WHITE PAPER

Smart Card Alliance

Payments Council

A SMART CARD ALLIANCE PAYMENTS COUNCIL WHITE PAPER

Technologies for Payment Fraud Prevention: EMV, Encryption and Tokenization

Publication Date: October 2014
Publication Number: PC-14002

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

This white paper presents three technologies that work in tandem to protect those businesses processing credit and debit cards against card fraud. The three technologies are:

- EMV, which improves the security of a payment transaction by providing cryptographic card authentication that protects the merchant and issuer against the acceptance of counterfeit cards. EMV also offers cardholder verification and several means of transaction authentication that help safely authorize transactions.
- End-to-end encryption (E2EE) or point-to-point encryption (P2PE), which can immediately encrypt card data at inception – at card swipe, key entry, tap or insertion – so that no one else can read it and monetize the card data.
- Tokenization, which replaces card data with "tokens" that are unusable by outsiders and have no value outside of a specific merchant or acceptance channel.

Why are these three technologies discussed in this paper and needed by the payments industry? According to the Verizon 2014 Data Breach Investigations Report, restaurants, hotels, grocery stores, gas stations and other brick-and-mortar outlets suffered 285 security breaches with confirmed data losses during 2013.[1] While retailers such as Target and Neiman Marcus made the news, the report states that the vast majority of these breaches occurred against small to mid-sized companies.

Verizon's report declares that 2013 can be characterized as "a year of transition from geopolitical attacks to large-scale attacks on payment card systems." During 2013, POS intrusions accounted for 31 percent of the 148 retail breaches, with payment card skimming accounting for another six percent. POS intrusions accounted for 75 percent of the 137 accommodation sector breaches.

This white paper presents the authorization process for EMV, drivers leading the United States to implement EMV, the value of EMV to issuers and the value of EMV to merchants. It then discusses E2EE and P2PE, defining both while presenting different implementations of transaction encryption used by the payments industry. Finally, the paper speaks to tokenization – the standards, its complementary role with respect to EMV and encryption, tokenization assurance and activities relative to tokenization that are taking place in the payments industry today.

The white paper concludes with a discussion of how payments industry implementation of the three technologies together secures the payments infrastructure and prevents payment fraud.

[1] Verizon 2014 Data Breach Investigations Report: http://www.verizonenterprise.com/DBIR/2014/.

2 EMV

The growth in counterfeit card fraud was what originally motivated the global payments industry to move to chip technology for bank cards and to develop the EMV specification for cards based on chip technology (smart cards). The EMV specification defines a global interoperable standard for smart chip-based bank cards. The specification is managed by EMVCo and has been available since 1996.

Financial institutions in Europe, Latin America, Asia/Pacific, Canada and the United States are either already issuing EMV chip cards for credit and debit payment or migrating to EMV. According to EMVCo, approximately 2.3 billion EMV chip cards have been issued globally and 36.9 million point-of-sale (POS) terminals accept EMV chip cards as of the fourth quarter of 2013.[2]

In addition to growth in fraud, the cost and reliability of the communications and transaction processing infrastructure contributed to the adoption of EMV technology outside of the U.S. Markets in Western Europe, Australia, Latin America, and Canada have historically experienced much higher rates of payment card fraud than what the U.S. market has experienced. These higher fraud rates led to the early adoption of EMV. In addition, the lack of cost-effective processing and reliable communications at the merchant led to the adoption of offline EMV capabilities to increase transaction security and enable offline payments processing between the card and the terminal. Each of these markets is more homogeneous than the U.S. market, requiring fewer financial institutions and merchants to convert to chip technology, so the business case for making the investment in EMV has been very strong. Countries that have implemented EMV have seen counterfeit fraud decline by as much as 67 percent in the face-to-face environment.[3]

The U.S. has started to migrate to EMV chip technology. Between July 2011 and June 2012, American Express, Discover, MasterCard, and Visa announced plans for moving the U.S. to an EMV-based payments infrastructure. The plans include a series of incentives and policy changes for card issuers and merchants, with a target date of October 2015 to complete implementation of EMV chip cards, terminals, and processing systems. The global payment brands set October 2015 as the date for the payment liability shift, at which point the responsibility for fraud resulting from a card-present payment transaction will shift to the party using the least secure technology. The liability shift date for ATM operators and retail petroleum outlets are 2016 (MasterCard only) and 2017 (all other payment brands), respectively.[4]

2.1 Functionality

Smart card technology embeds a secure integrated circuit chip with a microprocessor in a card or other form factor. The plastic card is the most commonly used form factor; however, key fobs, microSD memory cards, adhesive stickers, and most recently, NFC-enabled smartphones can all accommodate the same chip technology. The chip is powered by the card reader or by a battery associated with the form factor, enabling the chip to communicate with the reader.

The interface with the reader can require physical contact (compliant with ISO/IEC 7816[5]) or be contactless (ISO/IEC 14443[6]). Dual-interface cards include both contact and contactless interfaces and can communicate over either interface, depending on the capabilities of the acceptance device.

---

[2] EMVCo, "Worldwide EMV Card and Terminal Deployment," http://www.emvco.com/about_emvco.aspx?id=202.

[3] "New Card and Banking Fraud Figures," UK Cards Association, March 10, 2010, http://www.theukcardsassociation.org.uk/news/new-card-banking-fraud-figures.asp.

[4] Additional information on the payment brand liability shift dates can be found at: http://www.emv-connection.com/emv-faq/.

[5] ISO/IEC 7816 – Identification Cards – Integrated Circuit Cards, https://www.iso.org.

[6] ISO/IEC 14443 Series – Identification Cards – Contactless Integrated Circuit(s) Cards – Proximity Cards, https://www.iso.org.

Contact cards communicate through a contact plate on the card. The plate must come into contact with the terminal contacts, usually through a reader into which the card is inserted. ATMs often rely on motorized readers that draw the card into the ATM, where it is staged, to prevent withdrawal during a transaction. Some ATMs may support dip readers which require the cardholder to insert the card; the ATM will lock the card and read the data from the card while executing the EMV transaction. Contactless cards contain an antenna and communicate over a radio frequency (RF). Dual-interface cards combine both interface techniques, using a single chip.

In a contact or dual-interface card, the contact plate is the gold or silver plate on the front of the card. The embedded antenna is not visible on most contactless cards; however, many contactless cards display a symbol indicating that they have contactless capability.[7]

2.2 Payment Transaction Processing

Because online-only magnetic stripe cards are prevalent in the United States, the current transaction authorization process relies on static data to authenticate a card. Issuers measure risk using sophisticated fraud management systems and online networks that incorporate specific rules and parameters before authorizing a payment transaction.

2.2.1 Magnetic Stripe Transaction Processing

Magnetic stripe card transaction authorization follows this process:

1. A cardholder swipes a magnetic stripe card at a terminal.
2. Static Track 1 and/or Track 2 data are captured.[8]
3. An authorization request is formed.
4. The transaction is sent to an acquirer, then routed to the appropriate payment brand or network, and finally delivered to an issuer for authentication and authorization.

The current transaction authorization process relies on static card data to authenticate the card and on online networks to authorize transactions. The issuer validates the track data and determines the authenticity of the card based on the static card security code[9] data element within the track. The issuer may then also verify the PIN (if appropriate for debit transactions). At this stage of the transaction, the issuer cannot assume that the card is authentic or that the cardholder is present. Issuers therefore employ fraud management systems that apply their particular risk management rules and parameters to determine whether the card is genuine and to verify that it's being used by the rightful cardholder.

Occasionally, an issuer responds to an authorization request with a referral or contacts the cardholder directly, using a text message or telephoning the cardholder. Only after issuers are comfortable that the card is genuine and the rightful cardholder is present do they determine whether the cardholder has the funds or credit line available to pay for the transaction.

For a long time, U.S. issuers effectively managed fraud in the zero floor-limit (always online) environment using online fraud detection tools. However, the rapidly changing fraud landscape and the scale of recent data breaches make EMV a compelling long-term solution. The value of EMV is that it devalues static magnetic stripe track data and introduces a secure dynamic element into each and every transaction. In addition, issuers can exploit the risk-

---

[7] http://www.emvco.com/best_practices.aspx?id=117.

[8] It is important to note that static track data can be easily read and written to any magnetic stripe card (e.g., a hotel key or other blank mag-stripe card).

[9] These are referred to as Card Verification Value (CVV), Card Verification Code (CVC) or Card ID (CID) by the different payment brands.

management capabilities of EMV to authorize transactions at the POS when the transaction value is low or the network is not available.

2.2.2 EMV Transaction Processing

Contrary to magnetic stripe cards, EMV chip cards are designed to store sensitive data (such as PINs or keys) securely, and they have the processing power that allows them to manage risk and perform cryptographic computations dynamically.

The logic behind EMV transaction processing is not radically different from magnetic stripe transaction processing. Just 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 that must be performed before a transaction can be authorized.

However, thanks to the secure chip technology, EMV processing brings new features to enhance interoperability and security:

- EMV offers the possibility to define flexible cardholder verification; for example, banks that manage multiple card portfolios may configure some cards to be PIN-preferring and other cards to be signature-preferring;
- EMV offers enhanced card authentication methods that rely on dynamic data and strong cryptographic techniques.

The EMV transaction authentication process relies on the generation of dynamic data (i.e., a digital signature) to authenticate a card or device. The online and offline signatures are generated using either and sometimes both asymmetric and symmetric cryptographic keys and algorithms stored and executed securely on the card.

EMV transaction authorization follows this process:

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

One of the key attributes of EMV is the ability to authenticate the card to be sure that it is not a clone or counterfeit of the card. Two methods are defined within the EMV specification, offline card authentication and online card authentication

Offline card authentication uses the asymmetric cryptography defined by EMV 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 magnetic stripe, allowing the issuer to further authenticate the card and authorize the transaction. The important difference is the card's use of symmetric key technology to generate the unique application cryptogram. This cryptogram, called the authorization request cryptogram (ARQC), 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 the risk of skimming. The chip generates unique digital signatures and cryptograms by applying an algorithm to data provided by the card and the acceptance device and to transaction-specific data (e.g., card verification result, application transaction counter value, amount of the transaction, the date, and a terminal-generated unpredictable number).

Figure 1 illustrates the online EMV card authentication and authorization process.

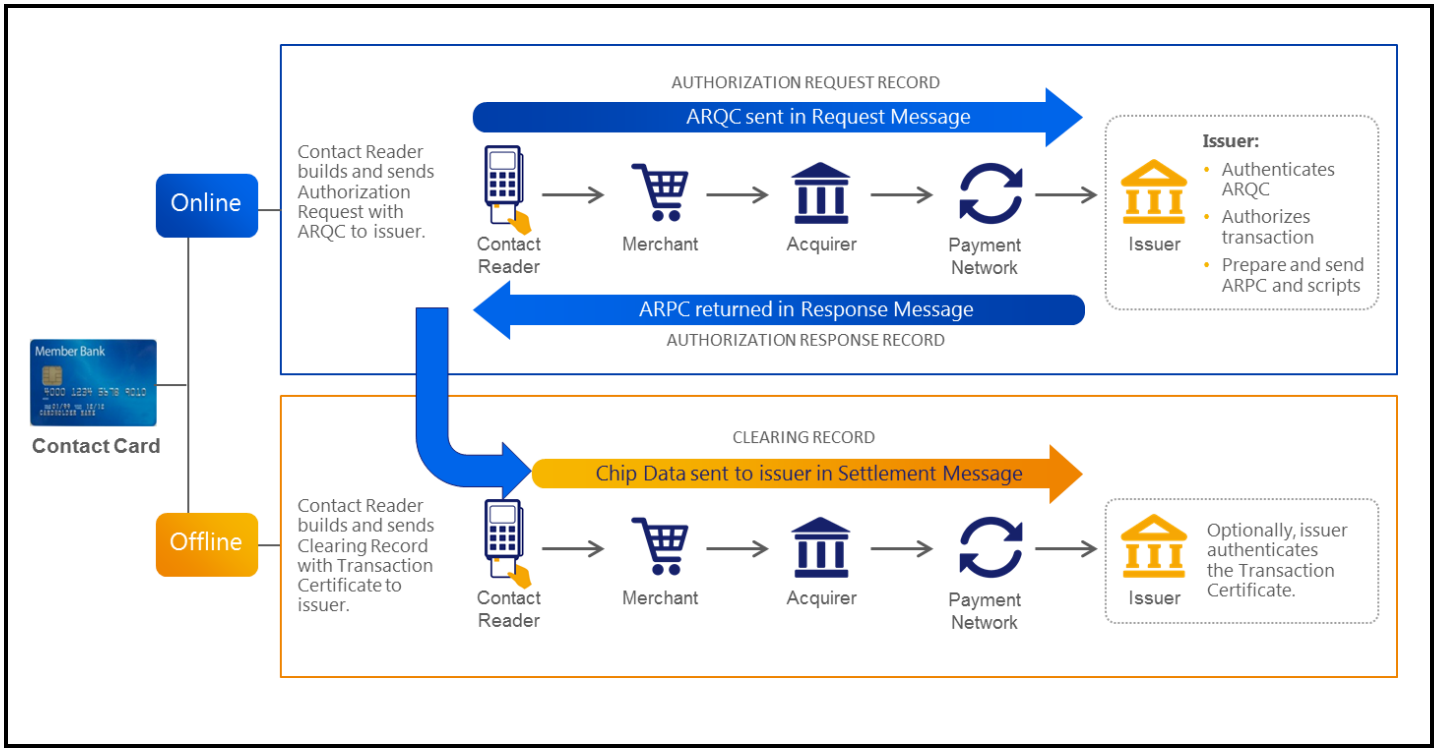


Figure 1. EMV Authentication Process

2.3 Drivers for U.S. Adoption of EMV

EMV adoption in the U.S. is motivated by the desire to mitigate growing magnetic stripe counterfeit fraud, provide a secure platform for transactions involving mobile devices, and enhance acceptance of cross-border transactions.

2.3.1 Fraud Mitigation

A key objective for the payments ecosystem is to move away from the dependency on static data and toward the use of dynamic cryptographic data to secure all transactions. Recent data breaches have given acquirers, issuers, and merchants a clear understanding of the increasing risk associated with relying on static magnetic stripe data for transaction processing. Merchant processors and acquirers who process, transmit, and store transaction data must secure it. Issuers must employ costly fraud mitigation schemes to prevent counterfeit transactions.

Moving to EMV technology can reduce the burden on issuers, processors, acquirers and merchants. The cryptogram is unique for each transaction, and the data cannot yield the information required to create a counterfeit magnetic stripe or chip card. Issuers enjoy increased security due to dynamic authentication. Both merchants and issuers can make authorization decisions with more confidence.

2.3.2 Mobile Transaction Capability

Consumers are increasingly using their mobile devices to pay. According to Starbucks, 10 million customers actively use the Starbucks mobile payments app, and the number of mobile transactions in their stores is approaching 5 million each week.[10]

[10] Starbucks' CEO Discusses F1Q 2014 Results - Earnings Call Transcript, January 23, 2014, http://finance.yahoo.com/news/starbucks-ceo-discusses-f1q-2014-031803145.html.

Deploying the EMV infrastructure for both contact and contactless payments will help build the framework for secure mobile payments. Using a Near Field Communication (NFC)-enabled mobile device with an EMV-compliant contactless payment application will provide strong authentication at the POS. The dynamic nature of the EMV authorization request cryptogram protects contactless mobile transactions in the same way it secures a contact or contactless EMV transaction originating from a payment card.

2.3.3 Global Interoperability

Standards for smart card technology are rooted in global standards that are historically interoperable and appropriate for current security requirements. In addition to being interoperable, smart card technology leverages advances in semiconductor design and miniaturization, increasing computational efficiency and complexity, to keep pace with the need for enhanced semiconductor security features to address security threats.

Deploying EMV in the U.S. will bring the United States in line with how the rest of the world processes payment card transactions. U.S. issuers who issue EMV chip cards provide their cardholders with greater convenience and less friction at the POS when they travel internationally. The stronger authentication by using the EMV cryptogram allows U.S. issuers to confidently authorize EMV transactions made using EMV chip cards and approve more cross-border transactions, reducing the impact on traveling cardholders. This should help minimize cardholder attrition.

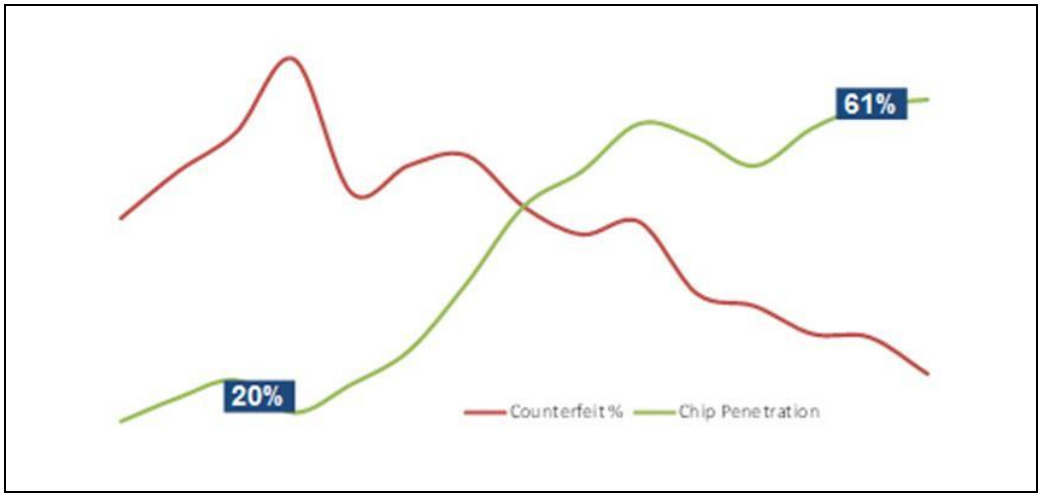
While the core EMV specification is over 20 years old, it is continuously updated to counter new security threats and provides a proven global platform for secure payment card transactions well into the future. Moreover, integrated circuit technology is enhanced annually incorporating new security features that further protect the future of the EMV security architecture.

2.4 Value to Issuers

Issuers in the U.S. have traditionally enjoyed the security benefits of a zero floor-limit, always-online transaction environment, which drove counterfeit payment card fraud to less sophisticated markets. However, with most of the rest of the world's payment infrastructure now EMV chip-enabled, the U.S. is beginning to see an increase in counterfeit fraud, as fraudsters target the weaker U.S. infrastructure.

2.4.1 Fraud Protection

Brazil's rollout of EMV chip cards illustrates the impact on fraud of adopting EMV (Figure 2).



Source: Visa HRFA Fraud Reports & Operating Certificates (as of September 2010), Card Sales Volume for all products (excluding cash).

Figure 2. Counterfeit Fraud and Chip Card Volume in Brazil

Issuers who rely on EMV's dynamic authentication cryptograms rather than static magnetic stripe data can modify their authorization systems to approve more transactions. For example, in a study carried out between May 2009 and April 2010, Brazilian issuers realized an 8 percent higher domestic authorization approval rate for chip cards as opposed to magnetic stripe cards and a 14 percent higher authorization approval rate for cross-border transactions using chip cards.[11]

U.S. issuers can feel more confident in their authorization decisions when processing an EMV transaction as opposed to a magnetic stripe transaction. Suppose a fraudster copies the data from the magnetic stripe of an EMV chip card and encodes this data onto the magnetic stripe of a counterfeit card. The card service code will indicate that the data originated from a chip card. If a fraudster tries to use the counterfeit card at the POS, the transaction will not be accepted at a chip-enabled terminal. Instead, the terminal forces the transaction to use the chip in the card. If the chip cannot be read for some reason (such as there being no chip on the counterfeit card), the merchant may refuse to accept the card or the transaction will be sent to the issuer as a "fallback" transaction. The issuer can make an authorization decision knowing that there is additional risk and that what appears to be that issuer's chip card cannot be read by a chip reader. If a fraudster alters the service code to hide the fact that the data came from a chip card, the card security code would fail validation during the online authorization process and the transaction would be declined. However, if magnetic stripe data is copied from a chip card and is used at a non-chip enabled terminal, the service code is ignored. The transaction may be approved, and, after October 2015, the issuer will have the right to charge this transaction back to the acquirer as counterfeit fraud. These are the transactions covered by the EMV liability shift.

2.4.2 Other Benefits of EMV Adoption

U.S. issuers who issue EMV chip cards benefit from the use of stronger, dynamic authentication for face-to-face POS transactions, leading to more approvals and greater revenue. This stronger authentication has the following advantages:

- Proves the transaction came from an authentic form factor (card or smartphone)
- Proves the integrity of the transaction
- Creates transaction data that cannot be replayed without detection by the issuer

The use of EMV chip cards to reduce counterfeit card fraud may also reduce the number of cards that must be reissued (and the associated expense) due to fraud.

Counterfeit fraud has always moved to the weakest link in the payments infrastructure chain. Full implementation of EMV chip technology in the U.S. will substantially reduce global counterfeit payment card fraud.

2.5 Value to Merchants

As highlighted by the data breaches in late 2013 and 2014, merchants have a lot to lose from fraud. U.S. merchants can mitigate much of the risk of processing face-to-face transaction data by migrating to EMV.

The current static magnetic stripe transaction data elements can be copied and used to generate other payment transactions. The dynamic cryptogram used in EMV transactions cannot be used to counterfeit a card. A fraudster who is able to breach a merchant's data security infrastructure and steal EMV transaction data cannot reuse the data fraudulently in the card-present environment, because a new and unique cryptogram value is generated for each transaction. As a result, any data that is stolen is significantly devalued and cannot be used to create counterfeit magnetic stripe cards.

[11] Visa Vue Online (VVO) transactional analysis & Visa Quarterly Operating Certificates (as of April 2010)

In addition, as noted in Section 2.4.1, if a fraudster creates a counterfeit magnetic stripe card using EMV transaction data and alters the service code to hide the fact that the data was from an EMV transaction, the card security code will fail validation during the online authorization process, and the transaction can be declined.

There are other merchant advantages to adopting EMV. U.S. merchants who update their POS systems to accept contact and contactless chip transactions can qualify for Payment Card Industry (PCI) audit relief and MasterCard Account Data Compromise relief. All global payment brands support PCI audit relief for merchants processing a significant percentage of their transactions using fully enabled dual-interface terminals, to help offset the costs of investing in EMV technology. Merchants who qualify can waive their obligation to complete an annual PCI Data Security Standard (DSS) validation assessment but will still need to comply with the PCI DSS requirements. The elimination of this requirement could represent a significant cost reduction for participating merchants.

Qualifying merchants who achieve EMV transaction processing milestones will also be relieved of some or all of the MasterCard penalties[12] for account data compromise.

In addition, by updating POS systems to process online contact and contactless EMV chip transactions, merchants are making the necessary changes to build an infrastructure that will support emerging payment innovations (such as secure mobile face-to-face transactions).

[12] Excluding any judicial or regulatory penalties, if applicable.

3 Transaction Data Encryption

Encrypting transaction data (both cardholder data and other data describing a transaction) can prevent intermediaries, such as hackers, Internet providers, or application service providers, from discovering or tampering with the data. Two approaches to encryption are commonly used to provide such protection: end-to-end encryption (E2EE) and point-to-point encryption (P2PE). In a P2PE solution, the data is decrypted at each stop (e.g., merchant to processor, processor to issuer, issuer to merchant). In an E2EE solution, the cardholder data is encrypted at the point of entry and decrypted only at the intended recipient end. Both methods require an originating party to encrypt data so that it is readable only by the intended recipient. Both methods can simplify PCI compliance requirements for a merchant.

Figure 3 divides the process of encryption, transfer, decryption and storage into zones. Reviewing the overall process, cardholder data is encrypted as soon as it enters a payment system at the POS terminal or PIN pad; the data remain encrypted until it reaches the processor or acquirer, where it can be decrypted safely and securely, with no involvement of third parties or the merchant in the encryption or decryption process. Using P2PE, cardholder data is encrypted at the point of acceptance; the data is decrypted by the provider, who can be a gateway provider, acquirer, processor, or independent sales organization (ISO). In both cases, the payment processor is responsible for managing the cryptographic keys, as the merchant never has access to the keys or the raw cardholder data. All involved in authorizing and settling the transaction, regardless of whether speaking of E2EE or P2PE, are responsible for PCI compliance. In summary, P2PE and E2EE protect data confidentiality and integrity.

3.1 Value to Merchants

Transaction data encryption offers the following value to merchants:

- Encrypts the PAN and/or transaction, thus eliminating the opportunity for monetization of the card data.
- Eliminates the risk of monetization of stolen card data. Criminals cannot monetize data that they cannot decrypt.
- Responds to the admonition of ongoing issue of network compromises that "all organizations should assume they've been hacked."[13]
- Reduces a merchant's PCI DSS compliance scope.[14]

Figure 3 provides a picture of the flow of a transaction that has been encrypted as noted in zones. In Zone 1 the cardholder data is encrypted at inception – swipe, key, tap or insert. The transaction and encrypted cardholder data passes into Zone 2 which can be a gateway or a network. In Zone 3, the transaction is passed to the acquirer or processor for authorization by way of the card brands. Lastly and in Zone 4, the PAN is stored securely within the processor or acquirer's PCI certified data center.

[13] Cisco Systems, Inc., *Cisco 2014 Annual Security Report*, https://www.cisco.com/web/offer/gist_ty2_asset/Cisco_2014_ASR.pdf.

[14] Coalfire, *Heartland Payment Systems E3™ MSR Wedge Technical Assessment White Paper*, Jan. 4, 2011, http://www.heartlandpaymentsystems.com/Heartland/files/70/70ce486a-ca66-4c8f-9098-463900ac2c6b.pdf.

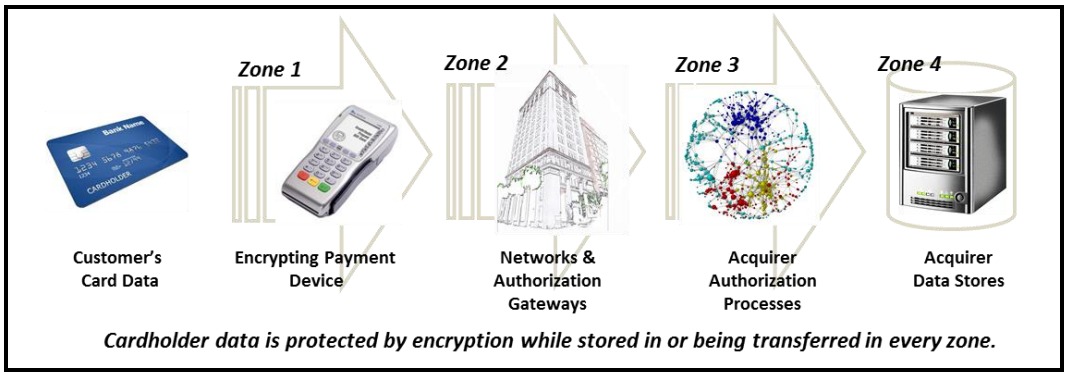


Figure 3. End-to-End Encryption

Figure 4 lists some of the ways in which payment providers have implemented E2EE for use by merchants.

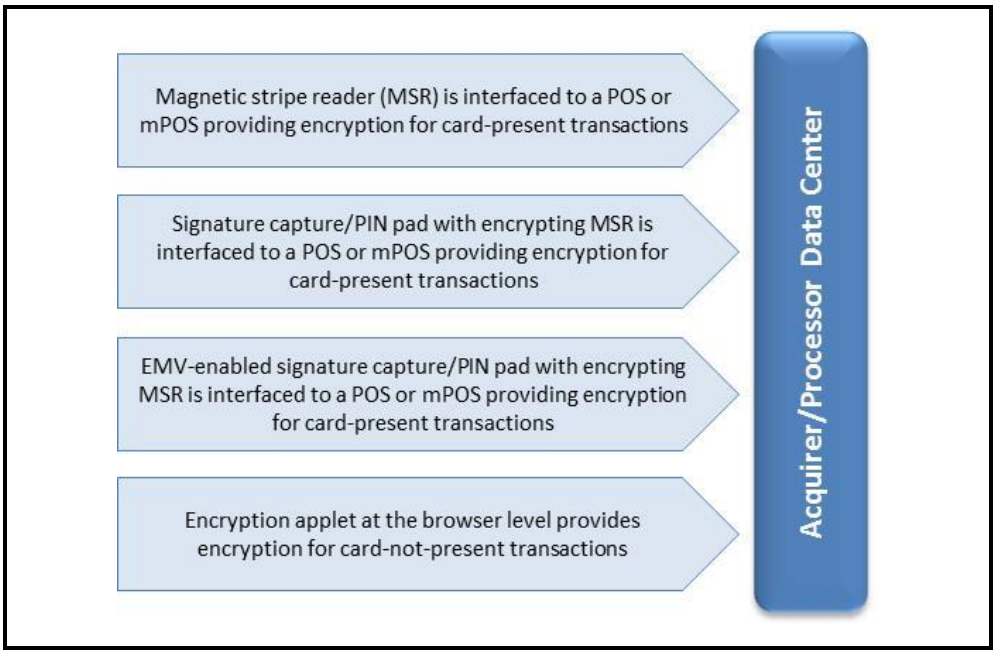


Figure 4. Examples of E2EE Implementation for Use by Merchants

The first three implementations listed in Figure 4 encrypt cardholder data within a tamper-resistant security module for optimal protection. Certain implementations of mobile-enabled encrypting readers (dongles) do not provide hardware protection for the encryption process or protect encryption keys. However, dongles can still encrypt cardholder data and contribute to a safer acceptance ecosystem.

The final implementation example, software-based encryption, does not provide hardware protection for the encryption applet or the keys used for encryption. However, this implementation can still contribute to a safer payment ecosystem.

3.2 Differences among Solution Offerings

It can be argued that no payment solution is truly an end-to-end solution unless the transaction is encrypted at the point of interaction and remains encrypted until it reaches the issuer. However, the solution provider's perspective can influence whether that provider characterizes the solution as an E2EE or a P2PE solution. A gateway provider may present an encryption solution as E2EE because it encrypts data at the point of interaction and decrypts data at the provider's PCI-compliant data center. An acquirer would not consider that

implementation to be E2EE but rather P2PE, since it decrypts the PAN and discretionary data before they are received by the acquirer or processor for authorization. An issuer may believe that the PAN and discretionary data should be encrypted at the point of interaction and not be decrypted until they reach the issuer.

A true E2EE solution is not possible. The PAN and discretionary data must be decrypted at some point to be routed to the correct payment network and issuer. The most likely provider of an E2EE solution may therefore be an acquirer or processor, who represents payment brands to the merchant and interfaces directly with the payment networks. A gateway provider or independent sales organization (ISO) that provides a service that encrypts at the point of interaction must decrypt the cardholder information at the ISO's data center before sending the data to the acquirer or processor for authorization. This breaks the encryption chain and may be considered a P2PE offering since the gateway or ISO is not the acquirer or processor. Decrypting data before authorization may risk exposing the data to crimeware in the gateway provider's or ISO's system. There is also risk wherever card data is decrypted – at the acquirer or processor, payment brand networks, or issuer systems.

Table 1 describes three types of encryption that are used by ISOs, acquirers, and processors to assist merchants in protecting cardholder data.

Table 1. Example Encryption Solutions

Encryption Type	Description
Identity-Based Encryption	Identity-based encryption (IBE) is an encryption process that can be initiated by a sender using a unique identifier such as the recipient's e-mail address to calculate a public key. A trusted third-party server, called the private-key generator, uses a cryptographic algorithm to calculate the corresponding private key from the public key. The benefit of IBE is that senders can easily generate the public key of the recipient. When the recipient needs to acquire their private key, they simply send a request to the private-key generator. The key advantage is that no one has to worry about distributing their public key, allowing anyone to encrypt data and securely send it or sign data to assure authenticity. Encryption techniques have relied on randomly generated keys that are mapped to identities called digital certificates. The management of these certificates and the need to procure a certificate before encrypting a message or record has made encryption using traditional approaches very difficult for end users, costly to operate, and complex for IT operations. IBE can use any arbitrary string as a public key, enabling the PAN or a transaction to be protected without the need for certificates. In a payments scenario, the PAN and discretionary data found on the card are encrypted immediately after the data is acquired using the public key thus negating the need for tamper-resistant hardware. IBE supports magnetic stripe and contactless and contact chip cards. IBE uses any number of public key encryption algorithms offering a variety of levels of security.
Symmetric Key Encryption	In symmetric key encryption, each computer has a secret key that it can use to encrypt a packet of information before it is sent over the network to another computer. Symmetric key encryption requires that you know which computers will be talking to each other so you can install the key on each one. The key provides the key to decoding the message. With symmetric key encryption as used in payments, the PAN and discretionary data are encrypted when read by tamper-resistant hardware. Symmetric key encryption supports magnetic stripe and contactless and contact chip cards. It uses 128-bit TDES or AES format-preserving symmetric key encryption.
Asymmetric Key Encryption	Asymmetric encryption is a form of encryption where keys come in pairs. What one key encrypts, only the other can decrypt. Frequently, but not necessarily, the keys are interchangeable in the sense that if key A encrypts a message then key B can decrypt it, and if key B encrypts a message then key A can decrypt it. While asymmetric key encryption supports magnetic stripe and contactless and contact chip cards, it is typically used for card-not-present transaction encryption when referenced in terms of payment. Asymmetric key encryption is used to encrypt data (e.g., Track 1 and Track 2) as well as the transaction.

Identity-based encryption and symmetric key encryption combine hardware protection with software encryption at the point of interaction to encrypt the PAN, regardless of how data are entered—by swipe, tap, insertion, or key entry. For other payment use cases, asymmetric key encryption does not require hardware protection but does encrypt at data entry. Asymmetric key encryption is typically used on card-not-present or non-face-to-face transactions.

3.3 Implications of Encryption for PCI DSS Compliance Requirements

PCI DSS compliance applies to any merchant who stores, processes, or transmits payment card data anywhere within the merchant's business. Any system that transmits, processes, or stores encrypted PANs falls within the scope of the PCI DSS, especially if the organization has the ability to decrypt the data.

Many merchants focus on minimizing the number of systems that require compliance with PCI DSS or that are subject to compliance, thus reducing the scope of PCI DSS compliance. The PCI Security Standards Council (PCI SSC) has provided the following guidance:

- The presence or absence of the PAN determines whether a system is in scope for PCI compliance.
- An encrypted PAN is still defined as cardholder data, because it is theoretically possible to decrypt and thus recover the PAN. Therefore, any system transmitting, processing, or storing encrypted PANs are still considered in scope for PCI DSS compliance, but if an entity (such as a merchant) has no ability to decrypt encrypted data, then the encrypted data is not card data, and therefore systems that transmit, process, and store this data are not in scope.

Even the best encryption solutions do not completely reduce the need for PCI compliance. Certain controls will always have to be validated and measures taken. Table 2 describes the extent to which E2EE and P2PE can reduce a merchant's scope of PCI DSS compliance.[15]

Table 2. Effect of E2EE and P2PE on Merchant PCI DSS Compliance Scope

PCI DSS Requirement	Scope Reduction
Install and maintain a firewall configuration to protect cardholder data.	Minor
Do not use vendor-supplied defaults for system passwords and other security parameters.	Moderate
Protect stored cardholder data.	Major
Encrypt transmission of cardholder and sensitive information across public networks.	Major
Use and regularly update anti-virus software.	Minor
Develop and maintain secure systems and applications.	Moderate
Assign a unique ID to each person with computer access.	Major
Restrict access to cardholder data by business need-to-know.	Major

[15] Ibid.

PCI DSS Requirement	Scope Reduction
Restrict physical access to cardholder data.	Major
Track and monitor all access to network resources and cardholder data.	Moderate
Regularly test security systems and processes.	Moderate
Maintain a policy that addresses information security for employees and contractors.	Minor

While encryption reduces the scope of a merchant's PCI DSS compliance requirements, merchants must ensure that the encryption environment is properly segregated from other payment channels, such as e-commerce. Even when encryption is implemented, a number of components within the merchant's cardholder data ecosystem must still be evaluated against the PCI DSS requirements to keep the merchant's system secure and to maintain PCI compliance. Encryption also provides additional value to merchants by reducing the opportunity for stolen card data to be monetized.

3.4 Implementation Considerations

Today's merchants want to transact with customers across a wide range shopping channels that include traditional POS, mobile, online, telephone, and others. To accomplish this, merchants need to accept payments through tablets, smartphones, kiosks, and self-service terminals. Many of these platforms are "off the shelf" consumer devices and are susceptible to malware and crimeware. Without the means of reducing the risk of compromise, use of these platforms is risky. Both P2PE and E2EE, by way of encryption at time of swipe, tap or card insertion, can contribute to a merchant's efforts to secure their payments infrastructure while enabling the diverse ways a merchant can accept a consumer's payment

Implementing E2EE or P2PE can require investment in upgrades to POS hardware and software that incur vendor fees. The implementation process itself can be complicated, especially the device management process. In accordance with P2PE, tracking and protecting devices effectively can be cumbersome. But, while the investment in P2PE and E2EE may not show a verifiable return initially, knowing that a merchant has implemented a secure payment ecosystem that goes beyond PCI DSS will reduce or eliminate their chance of being hacked and the significant penalties that are assessed.

3.5 Summary

Encryption of transaction data enables a merchant to go beyond what is required by PCI to protect their business – financially and reputation-wise. Encryption works to make magnetic stripe, EMV and non-face-to-face transactions more secure by taking away the ability for crimeware to collect and hackers to monetize cardholder data. Hackers and criminals cannot sell what they cannot decrypt. As described above, while there are different means and methods of encryption available, it is recommended that a merchant work closely with their acquirer, processor or ISO to select the encryption methodology and solutions best suited for different requirements. As stated earlier, P2PE and E2EE protect data confidentiality and integrity.

4 Tokenization

Tokenization is a process that replaces a high-value credential (e.g., a payment card primary account number (PAN), a Social Security number) with a surrogate value that is used in transactions in place of that credential. Tokenization can map the credential to a new value that is in a different format or that is similar to the format of the original high-value credential (e.g., a payment card PAN in the payments industry). In payments, the objective of tokenization is to remove account data from the payment environment and replace it with something that is useless outside of the environment in which the token was created. While tokenization is not a new concept, recent data breaches have increased awareness of the need to protect payment account credentials. Tokenization is one approach that can be used to safeguard payment credentials from being stolen and used for fraudulent transactions. Merchants using tokenization may be able to reduce the scope of a PCI DSS assessment.

There are different kinds of tokens and different ways to create them. A token can be merchant specific. It can be single use or multi-use. It can be stored and managed in the cloud, in a token vault, or at a merchant location. A token is created using a process defined by the token solution provider. Once a token has been created, it may be tied to a card on file, individual transaction, payment card, or device.

Two types of tokens are being used and/or defined in the payments industry:[16] tokens that will function in place of the actual payment account number to perform a payment transaction;[17] tokens that replace the payment account number and are stored by merchants and/or acquirers in place of actual account numbers and used for other uses.[18] The tokenization creation and management process, use of tokens in a payment transaction, and business relationships differ based on the type of credential.

Various proprietary tokenization solutions are commercially available and already used by merchants and acquirers to protect cardholder data in both card-present and card-not-present (CNP) environments. New tokenization standards are also being introduced.

4.1 Standards and Specifications

Industry bodies such as the American National Standards Institute (ANSI) Accredited Standards Committee (ASC) X9, EMVCo, PCI Security Standards Council (PCI SSC), and The Clearing House have started to develop tokenization specifications for bank card payment industry use. In addition, the National Institute of Standards and Technology (NIST) has developed standards for an approach similar to tokenization for identity credentials that also includes consideration of levels of assurance.

4.1.1 ANSI ASC X9[19]

The X9 F6 work group is working on a security tokenization standard that addresses tokens used after initial payment authorization, such as when an acquirer provides tokenization services to merchants. The merchant securely sends payment authorization requests to the acquirer, which replaces the payment card number with a token. This token is returned to the merchant and stored in place of the payment card number. The acquirer keeps a record of the PAN-token pairing for situations where the PAN is required such as for settlement or disputed charges. This token has no use other than to replace the payment card number in the merchant data

[16] Tokenization specifications are currently being defined by the industry, with different names for the types of tokens being proposed.

[17] An example of this type of token is discussed in Section 4.1.2.

[18] Examples of this type of token are discussed in Sections 4.1.1 and 4.1.3. These types of tokens are also being referred to as "security tokens" or "acquirer tokens."

[19] This section is based on content provided by ASC X9. Information on X9 can be found at http://www.x9.org.

repositories. If the underlying payment card number is needed, an authorized request containing the token must be sent to the tokenization service (i.e., the acquirer).

X9 F6 defines tokenization as the act of generating and mapping a token to an underlying sensitive value (USV), such as a payment card number, using a centralized service that protects the core tokenization mechanism while still making it available to authorized entities.

Figure 5 illustrates the X9 F6 model for the tokenization process.

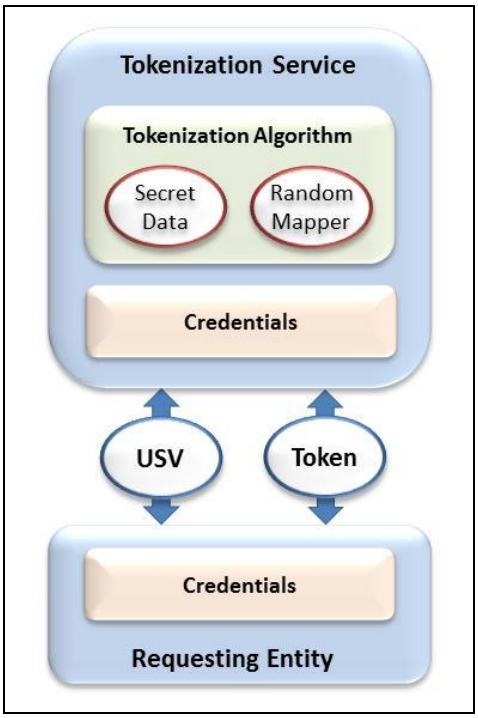


Figure 5. ANSI X9 F6 Tokenization Process Model

X9 F6 is working on the requirements[20] for secure design and implementation of this security tokenization process, including:

- A list of acceptable algorithms to implement the random mapping of USVs to tokens and the required strength of those algorithms
- Requirements for the protection of the tokenization service
- Requirements for tokenization service access control

X9F6 is currently working on a security tokenization standard named X9.119 Part 2 which is scheduled for release the first part of 2015.

[20] X9 F6 is still in the process of developing this standard and would welcome the contributions of anyone willing to join X9 and participate. Those interested in joining X9 should contact Janet Busch at janet.busch@x9.org.

4.1.2 EMVCo

In March 2014, EMVCo published version 1.0 of its tokenization specification[21] for payment industry participants.[22] This specification defines a framework to be used by payment brands, payment issuers, acquirers, merchants, and mobile and digital commerce solution providers to enhance transaction security at various points in the payment process. Various entities are creating token services based on the EMVCo specification.

EMVCo tokenization was designed to use current ISO/IEC 8583 message formats that support interoperability with the existing payments infrastructure; the specification adds additional values which may be mapped to existing fields. EMVCo's tokenization approach is intended to guard against fraud in current CNP channels, such as online account-on-file transactions. Tokens based on the EMVCo specification (referred to "EMV tokens") can also be used in the card-present channel with EMV chip cards, where a token replaces the PAN that would otherwise be encoded on the chip, while the magnetic stripe and embossing/printing on the card would contain the PAN.[23] Lastly, EMV tokens can be accepted in emerging mobile channels whether they are using QR codes, Near Field Communication (NFC), Bluetooth low energy (BLE) or a range of other future possibilities.

The intent of the EMVCo tokenization model is to limit risk levels in case of a data breach, and within specific defined domains (e.g., by a specific online merchant or a particular device in a specific acceptance channel). Additionally EMV tokens have an associated token assurance level which is determined by the identification and verification process performed at the time of token issuance. EMV tokens are designed to be interoperable between payment networks. Tokenized payment data is far less attractive to attackers and may eventually reduce data protection requirements for merchants and acquirers.

The EMVCo tokenization model introduces a new entity, called a token service provider (TSP). The TSP creates tokens and manages them throughout their life cycle. Token life-cycle management can be implemented using a method such as ISO/IEC 8583 message exchange, batch files, or Web services that are established for secure token-based interactions. The TSP is responsible for managing a registry of entities that can request tokens, a token provisioning system, token security, token vaults (to secure tokens and PAN mappings), APIs, and detokenization. The APIs allow participants to interact with the TSP.

In the EMVCo tokenization model, the token, referred to as a payment token, shares the same overt characteristics of a PAN (including the Luhn check mechanism, bank identification number (BIN) range, and expiration date) to support the current transaction flow and minimize friction in the existing payment processing environment. However, tokens are required to be guaranteed to never collide with PANs. In practice this means that tokens must be issued from separately designated BINs (or ranges within a BIN).

Once a token requestor has enrolled with a TSP and identified the domain in which its tokens may be used, the token issuance process starts with a request to a TSP, using a token service API, to tokenize a specific PAN. The token requester can be a merchant, a digital or mobile wallet service provider, a card-on-file system, an issuer, or any other payment enabler. The token is generated within a range of token BINs that are associated with a specific issuer to avoid conflicts with a PAN, and is assigned to a domain within which it can operate. (For example, a token issued for an NFC payment domain will not work in an e-commerce or magnetic stripe environment.)

A two-digit token assurance level, similar to a payment instrument risk score, is also assigned to indicate what identification and verification (ID&V) process was done to validate the cardholder's identity and ownership of the original payment credential; a value of 00 would indicate no ID&V and 99 would indicate the highest level of

---

[21] EMVCo, *EMV Payment Tokenisation Specification – Technical Framework*, Version 1.0, March 2014, http://www.emvco.com/specifications.aspx?id=263.

[22] The EMVCo specification defines "payment tokens" or "EMV tokens" that will function in place of the actual payment account number to perform a payment transaction.

[23] EMVCo, *EMV Payment Tokenisation Specification – Technical Framework*, Version 1.0, March 2014, p. 69.

assurance. The token assurance level can be used by specific programs or for transaction classification and can be influenced by the security requirements for token storage location. ID&V methods can be used for different purposes such as card-on-file account number replacement with a token, or medium or higher assurance level transactions. ID&V methods generally fall into the following categories:

- No ID&V performed
- Account verification
- Risk score derived from the TSP
- Risk score derived from token user data combined with payment network data
- Card issuer authentication of cardholder

Detokenization is the reverse of tokenization and is necessary for transaction processing, settlement and chargebacks. When requested by an authorized and authenticated entity, the detokenization process returns the PAN associated with a token, the associated expiration date, and status. Depending on where the TSP is located in the transaction flow, it may perform the token domain restriction controls directly or provide the transaction processor with the details needed for it to, in turn, perform that task.

The BIN plays an important role in routing transactions to the right endpoint. The BIN token range used in transactions will have similar characteristics to the BIN range for the cards and will be part of the BIN routing table distributed to participating entities to support routing of tokenized transactions.

Payment tokens have life cycles similar to PAN life cycles. While payment tokens experience their own life cycle events (such as expiration, fraud, loss, transfer of devices, reissuance, theft, changes due to customer profile updates), they may also be affected by changes to the PAN life cycle. The TSP is responsible for communicating changes to the token (or to the PAN associated with the token) to token users in the payments transaction process.

4.1.2.1 TRANSACTION PROCESSING

Tokenized payment transaction processing passes the token instead of the PAN, so it becomes the responsibility of the TSP and the payment processing platforms to restrict a particular token to specific payment channels or domains. This restriction will affect the current data fields and require the definition of both mandatory and optional new fields that have been defined for tokenized transactions. Some of the fields required to control domain restriction are already in place, such as POS Entry Mode, and merchant detail fields. New field use may depend on the specific payment use case, in which merchants, acquirers, and processing platforms may be affected by such use cases.

4.1.2.2 NFC MOBILE PAYMENT TRANSACTION USE CASE EXAMPLE

Figure 6 illustrates the possible use of EMVCo tokenization in an NFC mobile payment transaction. Tokenization is likely to be used in NFC mobile payment implementations using either secure elements (SE)[24] or host card emulation (HCE).[25]

[24] "Apple Announces Apple Pay," Apple press release, Sept. 9, 2014, https://www.apple.com/pr/library/2014/09/09Apple-Announces-Apple-Pay.html

[25] Additional information on NFC mobile payment using secure elements or HCE can be found in the Smart Card Alliance white paper, "Host Card Emulation (HCE) 101," http://www.smartcardalliance.org/publications-host-card-emulation-101/.

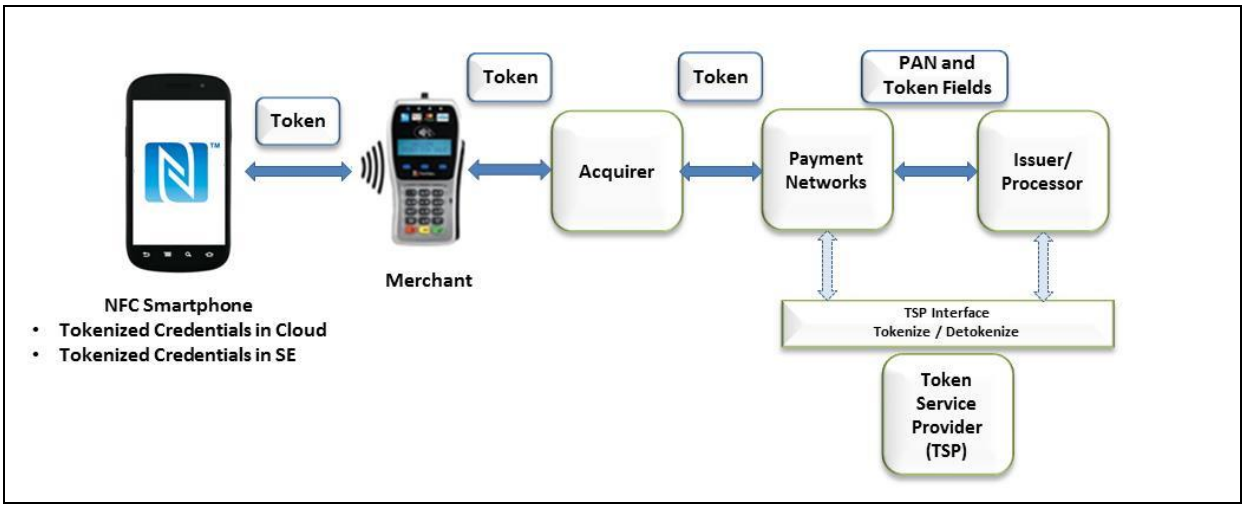


Figure 6. Use of Tokenization in an NFC Transaction

4.1.3 PCI Tokenization Initiative[26]

The PCI SSC is currently developing security requirements for tokenization products (e.g., tokenization applications or appliances) that replace a PAN with a token. The tokenization processes described by PCI include functionality to exchange a token back to the original PAN ("detokenization") as well as "irreversible" tokens for which there is no mechanism supported to reproduce the PAN. The goal of this effort is to remove the need to store PANs, thereby reducing the risk of unauthorized disclosure, and is focused on tokens used in the acquiring environment.

It is anticipated that use of secure tokenization products will help to minimize the locations, systems and networks where cardholder data is stored, processed or transmitted. A secure tokenization implementation may help minimize the retention of payment card data in an entity's environment and hence simplify their PCI DSS compliance efforts. These tokenization security requirements are part of the Council's ongoing work to provide standards and guidance on technologies that can improve cardholder data security along the payment transaction chain.

The PCI effort will provide tokenization product vendors and developers with detailed technical requirements for how to generate and store tokens securely. A mechanism to evaluate tokenization products against the requirements is under consideration.

PCI security requirements are developed with the input of the PCI community of participating organization members, security assessors, testing laboratories and other key stakeholders. In addition, PCI SSC has held conceptual and technical discussions with a number of organizations that already offer tokenization products or services. PCI SSC also liaises with X9 and EMVCo on their respective tokenization efforts.

PCI SSC anticipates publication of security requirements later in 2014. For more information, contact tokenization@pcisecuritystandards.org.

[26] Section 4.1.3was contributed by the PCI Security Standards Council. Additional information on PCI SSC can be found at https://www.pcisecuritystandards.org/.

4.1.4 The Clearing House Tokenization Initiative[27]

As a member organization of 23 commercial banks, The Clearing House (TCH) operates under a directive to both assist in the development of tokenization standards, as well as operates a multi-issuer token vault that works across all major card networks. The Secure Token Exchange effort began in 2012, was piloted in 2013, and now has participating banks that represent 70% of U.S. retail card volumes. In addition to card volumes, the Secure Token Exchange will also support the future tokenization of Automated Clearing House (ACH)/demand deposit account (DDA) payments.

The initial Secure Token Exchange standards were very similar to the EMVCo standards published in March 2014. The Clearing House is adopting the core EMVCo messages to allow for industry interoperability while retaining proprietary provisioning, exceptions and lifecycle management flows. The Clearing House has also proposed several changes to the current EMVCo specifications to include these flows and to increase the overall safety and soundness of the framework. It is the position of U.S. banks that greater standardization of tokenization specifications will allow for faster adoption and innovation.

4.2 Assurance Process for Token Issuance

In many token use cases, the sole purpose of the token is to remove sensitive card data from the payments ecosystem. In such cases, there is little need to validate that a given PAN is authorized prior to tokenizing it. The payment system will perform that function during transaction processing. However, in some instances, principally when the token replaces a PAN for use in an NFC transaction or similar situations, simply replacing the PAN with a token doesn't address the risk of a criminal using stolen payment credentials and having a valid token assigned to the stolen credential.

To address this, critical parts of the tokenization process are to identify and verify that the cardholder presenting the payment account for tokenization is the valid cardholder and to associate an assurance level to each token to indicate the confidence level in the token to PAN/cardholder binding.

As discussed in Section 4.1.2, the EMVCo tokenization specification refers to several possible ID&V methods that may be performed via card issuer verification of the cardholder. The ID&V methods are utilized to assign an assurance level to each token that will be used to transact. ID&V processes are critical to tokenization initiatives to prevent fraudulent use of payment card data.[28]

4.3 Summary

Commercial acquiring tokenization solutions are currently available and in use by merchants to remove cardholder data from their business environment (e.g., for loyalty programs or card-on-file transactions).

Tokenization standards are also now being developed and published by a number of industry organizations, with commercial solutions starting to use those specifications to provide tokenization services. Some standardization efforts are focused on card-present merchants to remove cardholder data from the business environment, while others are focused on e-commerce and mobile transactions.

---

[27] Section 4.1.4 was developed with contributions from The Clearing House. Additional information on the The Clearing House can be found at https://www.theclearinghouse.org/.

[28] Other industries have addressed credential assurance levels. For example, NIST has defined assurance level processes for the derived credential associated with the Federal government's Personal Identification Verification (PIV) card, allowing a credential to be used across multiple channels. For additional information see *Guidelines for Derived Personal Identity Verification (PIV) Credentials*, Draft NIST Special Publication 800-157, available at http://csrc.nist.gov/publications/PubsDrafts.html.

Tokenization standardization and broader implementation are evolving. The industry is starting to see alignment among the standardization efforts around the EMVCo tokenization specification. The EMVCo tokenization framework also references its use with EMV chip cards, combining the security benefits of EMV chip with tokenization. Acquirers will also continue to offer tokenization solutions to merchants that address specific merchant needs not otherwise addressed.

5 Payment System Security Layers

The payments industry can provide improved payments protection by using a layered approach. Implementing all three of the technologies described in previous sections and using them in combination can provide a better solution than using any single technology by itself.

To understand how EMV, encryption and tokenization work together to provide security for payment transactions, it is beneficial to understand the various use cases for customers presenting payment credentials at merchants. This section looks at several scenarios and provides guidance on how EMV, encryption and tokenization are used to provide payment transaction security.

Scenarios discussed include:

- Card-present transactions
- Card-not-present transactions
- Mobile transactions in a store with payment credentials stored in the cloud and transferred to the POS using one of multiple technologies

5.1 Card-Present Transactions

Card-present transactions include those where customers are in a merchant's store and are paying with a magnetic stripe card, an EMV chip card or an NFC-enabled mobile device with credentials stored on a secure element on the mobile device.

EMV was designed to combat counterfeit card fraud in a card-present environment. Key EMV security features include:

- Card authentication using dynamic authentication data (either online or offline), which proves that a card is authentic to the merchant and issuer.
- EMV chip transaction data, which cannot be used to create counterfeit magnetic stripe cards if the data is stolen.
- Potential PIN addition to an EMV transaction, providing stronger verification of the cardholder identity and addressing lost and stolen card fraud.

However, although EMV uses dynamic cryptograms, some sensitive data (such as the PAN and expiration date) that is needed to support routing and legacy system messaging, is sent in the clear during EMV transactions.

Encryption can protect transaction data at rest and in transit, whether it's a magnetic stripe transaction or an EMV chip transaction. A merchant deploying encryption without EMV will not be protected from counterfeit card transactions; EMV technology mitigates the risk of counterfeit transactions. The combination of EMV and encryption protects transactions in the card-present environment. This two-layered approach is a proactive step that merchants can take to protect their card acceptance environment from becoming a source of fraudulent transactions.

In addition, tokenization may be implemented in card-present merchant environments to secure data-at-rest for payment transactions. This will most typically be done in order to support the legitimate on-going uses of card data in an inherently secure manner. This is contrasted with encryption, where the encrypted data must typically be decrypted before it can be used. Whenever data is decrypted, it is at risk of being compromised, while tokens can be used without concern as long as the integrity of the token vault is maintained.

Use cases include the following:

- Some merchants use card information to simplify the return experience for the customers. When a consumer wishes to return an item, the merchant collects the card data, sends it to the token service to be tokenized, and then looks up the transactions in their transaction history.
- Lodging merchants may need to perform an EMV authorization upon check-in, but also perform incremental authorizations during the guest's stay. Instead of retaining the cardholder account number, the merchant may use a token specific to the merchant's use. The token vault in this case could be at a corporate host or at the acquirer/processor. Similar use cases exist for tokenization in auto rental, equipment rental and other merchant types where a deposit is taken in person, followed by a CNP balance payment.

EMV tokens can also be used in the card-present environment when they have been personalized into a mobile device or onto EMV chip cards. When the consumer is in the store and uses a device with credentials stored on a secure element and accessed through a mobile wallet (e.g., Softcard[29]) or on the EMV chip card, the transaction is a card-present transaction and is implemented as an EMV contactless or contact transaction. As with the other card-present use cases, EMV protects against counterfeit credentials and provides card authentication. The merchant may use encryption and/or tokenization to protect the transaction information while at rest or in transit. Alternatively, the issuer can personalize the chip with an EMV token in lieu of the PAN. This will protect all chip transactions from cross-channel fraud (e.g., CNP fraud) in addition to counterfeit fraud.

5.2 Card-Not-Present Transactions

CNP transactions are those where the customer and merchant are not interacting face-to-face. The customer may be entering payment credentials using a keyboard on a computer, tablet or mobile phone or may have previously provided the payment credentials to a merchant and the merchant uses the stored "card on file" credentials for payment (for individual or recurring payments).

Merchants and the payments industry currently take a variety of approaches to authenticate consumers during CNP transactions to help mitigate against CNP fraud. Approaches include static or random passwords, dynamic information such as one-time passwords generated in software or using a smart card or mobile phone, knowledge-based approaches (such as asking secret questions) and device fingerprinting, where some information is used to identify the device by which the user is accessing an e-commerce site.

The payments industry has implemented a number of standard approaches for CNP authentication. Asking for the cardholder's zip code for address verification and entering the "card security code" printed on the card are common methods used by many, but not all, merchants. Card issuers validate that this information is correct during the transaction authorization. The payments networks have also defined the standard 3D Secure authentication protocol that is in use. The 3D Secure software protocol is used by merchants and issuers to validate cardholder identity during an e-commerce transaction. Looking at Europe's experience, the UK Cards Association reported a one-third drop in CNP fraud since 2007 due to increasing use of fraud screening tools and 3D Secure.[30]

Online e-commerce merchants typically implement multiple solutions to mitigate CNP fraud or use a commercial service to mitigate transaction risk. Since merchants today assume the costs of CNP fraud as well as typically pay higher fees for e-commerce transactions, merchants also may have their own internal fraud departments and often use tools to score the risk of online shopping behavior to determine which online purchases to accept, reject or send for review.

---

[29] "A Message from CEO, Michael Abbott: Isis Wallet is Becoming Softcard," Isis press release, Sept. 3, 2014, http://news.paywithisis.com/2014/09/03/isis-wallet-becoming-softcard/.

[30] "Second Report on Card Fraud," European Central Bank, July, 2013, http://www.ecb.europa.eu/pub/pdf/other/cardfraudreport201307en.pdf; "Fraud the Facts 2012," Financial Fraud Action UK, http://www.theukcardsassociation.org.uk/wm_documents/Fraud_The_Facts_2012.pdf.

In the card-not-present environment, security approaches should consider:

- Some form of cardholder authentication, such as 3D Secure.
- Encryption to protect data-in-transit and data-at-rest.
- Tokenization to protect data, by creating a token for each CNP transaction that can only be used for that card and a specific merchant. This could be accomplished through either acquiring tokens or EMV tokens.

For example, e-commerce merchants can secure cardholder data by implementing the process for card-on-file tokens. The merchant, acting as a token requestor, can request tokens by submitting a token request to a token service provider. The token is provided to the card-on-file merchant. The token assigned is specific to the cardholder and merchant domain. If the token were to be compromised, it could not be used anywhere except by the registered user and at the registered card-on-file merchant.

5.3 Mobile Transactions with Credentials Stored in the Cloud

Mobile payment solutions that store payment credentials in the cloud but present them in a face-to-face merchant environment (e.g., those that use QR Codes, bar codes or Bluetooth) are now typically considered CNP transactions since the credentials are not authenticated during the transaction, even though the mobile device may be physically present at the POS.

The industry has launched a number of initiatives to develop network-based specifications for tokenized credentials that can be used for mobile commerce transactions (see Section 4). When these tokenized credentials are stored on the mobile device and used face-to-face for purchases at physical merchants (e.g., for host card emulation (HCE)-enabled or secure element (SE)-enabled NFC transactions), it is anticipated that these will be considered card-present transactions.

5.4 Summary and Best Practices

Using a layered approach – that is, utilizing all three technologies together –helps to secure the payments infrastructure and prevent payment fraud. Table 3 and Figure 7 illustrate how each is used to protect transactions.

Table 3. How EMV, Encryption, and Tokenization Protect Transactions

	Card-Present Transactions		Card-Not-Present Transactions	
	Protects against:	**Using:**	**Protects against:**	**Using:**
EMV	Counterfeit cards	Card authentication	Not applicable. Can be used with separate reader, but not widely deployed	Not applicable
	Re-using stolen data	Dynamic data		
	Lost/stolen cards (with PIN)	Cardholder verification (PIN)		
Encryption	Stealing data in transit	P2PE or E2EE	Stealing data in transit	P2PE or E2EE
	Stealing data at rest Re-using stolen encrypted data	Various methods of encryption	Stealing data at rest Re-using stolen encrypted data	Various methods Of encryption
Tokenization	Stealing data in transit Stealing data at rest Re-using stolen data	Specific-use or limited-use token replacement for payment card data[31]	Stealing data in transit Stealing data at rest Re-using stolen data	Specific-use or limited-use token replacement for payment card data

[31] Encryption is also used during the tokenization and de-tokenization process.

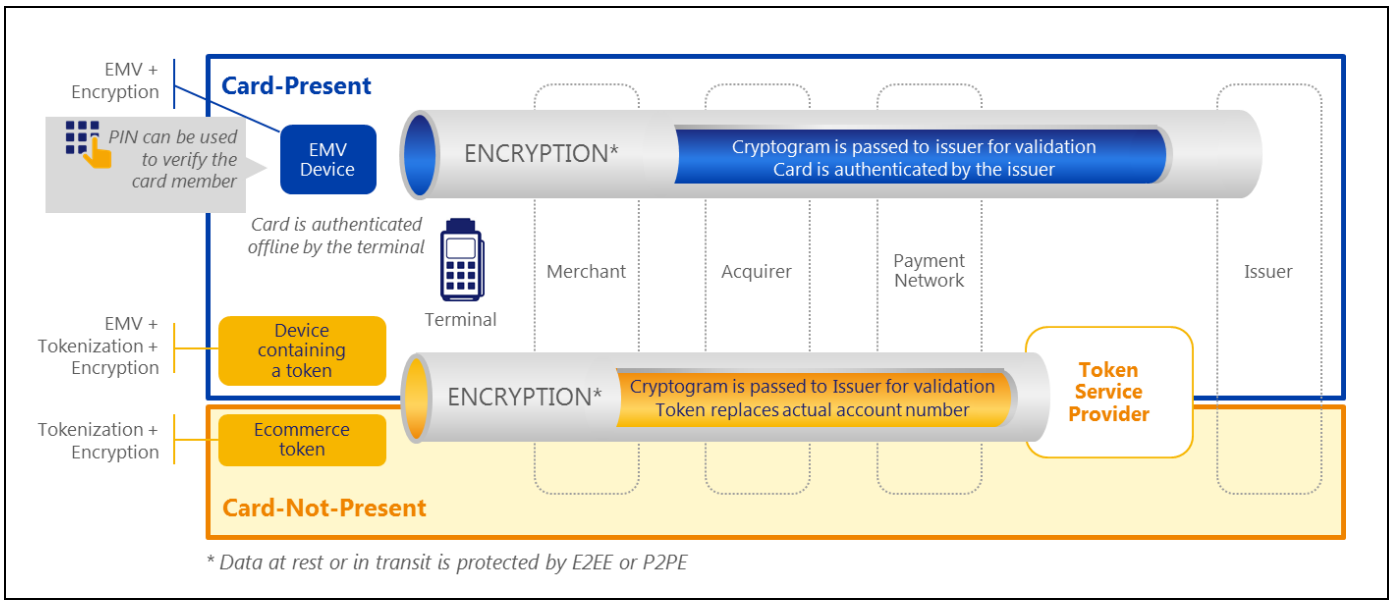


Figure 7: Role of EMV, Encryption and Tokenization in the Payment Ecosystem

The layered security approach is based on the following key guiding principles.

- Continued migration away from transactions based on static authentication by implementing EMV for the card-present environment.
- Protection of data-at-rest and data-in-transit through the payment process, for both card-present and card-not-present environments.
- Adoption of encryption and tokenization technologies to protect sensitive data, including PAN and expiration date, for both card-present and card-not-present environments.
- Adoption of cardholder authentication (e.g., 3D Secure) for the card-not-present environment.

No silver bullet is available to stop fraud. However, as summarized in Table 3 and Figure 7, a layered security strategy that includes EMV, tokenization, and encryption is the right approach for securing payment card transactions.

6 Conclusion

This white paper outlines the characteristics of three different technologies that are useful to securing payment transactions well into the future. Payments stakeholders seeking to reduce cost and complexity but facing limited budgets should optimize implementation based on the benefits of each technology.

EMV provides strong card authentication through the use of cryptograms to prevent counterfeit transactions. Encryption protects account numbers and other critical transaction elements that are sent through the payment system. Tokenization completes the protection of the payment card data by removing the PAN and expiration date from EMV chip, CNP and mobile transactions.

When layered, these three technologies secure the payments ecosystem. The degree of layering is determined by the need of each payments stakeholder.

Issuers are already moving to EMV to address counterfeit card fraud. Issuers now should consider support for tokenization to protect payment data received from EMV chip, CNP, and mobile channels.

Merchants should invest in the technologies that offer the protection they need. For example:

- A low-value-ticket card-present merchant may have very few chargebacks and may not be worried about counterfeit cards. The merchant will still have PCI and data-in-transit concerns, so their investment may focus on the encryption of data in transit and at rest.
- A high-value-ticket card-present merchant may be most concerned about counterfeit cards. The investment focus would be on EMV first and encryption of data in their network.
- A large e-commerce retailer's investment focus may be first on tokenization with cardholder authentication, and securing e-commerce transactions. Encryption of data on its way to the acquirer or processor would be another priority.
- Face-to-face merchants with complex environments that have a need to use card data for purposes in addition to authorization may wish to include an acquiring tokenization solution with encryption and EMV in order to ensure that they can securely replace sensitive card data throughout their systems as needed.

Payments stakeholders should give careful thought to their approach for layering the three technologies. The decision should be based on the needs of the particular entity, industry requirements and regulations, anticipated trends, and, of course, cost.

7 Publication Acknowledgements

This white paper was developed by the Smart Card Alliance Payments Council to describe the role of EMV, encryption and tokenization for securing the payments infrastructure and preventing payment fraud.

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 Payments Council members for their contributions. Participants involved in the development of this white paper included: Accenture; American Express; Bell ID;CH2M Hill; Chase Card Services; CPI Card Group; Datacard Group; First Data Corporation; Fiserv, Inc.; Gemalto; Giesecke & Devrient; Heartland Payment Systems; Ingenico; INSIDE Secure; MasterCard; NXP Semiconductors; Oberthur Technologies; SHAZAM; Tyfone; Valid USA; Vantiv; Visa, Inc.; Washington Metropolitan Area Transit Authority (WMATA); Wells Fargo.

The Smart Card Alliance thanks **Deana Cook**, Chase, **Mike English**, Heartland Payment Systems, **Siva Narendra**, Tyfone, and **Joe Scott**, Visa, who were the member project leads, and the Council members who participated in the project team to write the document, including:

- **Philip Andreae**, Oberthur Technologies
- **Louis Bianchin**, Valid USA
- **Greg Boardman**, Ingenico
- **Charl Botes**, MasterCard
- **Brent Bowen**, Valid USA
- **Myeong Choi**, Giesecke & Devrient
- **Deana Cook**, Chase Card Services
- **Jose Correa**, NXP Semiconductors
- **Brady Cullimore**, American Express
- **Michael English,** Heartland Payment Systems
- **Mike Esser**, Fiserv
- **Allen Friedman**, Ingenico
- **Simon Hurry**, Visa
- **Jack Jania**, Gemalto
- **Jeff Langus**, MasterCard
- **Christine Lopez**, Vantiv
- **Mark Lulic**, MasterCard
- **Cathy Medich**, Smart Card Alliance
- **Siva Narendra**, Tyfone
- **Manish Nathwani**, SHAZAM
- **Bruce Rutherford**, MasterCard
- **Joe Scott**, Visa
- **John Sheets**, Visa
- **Brian Stein**, CH2M Hill
- **Sree Swaminathan**, First Data
- **Drew Thomas**, Tyfone
- **Astrid Wang-Reboud**, Gemalto

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

- **Steve Arebalo**, INSIDE Secure
- **Greg Garback**, WMATA
- **Benoit Guez**, CPI Card Group
- **Michelle Lehouck**, Bell ID
- **Michael Simanek**, Accenture
- **Paul Simon**, Chase
- **Terry Strickland**, Wells Fargo
- **Sebastian Tormos**, Datacard Group

The Smart Card Alliance thanks **Steve Schmalz**, RSA, and **Steve Stevens**, X9; **Laura Johnson**, PCI SSC; and **David Fortney**, The Clearing House, for their contributions to the ASC X9, PCI and The Clearing House sections, respectively, and their review of the tokenization section; and **Brian Byrne**, EMVCo, for his review of the tokenization section.

Trademark Notice

Smart Card Alliance
Payments Council

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.

8 Glossary

Accredited Standards Committee (ASC) X9. The American National Standards Institute Standards Committee on Banking. The committee is composed of vendors, insurance companies, associations, retailers, regulators, and others in the financial services area.

AES. See **Advanced Encryption Standard.**

Advanced Encryption Standard (AES). Specification for the encryption of electronic data, established in 2001 by the U.S. National Institute of Standards and Technology (NIST). AES is based on a design principle known as a substitution-permutation network and operates quickly in both software and hardware.

Asymmetric key encryption. Encryption using two related keys – a key pair. The public key is freely available to anyone. A second key is kept secret (a private key). Any data that is encrypted using the public key can only be decrypted by applying the same algorithm using the private key member of the key pair. Any data that is encrypted using the private key can only be decrypted using the public key member of the key pair.

Bank Identification Number (BIN). First 6 digits of a credit or debit card number, assigned by a payment network to identify the card issuer.

BIN. See **Bank Identification Number**.

Bluetooth low energy (BLE). Wireless computer network technology designed and marketed by the Bluetooth Special Interest Group. Compared to classic Bluetooth, Bluetooth low energy is intended to provide considerably reduced power consumption and cost while maintaining a similar communication range.

CNP. See **Card-not-present transaction**.

Card-present transaction. Payment card transaction in which a bank card is physically present. Because the card is available for inspection, such transactions are considered less risky and therefore carry lower fees than e-commerce or telephone transactions.

Card-not-present (CNP) transaction. Payment card transaction in which the cardholder does not or cannot present the bank card for a merchant's visual examination. Card-not-present transactions are a major candidate for payment card fraud, because it is difficult for a merchant to verify that the actual cardholder is authorizing a purchase.

Card security code. Numeric codes either written on the payment card magnetic stripe or printed on the card that are used by the financial payment brands for credit, debit, and prepaid transactions to protect against card fraud for magnetic stripe or e-commerce transactions.

Card verification code (CVC)/card verification value (CVV)/card ID (CID). Terms used by MasterCard, Visa and American Express, respectively, for the card security codes used for credit and debit transactions to protect against card fraud.

Cardholder verification method (CVM). Method used to authenticate that the person presenting a payment card is the valid cardholder.

Chip card. Device that includes an embedded secure integrated circuit that can be either a secure microcontroller or equivalent intelligence with internal memory, or a secure memory chip alone. The card connects to a reader with direct physical contact or with a remote contactless radio frequency interface. Chip card technology conforms to international standards (ISO/IEC 7816 and ISO/IEC 14443) and is available in a variety of form factors, including plastic cards, key fobs, subscriber identity modules used in mobile phones, and USB-based tokens.

Contact chip card. Chip card that communicates with a reader through a contact plate.

Contactless chip card. Chip card that communicates with a reader over a radio frequency.

CVC. See **card verification code/card verification value/card ID**.

CVV. See **card verification code/card verification value/card ID**.

Detokenization. Process of retrieving the **PAN** value associated with a payment token based on the payment-token-to-**PAN** mapping stored in a **token vault**.

Dynamic authentication data. Information that is used during a transaction to generate the cryptogram used to verify the card participating in the transaction and that changes from transaction to transaction.

EMV. Specifications initially developed by Europay, MasterCard, and Visa to define a set of requirements to ensure interoperability between payment chip cards and terminals. EMV specifications now encompass contact chip, contactless chip, common payment application (CPA), card personalization, and tokenization.

EMV chip card. A payment chip card that has an EMV application.

EMV token. A token generated based on the EMVCo tokenization specification.

EMVCo. Organization formed in February 1999 by Europay International, MasterCard International, and Visa International to manage, maintain, and enhance the EMV specifications. EMVCo is currently owned by American Express, Discover Financial Services, JCB, MasterCard Worldwide, UnionPay, and Visa, Inc.

End-to-end encryption (E2EE). Uninterrupted protection of payment data by encryption along the entire processing chain. The data is encrypted as soon as it enters a payment system at the POS terminal; the data remains encrypted until it reaches the processor or acquirer, where it is decrypted.

E2EE. See **End-to-end encryption.**

Format-preserving encryption (FPE). Encryption that produces output in the same format as the input. For example:

- To encrypt a 16-digit payment card number so that the output is another 16-digit number
- To encrypt a word so that the output is another English word
- To encrypt an n-bit number so that the output is another n-bit number

FPE. See **Format-preserving encryption.**

Host card emulation. Presentation of a virtual and exact representation of a contactless smart card using only software.

IBE. See **Identity-based encryption**.

Identification and verification (ID&V). Method used to identify a cardholder and verify the cardholder's account to establish a confidence level for binding a token to a PAN or cardholder.

Identity-based encryption (IBE). A form of public-key cryptography in which a third-party server uses a simple identifier, such as an e-mail address, to generate a public key that can be used for encrypting and decrypting electronic messages.

ID&V. See **Identification and verification**.

Magnetic stripe card. Plastic card that uses a band of magnetic material to store data in three tracks. Data is stored by modifying the magnetism of the particles in the magnetic material and read by swiping the magnetic stripe through a reader.

Near Field Communication (NFC). Standards-based wireless communication technology that allows data to be exchanged between devices that are a few centimeters apart. NFC payment transactions use the ISO/IEC Standard 14443 communication protocol currently used by EMV and contactless credit and debit cards.

PAN. See **Primary Account Number**.

Payment Card Industry Data Security Standard (PCI DSS). A framework developed by the PCI Security Standards Council (SSC) for developing a robust payment card data security process – including prevention, detection, and appropriate reaction to security incidents. PCI DSS establishes a minimum set of requirements developed for protecting cardholder data.

PKI. See **Public key infrastructure.**

Point-to-point encryption (P2PE). Protection of payment data by encryption between two specific points in the payment processing chain. Cardholder data is encrypted at inception; the data is decrypted by the P2PE solution provider, which can be a gateway provider, acquirer, processor, or ISO.

Primary Account Number (PAN). Numeric value that identifies a payment card. The issuing organization associates the PAN electronically with a customer and the customer's designated accounts. The PAN is allocated in accordance with ISO/IEC 7812 and comprises 13 to 19 digits, structured as follows:

- A 6-digit issuer identification number, the first digit of which identifies the major industry.
- Up to 12 digits that identify the individual account associated with the card.
- A single check digit calculated using the Luhn algorithm.

Public key infrastructure (PKI). Architecture, organization, techniques, practices, and procedures that support the implementation and operation of a certificate-based public key cryptographic system.

P2PE. See **Point-to-point encryption**.

Symmetric key encryption. Technique for encrypting data in which a secret key, which can be a number, a word, or a string of random letters, is applied to the text of a message to change the content in a particular way. This encryption might be as simple as shifting each letter by a number of places in the alphabet. As long as both sender and recipient know the secret key, they can encrypt and decrypt all messages that use this key.

Token assurance level. Value that identifies a degree of confidence in the authenticity of the binding that ties a payment token to a **PAN** or a cardholder. Token assurance levels are determined by the type of **ID&V** performed and the entity that performed it. Values may also be influenced by additional factors such as token location. Token assurance levels are determined when a token is issued and may be updated if additional ID&V is performed.

Token BIN. Specific **BIN** or range of digits within a BIN that is designated for the purpose of issuing payment tokens and is flagged accordingly in BIN tables.

Token BIN range. Leading 6 to 12 digits of a **token BIN**. The token BIN range constitutes a unique identifier. It may be designed to have the same attributes as the associated issuer's card range and is included in the BIN routing table distributed to participating acquirers and merchants to support routing decisions.

Token cryptogram. Cryptogram that is generated using the token and additional transaction data to create a transaction-unique value.

Token domain. Types of transactions to which use of a token is restricted. Token domains can be channel specific (e.g., NFC only), merchant specific, digital-wallet specific, or any combination.

Token expiration date. The date after which a token is invalid. The date is maintained in the **token vault** and passed in the **PAN** expiration date field during transaction processing to ensure interoperability.

Token service provider (TSP). Entity that maintains the token vault and related processing, including token life cycle processing.

Token vault. Repository that maintains the token-to-**PAN** mapping. Token vaults may also maintain other token requestor attributes, such as domain restrictions or other transaction processing controls.

TSP. See **Token service provider.**

9 References

ANSI X9, http://x9.org/

"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/

"Card Payments Roadmap in the U.S.: How Will EMV Impact the Future Payments Infrastructure?," Smart Card Alliance Payments Council white paper, January 2013, http://www.emv-connection.com/card-payments-roadmap-in-the-u-s-how-will-emv-impact-the-future-payments-infrastructure/

"The Changing U.S. Payments Landscape: Impact on Payment Transactions at Physical Stores," Smart Card Alliance Payments Council white paper, November 2013, http://www.emv-connection.com/the-changing-u-s-payments-landscape-impact-on-payment-transactions-at-physical-stores/

"Cisco 2014 Annual Security Report," Cisco Systems, Inc., https://www.cisco.com/web/offer/gist_ty2_asset/Cisco_2014_ASR.pdf

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

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

"EMV Payment Tokenisation Specification – Technical Framework," Version 1.0, EMVCo, March 2014, http://www.emvco.com/specifications.aspx?id=263

EMVCo web site, http://www.emvco.com

"Guidelines for Derived Personal Identity Verification (PIV) Credentials," National Institute of Standards and Technology, Draft NIST Special Publication 800-157, http://csrc.nist.gov/publications/PubsSPs.html

"Heartland Payment Systems E3™ MSR Wedge Technical Assessment White Paper," Coalfire, Jan. 4, 2011, http://www.heartlandpaymentsystems.com/Heartland/files/70/70ce486a-ca66-4c8f-9098-463900ac2c6b.pdf

"P@$$1234: the end of strong password-only security," *TMT Technology Predictions 2013*, Deloitte, http://www2.deloitte.com/global/en/pages/technology-media-and-telecommunications/articles/tmt-technology-predictions-2013-end-of-strong-passwords.html

PCI Data Security Standards, https://www.pcisecuritystandards.org/security_standards/index.php

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

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

The Clearing House (TCH) web site, https://www.theclearinghouse.org/

"Verizon 2014 PCI Compliance Report," Verizon, http://www.verizonenterprise.com/resources/reports/rp_pci-report-2014-executive-summary_en_xg.pdf.

"Worldwide EMV Card and Terminal Deployment," EMVCo, http://www.emvco.com/about_emvco.aspx?id=202