibility check is done, the payment account must be provisioned onto the NFC mobile device. The payment data to be loaded onto the mobile device will likely be very similar to the data used for the personalization of traditional payment cards. Therefore, the issuers of both traditional cards and mobile payment cards should make sure that the personalization profiles created for card applications can be upgraded to NFC applications without introducing major changes in the profile structure or personalization process.

However, the fact that the creation of personalized payment data for an account must be created in real time presents a significant challenge using current card production systems. Currently, most systems deliver payment data for credit and debit products directly to the card manufacturer, typically in a batch file.

A new model for provisioning has emerged to address the difficulty of personalizing products for NFC-enabled mobile devices. Personalized account information is sent over-the-air (OTA) to mobile devices using trusted service managers (TSMs), third parties who work with the payment account issuer and the mobile operator. The OTA approach requires that the process be managed from the point at which the payment product is requested through delivery. Although OTA provisioning uses a new channel of transporting payment credentials securely, it relies on the same foundation defined by EMVCo in terms of formatting the data (using ECPS - EMV Card Personalization Specifications), and ensuring the highest level of security and confidentiality by using industry-proven cryptographic standards defined by EMVCo and GlobalPlatform.

During delivery, a customer may have to accept multiple downloads. The application must then be made available for use over the user interface, either through the EMV user interface or through a proprietary (wallet) process.

Mobile payment accounts are typically either prepaid accounts or a credit or debit account that is a companion to a current customer account. Mobile payment accounts are typically associated with accounts that also issue a physical plastic card, to accommodate use at acceptance points that are not enabled for contactless transactions. The model for issuance varies among providers.

- The Isis™ Mobile Wallet is expected to facilitate standardized integration of payment applications from a number of issuers (including American Express, Capital One, and Chase) into the secure element.
- Google Wallet has partnered with MasterCard and is implementing a solution based on a payment application loaded within the embedded secure element of the phone.[27] This application can then be linked any payment card, whose details are held centrally within a cloud-based wallet. The service also supports Citibank customers loading their payment card details onto the secure element.

[27] Google Wallet, http://www.google.com/wallet/faq.html#payments-online

In the UK, Orange and Barclaycard offer a prepaid product with Quick Tap. Orange and Barclaycard install their payment application in the SIM SE during the manufacture of a SIM for QuickTap; the SIM is associated with the consumer later.

EMVCo is specifying deployment models with specific SE structures and hierarchies to guarantee fully secure provisioning.[28] In addition, payment brands also have adapted their requirements for certification for the TSM and the OTA provisioning process.

3.8 Other Uses of EMV and NFC

As highlighted by Google Wallet, loyalty applications and couponing may offer the most significant market value opportunities for retailers. For example, in the United States several retailers, including American Eagle Outfitters, Macy*s, and The Container Store, have deployed Google Wallet to enhance the customer experience and accelerate the checkout process.

The EMV payment application can co-exist with these new functions if both the contactless reader payment application and the contactless card payment application are changed. There are currently no such products available in the United States. Only a few products are available in Europe, including the FinnishK-Plussa contactless loyalty and payment card.

The EMV AAUI specification may create opportunities to build platforms for loyalty and couponing in the future. However, using this functionality may introduce certification issues for handset applications that interface with other NFC mobile applications on a device.

[28] EMVCo Mobile Contactless - EMV Profiles of GlobalPlatform - UICC Configuration, v1.0 December 2010

4 Conclusions

EMV was introduced in 1996 as a globally interoperable payment standard, with the objective being to reduce fraud. Europe has witnessed a dramatic reduction in the amount of lost, stolen, and counterfeit card fraud since 2005, while fraud activity has tended to increase in the United States. The four major U.S. payment brands have therefore coordinated key milestones for U.S. implementation of EMV. Meanwhile, the United States is one of the largest contactless payments market in the world. In addition, a number of high profile NFC deployments are either in pilot or under way.

Implementing EMV at the same time that NFC spreads makes sense. The three payment technologies—contact EMV, contactless EMV, and NFC in contactless card emulation mode—are standards-based and interoperable within a payment brand. Not all consumers will adopt NFC mobile payments immediately. For those who do, the NFC mobile payment applications will typically be offered with companion plastic cards, to ensure universal acceptance at merchants without contactless readers. The EMV mobile payment application on the NFC mobile handset will be compatible with the EMV contactless acceptance infrastructure used for cards. As an additional safeguard for privacy, payment applications on NFC mobile phones can optionally include an additional layer of security, requiring a PIN to be entered on the handset to release payment details from the handset and confirm a payment.

Banks are under no mandate to issue EMV cards but are likely to issue EMV-compliant cards widely by 2015 to be ready for the fraud liability shift in October 2015. In addition, NFC mobile payment applications are starting to emerge in 2012, with prominent deployments in the U.S. Chip cards and mobile devices both require more complex certification and personalization than magnetic stripe cards. Personalization of mobile handsets requires the services of entities known as the trusted service managers, which interface with mobile operators, banks, and payment brands. Installation and personalization of the payment application on the mobile device can be conducted OTA. Over the longer-term, overall issuing costs will likely decrease, as mass compromise and reissuance scenarios disappear, and eventually the number of plastic cards decreases.

Consumers should find the safety and security of compromise-free cards appealing, and NFC mobile contactless payments offer attractive additional functionality. Payment applications can reside in an NFC mobile wallet, which can house other payment-related functions, such as coupons, offers, transit tickets, and loyalty applications. While these applications are technically feasible on multi-application chip cards or in the cloud, the mobile device's user interface makes them more appealing and easier to use.

Merchants should consider meeting the EMV milestones and preparing for all payment interfaces: EMV contact and EMV contactless. Doing so minimizes fraud exposure after the liability shift, ensures that all U.S. and foreign customers are able to perform transactions using their cards and mobile devices, reaps the benefits of PCI audit and account data compromise relief offered by the payment brands, and positions merchants to accept NFC-enabled EMV mobile contactless payments, as well as other NFC-enabled retail applications (e.g., loyalty programs, coupons and offers).

For the payments industry, adopting EMV could allow the U.S. market to reclaim a leading position, leapfrogging the rest of the world with EMV contactless and NFC-enabled EMV mobile contactless payments deployment. Fraud can be reduced, and the next generation of payments innovation can flourish.

5 Publication Acknowledgements

This white paper was developed by the Smart Card Alliance Payments Council to describe how EMV and NFC complement each other and work together.

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 the Payments Council members for their contributions. Participants involved in the development of this white paper included: Accenture LLP; Acumen Building Enterprise, Inc.; Apriva; Capgemini USA Inc.; Chase Card Services; Clear2Pay; Connexem Consulting; Consult Hyperion; Datacard Group; Exponent; First Data Corporation; FIS; Gemalto; Giesecke & Devrient; Heartland Payment Systems; Identification Technology Partners; Infineon Technologies; INSIDE Secure; Interac Association/Acxsys Corporation; NACHA – The Electronic Payment Association; NagraID Security; NXP Semiconductors; Quadagno & Associates; SHAZAM; TSYS; Visa Inc.; Watchdata Technologies Pte Ltd.

The Smart Card Alliance thanks the following Council members who contributed to writing and/or reviewing this white paper:

- **Christa Addy**, SHAZAM
- **Philip Andreae**, Accenture LLP
- **Nancy Baunis**, Connexem Consulting
- **Deborah Baxley**, Capgemini
- **Louis Bianchin**, Watchdata
- **Brent Bowen**, INSIDE Secure
- **Deana Cook**, Chase Card Services
- **Fred Csaky**, FIS
- **Michael English**, Heartland Payment Systems
- **Allen Friedman**, TSYS
- **Scott Green**, SHAZAM
- **Simon Hurry**, Visa Inc.
- **Brent Iles**, Datacard Group
- **Grace Jung**, Interac Association/Acxsys Corp.
- **Werner Koele**, Infineon Technologies
- **Brintha Koether**, NXP Semiconductors
- **Umesh Kulkari**, Clear2Pay
- **Edwin Lam**, Interac Association/Acxsys Corp.
- **Don Malloy**, NagraID Security
- **Brad McGoran**, Exponent
- **Cathy Medich**, Smart Card Alliance
- **Bob Murray**, Acumen Building Enterprise
- **Nick Norman**, Consult Hyperion
- **Susan Pandy**, NACHA
- **Anthony Pickup**, Consult Hyperion
- **Nick Pisarev**, Giesecke & Devrient
- **Peter Quadagno**, Quadagno & Associates
- **Bill Robertson**, Apriva
- **Dori Skelding**, Chase Card Services
- **Tammy Smith**, NXP Semiconductors
- **Brian Stein**, Accenture LLP
- **Sridher Swaminathan**, First Data Corp.
- **Astrid Wang-Reboud**, Gemalto
- **Mike Zercher**, NXP Semiconductors
- **Rob Zivney**, ID Technology Partners

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.