Impact of PCI P2PE on PCI DSS Compliance & Scope Reduction

Date: May 10, 2019

Prepared by:
Barry Johnson
CISSP, CISA, QSA, PA-QSA, QSA (P2PE), CHPSE
Dara Security
President/CEO

Table of Contents

payway

Executive Summary

The purpose of this white paper is to assist merchants in making compliance decisions related to the use of the Payway, Inc. P2PE solution. To do this, **Dara Security conducted an independent review of publicly available PCI Data Security Standards (PCI DSS)** compliance tools, as well as a review of the Payment Card Industry (PCI) Security Standard Council's (SSC) Point-to-Point Encryption (P2PE) program and how it fits into the modern payments security and compliance ecosystem.

Point-to-Point Encryption (P2PE) is a critical technology used to protect credit card data from being breached. While P2PE has been around for many years, only PCI Validated P2PE technologies, such as the Payway P2PE Solution, have been tested to rigorous standards and should be trusted to reduce risk and PCI DSS scope at a merchant.

In this white paper, we explore PCI validated P2PE in detail, including how P2PE works within an environment and with other technologies, and how the Payway P2PE Solution can be used to reduce both risk and scope in a MOTO environment. We present a challenging use case and demonstrate how P2PE provides an exceptional solution to PCI DSS and credit card security issues within that environment.

This white paper demonstrates how P2PE aligns with the PCI DSS compliance framework in order to simplify merchant compliance efforts.

The intended audience for this document is merchants who are considering or have already implemented the Payway P2PE Solution within their card-not-present [mail order/telephone order (MOTO)] processing environment. The impacts on compliance and risk discussed herein are tailored for merchant organizations, and therefore the term "merchant" is used throughout. Please consult with a qualified security assessor (QSA) for further clarification on how the Payway P2PE Solution may impact your organization's risk and compliance.

The PCI Security Standards Council and Programs

The PCI SSC was founded by the major card brands: Visa, Mastercard, American Express, Discover, and JCB. The PCI SSC maintains the PCI DSS and oversees additional standards that are used to validate devices, software, services, and solutions that aid merchants in meeting those standards. Among them are the Payment Application Data Security Standard (PA-DSS), which may be used to validate software applications; the PIN Transaction Security Standard (PCI PTS), which may be used in the approval of transaction devices; and the PCI Point-to-Point Encryption standard (PCI P2PE), which may be used to validate solution providers and components that are used to perform terminal-based encryption, key management, and decryption operations.

About PCI DSS 3.2.1

The Payment Card Industry Data Security Standard (PCI DSS) was developed to encourage and enhance cardholder data security and facilitates the broad adoption of consistent data security measures globally.

PCI DSS provides a baseline of technical and operational requirements designed to protect account data. PCI DSS applies to all entities involved in payment card processing—including merchants, processors, acquirers, issuers, and service providers. PCI DSS also applies to all other entities that store, process or transmit cardholder data (CHD) and/or sensitive authentication data (SAD).

PCI DSS comprises a minimum set of requirements for protecting account data and may be enhanced by additional controls and practices to further mitigate risks, as well as local, regional and sector laws and regulations. The primary account number is the defining factor for cardholder data. If cardholder name, service code, and/or expiration date are stored, processed or transmitted with the PAN, or are otherwise present in the cardholder data environment, they must be protected in accordance with applicable PCI DSS requirements.

PCI DSS requirements apply to organizations where account data (cardholder data and/or sensitive authentication data) is stored, processed or transmitted.

The PCI DSS security requirements apply to all system components included in or connected to the cardholder data environment. The cardholder data environment (CDE) is comprised of people, processes and technologies that store, process, or transmit cardholder data or sensitive authentication data. Some PCI DSS requirements may also be applicable to organizations that have outsourced their payment operations or management of their CDE. Additionally, organizations that outsource their CDE or payment operations to third parties are responsible for ensuring that the third party, per the applicable PCI DSS requirements, protects the account data.

About P2PE 2.0

P2PE 2.0 is standard developed by the card brands and the PCI SSC.
P2PE is the standard designed to work hand-in-hand with PCI DSS.

P2PE is a methodology for securing credit card data by encrypting it from the time a card is swiped until it reaches the payment processor where it is decrypted.

When implemented properly, these types of solutions make payment card transactions more secure by preventing the theft of credit card data while unencrypted on a POS device, or in transit.

Point-to-point encryption is designed to encrypt cardholder data at the time of swipe point-of-interaction (POI) utilizing an encryption key that is built into the POI. Once encrypted, sensitive cardholder data is not decrypted until it arrives at a secured end point, typically an acquirer, processor or gateway. By using P2PE, account data (cardholder data and sensitive authentication data) is unreadable until it reaches the secure decryption environment, which makes it less valuable if the data is stolen in a breach. By encrypting cardholder data at the POI, merchants can significantly reduce the risk of a data breach and the scope of PCI DSS compliance requirements.

Tools for Securing Transactions

There are three valuable technologies that are sometimes misunderstood. Here we discuss EMV, P2PE and Tokenization, where they may add value to a merchant's security program, and common misconceptions about their impact on a merchant's security and risk profile.

EMV – Securing Against Counterfeit Cards

EMVCo, which was founded by (and named after) Europay, Mastercard, and Visa in 1994, manages the EMV standards. The payment industry around the world has begun adopting EMV for production and transaction support for credit cards issued with integrated chips in order to provide new card fraud protections for consumers. To facilitate this transition in the United States, the major card brands have instituted phased liability shifts, where card present merchants or credit card issuers who fail to support these cards may be liable for counterfeit card fraud. As credit card issuers move to offer cardholder verification methods such as PIN, support for EMV may also help merchants shift liability for fraud resulting from lost or stolen cards. Important liability shift dates include October 2015, which affected most credit card networks and industries; October 2016 for ATMs accepting Mastercard; October 2017 for other ATM cards; and the upcoming liability shift in October 2020 for automated fuel dispensers.

The EMV chip embedded within the new chip cards is capable of using advanced cryptography to generate a unique code (iCVV) that is then sent to the card networks with each transaction to confirm that the physical card is legitimate. This process has been demonstrated to be effective at preventing fraudsters from creating counterfeit cards. However, the EMV chip does not provide any encryption for the credit card primary account number (PAN), expiration date, or cardholder name: three sensitive data elements classified as cardholder data and required to be protected according to PCI DSS. Threat actors that steal this information can use this data to conduct fraud through other channels such as online (e-commerce) or MOTO transactions.

Therefore, support for EMV does not reduce a merchant's PCI responsibilities for protecting account data, nor has recent movement throughout the industry to adopt EMV had any measurable impact on the number of cardholder data breaches. In summary, EMV is primarily effective for reducing card-present fraud by securing against counterfeit cards.

P2PE – Securing Card Data in Flight

P2PE is the term used by the PCI SSC to refer to its terminal-based encryption standard, where transactions are encrypted within specific PTS-approved hardware using encryption keys that reasonably protect the account data so that it can be transferred through the merchant environment safely, reducing risk of compromise. The role of P2PE is to immediately and fully encrypt all cardholder data and sensitive authentication.

By using strong encryption, device management practices, and key management, P2PE is effective at addressing the risk of card data compromise for card data in transit out of the merchant network as it is transmitted to the gateway or acquirer for decryption and processing.

There are two types of terminal encryption – PCI-listed P2PE solutions and unlisted solutions (sometimes called end-to-end encryption or E2EE).

There are three high-level requirements that every P2PE/E2EE solution must offer:

1 The card data must be encrypted using strong cryptography

2 The encryption must be performed within a secure hardware device

3 It must not be feasible to decrypt the data within the merchant environment

As a result of these requirements, it becomes physically improbable to access card data prior to encryption; it becomes computationally infeasible to derive captured card data using brute-force methods; and it becomes logically unattainable to access the decryption keys in order to decrypt directly.

Through this process, P2PE performs the function of devaluing the cardholder data in the eyes of any hacker who may otherwise seek to access this information within the merchant's software, systems, and network, therefore securing card data in flight.

Tokenization – Securing Card Data at Rest

Finally, there are merchants who must perform certain customer billing functions, such as delayed charges, subscriptions, refunds, or credits, which require credit card information. Some merchants may have also used cardholder data as a means to track consumer behavior (although this practice is generally prohibited). Traditionally, these operations require the merchant to store sensitive credit card information so that it can be accessible for future use. Unfortunately, this also leaves a "treasure trove" of stored credit card data that may be stolen. For that reason, the efforts required to fully protect stored card data (PCI DSS Requirement 3) can be quite extensive and expensive.

Tokenization is the technology where secure card data storage is centralized and a different value is used to represent the original cardholder data.

When ready to be re-used, the token must generally be passed to the tokenization provider, where the original cardholder data is retrieved, decrypted, and utilized.

Similar to P2PE, a compliant third-party service provider may perform this service on behalf of the merchant, including portions of the data security that rely on cryptography (in this case, storage encryption). However, unlike P2PE, the value that the merchant receives is not commonly a reversible encrypted form of the original PAN but is uniquely designed to be stored safely. The token value may resemble a credit card number or even retain certain non-sensitive portions of the card data, or it may look entirely different. In some cases, the token may be an encrypted form of the cardholder data, but in most cases, it is merely an arbitrary or random reference number used to access the stored information in the token vault. The entity performing the tokenization may be the gateway or another service provider, the acquirer, the card brand, or

even the issuing bank.

To take full advantage of the benefits of tokenization, PCI SSC recommends that merchants tokenize sensitive data as quickly as possible, replace cardholder data with tokens wherever it is stored, and use services that do not provide a mechanism to "detokenize" data, as this presents another avenue that may be exploited. In each case, the merchant must still observe PCI compliance requirements for systems that store, transmit, or process card data before the data has been tokenized.

When properly implemented, use of tokenization instead of storing actual cardholder data is valuable for securing card data at rest.

PCI P2PE-Listed vs. End-to-End Encryption Solutions (E2EE)

There are many ways in which to perform transaction encryption, and each has its own advantage. For the purposes of this review, terminal-based encryption solutions fall under two distinct categories: listed P2PE solutions and unlisted encryption solutions (sometimes called E2EE solutions).

Validated PCI P2PE Solutions

Validated PCI Point-to-Point Encryption (P2PE) systems protect cardholder data, such as the primary account number (PAN) from the Point-of-Interaction (POI) terminal within a merchant's environment, to a payment gateway that may decrypt the data, such as Payway, Inc. A merchant will never have access to unencrypted credit card data, removing entirely this critically sensitive data element from their environment, and eliminating the largest source of credit card data breaches.

In a credit card data breach, an attacker gains access to a store or corporate headquarters and targets any storage or processing of credit cards by using special tools to monitor memory or to scan disks. In a P2PE system, there is no unencrypted credit card data, and therefore the only data items that might be available to an attacker would be truncated data (e.g. the first six and last four digits of a credit card), encrypted credit card data, or tokenized credit card data. In each of these cases, there is little the criminal can do with this data.

As such, P2PE is one of the best methods a merchant can use to protect their customers, themselves and prevent a credit card breach. In return, merchants using these validated solutions receive a sizable reduction in both the size of their CDE and the number of PCI DSS requirements that apply to them.

Merchants who use a validated solution within their environment and keep this environment segmented from any card data from other channels (e.g., e-commerce) may be eligible to complete the authorized self-assessment questionnaire SAQ P2PE that is known and accepted by all acquirers. Under PCI DSS v3.2.1, this represents a significant reduction of controls, reducing the number of questions by nearly 90% for merchants moving from the SAQ D (329 questions) to SAQ P2PE (33 questions).

Another aspect of scope reduction is the impact of PCI P2PE on the definition of the CDE itself. Since merchant systems can no longer access the cardholder data once it is properly encrypted, P2PE effectively reduces the number of networks and systems considered to be within the scope of the PCI DSS assessment. This scoping guidance is endorsed by PCI and commonly followed by assessors, but only for solutions that have been through the validation process.

Non-Validated E2EE Solutions

Solutions that have not been validated, but still provide functions such as encrypting within the POI terminal and decrypting outside the merchant environment, are generally called non-validated P2PE solutions, or E2EE. The trouble with non-validated solutions is that there may be no way for a merchant to know whether the provider has fully addressed the controls identified by PCI SSC as necessary to properly protect the account data.

Since non-validated solutions have not been assessed under the standardized PCI P2PE framework by qualified assessors, merchants using these solutions may still need to implement additional security countermeasures to ensure threats associated with the absence of these controls.

Since there is no PCI-approved assessment framework for non-validated solutions, merchants using these solutions that wish to reduce the scope of their compliance assessment must be able to determine how thoroughly the E2EE solution has addressed the threats identified by PCI P2PE and use this risk assessment to identify any controls that are adequately addressed and, therefore, inapplicable. Non-validated solutions do not qualify for the reduced SAQ P2PE, so merchants using these solutions should use the SAQ D (or ROC template, if applicable), mark these controls as "N/A," provide full justification for these assertions within the "Appendix C: Explanation of Non-Applicability," and receive special approval from the acquirer for any control reductions.

P2PE Deployment

Card-not-present transaction types for Mail-Order-Telephone-Order (MOTO) merchants are the primary focus for the Payway P2PE Solution.

By utilizing the ID Tech SREDKey device listed in the solution's P2PE Instruction Manual (PIM), a merchant may implement the Payway P2PE Solution in their environment. The PIM provides instructions as to how to receive, set up and manage the POI devices, and other details surrounding the P2PE solution. It is important that the merchant follow all the applicable instructions within the PIM.

The scope reduction for the merchant would generally be the entire network supporting the workstations used to enter cardholder data. This requires all cardholder data entry be performed not on the keyboard of the end-user's workstation, but instead on an attached ID Tech SREDKey POI device. The customer's name, order information, address, etc., may be entered on the primary keyboard, but when the time comes to receive the credit card information, including Primary Account Number, Expiration Date and CVV2, these must be entered on the ID Tech SREDKey POI device which will then encrypt the data and fill out the form with encrypted data.

As the Payway P2PE Solution's supported POI device, the ID Tech SREDKey currently only supports USB interfaces. It is important to note that the client workstations that the POI devices are connected to are not considered in scope for PCI DSS unless they receive cardholder data from a non-P2PE input mechanism, such as manual entry on the keyboard. By using the validated Payway P2PE Solution, merchants are eligible to complete the authorized self-assessment questionnaire SAQ P2PE that is known and accepted by all acquirers. Under PCI DSS v3.2.1, this represents a significant reduction of controls, reducing the number of questions by nearly 90% for merchants moving from the SAQ D (329 questions) to SAQ P2PE (33 questions).

Use Case – MOTO Merchant

MOTO merchants have unique challenges when considering cardholder data security and PCI DSS. Cardholder data may be received by mail or telephone and must then be manually entered by employees. This data entry may be done into an internally deployed payment system that stores cardholder data or into a virtual terminal provided by a third party. In any case, the workstations used by these end users, the networks the workstations are deployed on and the deployed infrastructure devices are all in scope for PCI DSS. As these employees doing the data entry also require access to internal services such as email and file sharing, without additional segmentation controls, this may bring the entirety of the merchant's complex network into PCI DSS scope.

PCI DSS requires significant security controls around in-scope networks and systems including hardening, patching, logging, but most importantly, quarterly internal and external vulnerability scanning and annual internal and external penetration testing.

Up to this time, the primary alternative for a MOTO merchant was to identify all systems involved in card acceptance and segment all of the workstations and supporting services to a separate network. This is a significant undertaking and costly to perform and maintain.

P2PE solves this dilemma. Use of a P2PE device connected to a workstation or network does not bring that workstation or network into scope for PCI DSS. Additional endpoint controls, mandated by PCI DSS, are not required, reducing the amount of overhead that an already burdened IT department may have to support.

The P2PE devices may safely share the network segments with other workstations and networks. This brings flexibility and convenience to network design and allows for rapid changes on the network. The Payway P2PE Solution supports this model and is an ideal solution for the MOTO market.

Summary

Validated P2PE solutions represent the most effective way of protecting card-present and agent-entered [card-not-present (MOTO)] credit card transactions. By performing encryption on hardware at a POI device and decryption using hardware devices at Payway, Inc., card data is protected between these two points. This allows a merchant using the Payway P2PE Solution to receive scope reduction from their PCI DSS QSA, or to use the PCI SAQ-P2PE should they be eligible.

Payway, Inc. has raised the bar of encrypted payment service by validating to the PCI P2PE standard and providing their customers both the means to reduce their risk as well as their PCI DSS scope.

P2PE PCI DSS Audit Controls Impact to a Merchant Environment

PCI DSS Requirements v3.2.1	Control Reduction Automatically Provided			
Requirement 1: Install and maintain a firewall configuration to protect cardholder data	**P2PE**	**E2EE**	**Tokenization**	**EMV**
1.1 Establish and implement firewall and router configuration standards that include the following:	●			
1.1.1 A formal process for approving and testing all network connections and changes to the firewall and router configurations.	●			
1.1.2 Current network diagram that identifies all connections between the cardholder data environment and other networks, including any wireless networks.	●			
1.1.3 Current diagram that shows all cardholder data flows across systems and networks.	●			
1.1.4 Requirements for a firewall at each Internet connection and between any demilitarized zone (DMZ) and the internal network zone.	●			
1.1.5 Description of groups, roles, and responsibilities for management of network components.	●			
1.1.6 Documentation of business justification and approval for use of all services, protocols, and ports allowed, including documentation of security features implemented for those protocols considered to be insecure.	●			
1.1.7 Requirement to review firewall and router rule sets at least every six months.	●			

PCI DSS Requirements v3.2.1 (cont.)	Control Reduction Automatically Provided			
Requirement 1: Install and maintain a firewall configuration to protect cardholder data	**P2PE**	**E2EE**	**Tokenization**	**EMV**
1.2 Build firewall and router configurations that restrict connections between untrusted networks and any system components in the cardholder data environment. Note: An "untrusted network" is any network that is external to the networks belonging to the entity under review, and/or which is out of the entity's ability to control or manage.	●			
1.2.1 Restrict inbound and outbound traffic to that which is necessary for the cardholder data environment, and specifically deny all other traffic.	●			
1.2.2 Secure and synchronize router configuration files.	●			
1.2.3 Install perimeter firewalls between all wireless networks and the cardholder data environment, and configure these firewalls to deny or, if traffic is necessary for business purposes, permit only authorized traffic between the wireless environment and the cardholder data environment.	●			
1.3 Prohibit direct public access between the Internet and any system component in the cardholder data environment.	●			
1.3.1 Implement a DMZ to limit inbound traffic to only system components that provide authorized publicly accessible services, protocols, and ports.	●			
1.3.2 Limit inbound Internet traffic to IP addresses within the DMZ.	●			
1.3.3 Implement anti-spoofing measures to detect and block forged source IP addresses from entering the network. (For example, block traffic originating from the Internet with an internal source address.)	●			
1.3.4 Do not allow unauthorized outbound traffic from the cardholder data environment to the Internet.	●			
1.3.5 Permit only "established" connections into the network.	●			
1.3.6 Place system components that store cardholder data (such as a database) in an internal network zone, segregated from the DMZ and other untrusted networks.	●			
1.3.7 Do not disclose private IP addresses and routing information to unauthorized parties. **Note:** Methods to obscure IP addressing may include, but are not limited to: • Network Address Translation (NAT) • Placing servers containing cardholder data behind proxy servers/firewalls • Removal or filtering of route advertisements for private networks that employ registered addressing • Internal use of RFC1918 address space instead of registered addresses	●			

PCI DSS Requirements v3.2.1 (cont.)	Control Reduction Automatically Provided			
Requirement 1: Install and maintain a firewall configuration to protect cardholder data	**P2PE**	**E2EE**	**Tokenization**	**EMV**
1.4 Install personal firewall software or equivalent functionality on any portable computing devices (including company and/or employee-owned) that connect to the Internet when outside the network (for example, laptops used by employees), and which are also used to access the CDE. Firewall (or equivalent) configurations include: • Specific configuration settings are defined • Personal firewall (or equivalent functionality) is actively running • Personal firewall (or equivalent functionality) is not alterable by users of the portable computing devices	●			
1.5 Ensure that security policies and operational procedures for managing firewalls are documented, in use, and known to all affected parties.				
Requirement 2: Do not use vendor-supplied defaults for system passwords and other security parameters	Control Reduction Automatically Provided			
	P2PE	**E2EE**	**Tokenization**	**EMV**
2.1 Always change vendor-supplied defaults and remove or disable unnecessary default accounts before installing a system on the network. This applies to ALL default passwords, including but not limited to those used by operating systems, software that provides security services, application and system accounts, point-of-sale (POS) terminals, payment applications, Simple Network Management Protocol (SNMP) community strings, etc.	●			
2.1.1 For wireless environments connected to the cardholder data environment or transmitting cardholder data, change ALL wireless vendor defaults at installation, including but not limited to default wireless encryption keys, passwords, and SNMP community strings.	●			
2.2 Develop configuration standards for all system components. Assure that these standards address all known security vulnerabilities and are consistent with industry-accepted system hardening standards. Sources of industry-accepted system hardening standards may include, but are not limited to: • Center for Internet Security (CIS) • International Organization for Standardization (ISO) • SysAdmin Audit Network Security (SANS) Institute • National Institute of Standards Technology (NIST)	●			
2.2.1 Implement only one primary function per server to prevent functions that require different security levels from co-existing on the same server. (For example, web servers, database servers, and DNS should be implemented on separate servers.) **Note:** Where virtualization technologies are in use, implement only one primary function per virtual system component.	●			
2.2.2 Enable only necessary services, protocols, daemons, etc., as required for the function of the system.	●			

PCI DSS Requirements v3.2.1 (cont.)	Control Reduction Automatically Provided			
Requirement 2: Do not use vendor-supplied defaults for system passwords and other security parameters (cont.)	**P2PE**	**E2EE**	**Tokenization**	**EMV**
2.2.3 Implement additional security features for any required services, protocols, or daemons that are considered to be insecure. **Note:** Where SSL/early TLS is used, the requirements in Appendix A2 must be completed.	●			
2.2.4 Configure system security parameters to prevent misuse.	●			
2.2.5 Remove all unnecessary functionality, such as scripts, drivers, features, subsystems, file systems, and unnecessary web servers.	●			
2.3 Encrypt all non-console administrative access using strong cryptography. **Note:** Where SSL/early TLS is used, the requirements in Appendix A2 must be completed.	●			
2.4 Maintain an inventory of system components that are in scope for PCI DSS.	●			
2.5 Ensure that security policies and operational procedures for managing vendor defaults and other security parameters are documented, in use, and known to all affected parties.	●			
Requirement 3: Protect stored cardholder data **Note:** For P2PE deployments, non-checked requirements (3.1, 3.2, 3.2.2, & 3.7) only apply for those merchants that have paper records with the Primary Account Number (PAN).	Control Reduction Automatically Provided			
	P2PE	**E2EE**	**Tokenization**	**EMV**
3.1 Keep cardholder data storage to a minimum by implementing data retention and disposal policies, procedures and processes that include at least the following for all cardholder data (CHD) storage: • Limiting data storage amount and retention time to that which is required for legal, regulatory, and/or business requirements • Specific retention requirements for cardholder data • Processes for secure deletion of data when no longer needed • A quarterly process for identifying and securely deleting stored cardholder data that exceeds defined retention				
3.2 Do not store sensitive authentication data after authorization (even if encrypted). If sensitive authentication data is received, render all data unrecoverable upon completion of the authorization process. It is permissible for issuers and companies that support issuing services to store sensitive authentication data if: 1. There is a business justification; and 2. The data is stored securely. Sensitive authentication data includes the data as cited in the following Requirements 3.2.1 through 3.2.3:				

Requirement 3: Protect stored cardholder data (cont.) **Note:** For P2PE deployments, non-checked requirements (3.1, 3.2, 3.2.2, & 3.7) only apply for those merchants that have paper records with the Primary Account Number (PAN).	Control Reduction Automatically Provided			
	P2PE	**E2EE**	**Tokenization**	**EMV**

3.2.1 Do not store the full contents of any track (from the magnetic stripe located on the back of a card, equivalent data contained on a chip, or elsewhere) after authorization. This data is alternatively called full track, track, track 1, track 2, and magnetic-stripe data.
 	
Note: In the normal course of business, the following data elements from the magnetic stripe may need to be retained:
  • The cardholder's name
  • Primary account number (PAN)
  • Expiration date
  • Service code
To minimize risk, store only these data elements as needed for business.
	●			

3.2.2 Do not store the card verification code or value (three-digit or four-digit number printed on the front or back of a payment card used to verify card-not-present transactions) after authorization.				
3.2.3 Do not store the personal identification number (PIN) or the encrypted PIN block after authorization.	●			
3.3 Mask PAN when displayed (the first six and last four digits are the maximum number of digits to be displayed), such that only personnel with a legitimate business need can see more than the first six/last four digits of the PAN. **Note:** This requirement does not supersede stricter requirements in place for displays of cardholder data—for example, legal or payment card brand requirements for point-of-sale (POS) receipts.	●			

3.4 Render PAN unreadable anywhere it is stored (including on portable digital media, backup media, and in logs) by using any of the following approaches:
  • One-way hashes based on strong cryptography,
    (hash must be of the entire PAN)
  • Truncation
  • (hashing cannot be used to replace the truncated segment of PAN)
  • Index tokens and pads (pads must be securely stored)
  • Strong cryptography with associated key-management processes and procedures
 	
Note: It is a relatively trivial effort for a malicious individual to reconstruct original PAN data if they have access to both the truncated and hashed version of a PAN. Where hashed and truncated versions of the same PAN are present in an entity's environment, additional controls must be in place to ensure that the hashed and truncated versions cannot be correlated to reconstruct the original PAN.
	●		●	

3.4.1 If disk encryption is used (rather than file- or column-level database encryption), logical access must be managed separately and independently of native operating system authentication and access control mechanisms (for example, by not using local user account databases or general network login credentials). Decryption keys must not be associated with user accounts. **Note:** This requirement applies in addition to all other PCI DSS encryption and key-management requirements.	●		●	

Requirement 3: Protect stored cardholder data (cont.) **Note:** For P2PE deployments, non-checked requirements (3.1, 3.2, 3.2.2, & 3.7) only apply for those merchants that have paper records with the Primary Account Number (PAN).	Control Reduction Automatically Provided			
	P2PE	**E2EE**	**Tokenization**	**EMV**
3.5 Document and implement procedures to protect keys used to secure stored cardholder data against disclosure and misuse. **Note:** This requirement applies to keys used to encrypt stored cardholder data, and also applies to key-encrypting keys used to protect data-encrypting keys—such key-encrypting keys must be at least as strong as the data-encrypting key.	●		●	
3.5.1 Additional requirement for service providers only: Maintain a documented description of the cryptographic architecture that includes: • Details of all algorithms, protocols, and keys used for the protection of cardholder data, including key strength and expiry date • Description of the key usage for each key. • Inventory of any HSMs and other SCDs used for key management				
3.5.2 Restrict access to cryptographic keys to the fewest number of custodians necessary.	●		●	
3.5.3 Store secret and private keys used to encrypt/decrypt cardholder data in one (or more) of the following forms at all times: • Encrypted with a key-encrypting key that is at least as strong as the data-encrypting key, and that is stored separately from the data-encrypting key • Within a secure cryptographic device (such as a hardware (host) security module (HSM) or PTS-approved point-of-interaction device) • As at least two full-length key components or key shares, in accordance with an industry-accepted method **Note:** It is not required that public keys be stored in one of these forms.	●		●	
3.5.4 Store cryptographic keys in the fewest possible locations.	●		●	
3.6 Fully document and implement all key-management processes and procedures for cryptographic keys used for encryption of cardholder data, including the following: **Note:** Numerous industry standards for key management are available from various resources including NIST, which can be found at http://csrc.nist.gov.	●		●	
3.6.1 Generation of strong cryptographic keys	●		●	
3.6.2 Secure cryptographic key distribution	●		●	
3.6.3 Secure cryptographic key storage	●		●	
3.6.4 Cryptographic key changes for keys that have reached the end of their cryptoperiod (for example, after a defined period of time has passed and/or after a certain amount of cipher-text has been produced by a given key), as defined by the associated application vendor or key owner, and based on industry best practices and guidelines (for example, NIST Special Publication 800-57).	●		●	

Requirement 3: Protect stored cardholder data (cont.) **Note:** For P2PE deployments, non-checked requirements (3.1, 3.2, 3.2.2, & 3.7) only apply for those merchants that have paper records with the Primary Account Number (PAN).	Control Reduction Automatically Provided			
	P2PE	**E2EE**	**Tokenization**	**EMV**
3.6.5 Retirement or replacement (for example, archiving, destruction, and/or revocation) of keys as deemed necessary when the integrity of the key has been weakened (for example, departure of an employee with knowledge of a clear-text key component), or keys are suspected of being compromised. **Note:** If retired or replaced cryptographic keys need to be retained, these keys must be securely archived (for example, by using a key-encryption key). Archived cryptographic keys should only be used for decryption/verification purposes.	●		●	
3.6.6 If manual clear-text cryptographic key-management operations are used, these operations must be managed using split knowledge and dual control. **Note:** Examples of manual key-management operations include, but are not limited to: key generation, transmission, loading, storage and destruction.	●		●	
3.6.7 Prevention of unauthorized substitution of cryptographic keys.	●		●	
3.6.8 Requirement for cryptographic key custodians to formally acknowledge that they understand and accept their key-custodian responsibilities.	●		●	
3.7 Ensure that security policies and operational procedures for protecting stored cardholder data are documented, in use, and known to all affected parties.				

Requirement 4: Encrypt transmission of cardholder data across open, public networks	Control Reduction Automatically Provided			
	P2PE	**E2EE**	**Tokenization**	**EMV**
4.1 Use strong cryptography and security protocols to safeguard sensitive cardholder data during transmission over open, public networks, including the following: • Only trusted keys and certificates are accepted • The protocol in use only supports secure versions or configurations • The encryption strength is appropriate for the encryption methodology in use **Note:** Where SSL/early TLS is used, the requirements in Appendix A2 must be completed. Examples of open, public networks include but are not limited to: • The Internet • Wireless technologies, including 802.11 and Bluetooth • Cellular technologies, for example, Global System for Mobile communications (GSM), Code division multiple access (CDMA) • General Packet Radio Service (GPRS) • Satellite communications	●			

Requirement 4: Encrypt transmission of cardholder data across open, public networks (cont.)	Control Reduction Automatically Provided			
	P2PE	**E2EE**	**Tokenization**	**EMV**
4.1.1 Ensure wireless networks transmitting cardholder data, or connected to the cardholder data environment, use industry best practices to implement strong encryption for authentication and transmission.	●			
4.2 Never send unprotected PANs by end-user messaging technologies (for example, e-mail, instant messaging, SMS, chat, etc.).	●			
4.3 Ensure that security policies and operational procedures for encrypting transmissions of cardholder data are documented, in use, and known to all affected parties.	●			

Requirement 5: Use and regularly update anti-virus software or programs	Control Reduction Automatically Provided			
	P2PE	**E2EE**	**Tokenization**	**EMV**
5.1 Deploy anti-virus software on all systems commonly affected by malicious software (particularly personal computers and servers).	●			
5.1.1 Ensure that anti-virus programs are capable of detecting, removing, and protecting against all known types of malicious software.	●			
5.1.2 For systems considered to be not commonly affected by malicious software, perform periodic evaluations to identify and evaluate evolving malware threats in order to confirm whether such systems continue to not require anti-virus software.	●			
5.2 Ensure that all anti-virus mechanisms are maintained as follows: • Are kept current • Perform periodic scans • Generate audit logs which are retained per PCI DSS Requirement 10.7	●			
5.3 Ensure that anti-virus mechanisms are actively running and cannot be disabled or altered by users, unless specifically authorized by management on a case-by-case basis for a limited time period. **Note:** Anti-virus solutions may be temporarily disabled only if there is legitimate technical need, as authorized by management on a case-by-case basis. If anti-virus protection needs to be disabled for a specific purpose, it must be formally authorized. Additional security measures may also need to be implemented for the period of time during which anti-virus protection is not active.	●			
5.4 Ensure that security policies and operational procedures for protecting systems against malware are documented, in use, and known to all affected parties.	●			

Requirement 6: Develop and maintain secure systems and applications	Control Reduction Automatically Provided			
	P2PE	E2EE	Tokenization	EMV
6.1 Establish a process to identify security vulnerabilities, using reputable outside sources for security vulnerability information, and assign a risk ranking (for example, as "high," "medium," or "low") to newly discovered security vulnerabilities. **Note:** Risk rankings should be based on industry best practices as well as consideration of potential impact. For example, criteria for ranking vulnerabilities may include consideration of the CVSS base score, and/or the classification by the vendor, and/or type of systems affected. Methods for evaluating vulnerabilities and assigning risk ratings will vary based on an organization's environment and risk-assessment strategy. Risk rankings should, at a minimum, identify all vulnerabilities considered to be a "high risk" to the environment. In addition to the risk ranking, vulnerabilities may be considered "critical" if they pose an imminent threat to the environment, impact critical systems, and/or would result in a potential compromise if not addressed. Examples of critical systems may include security systems, public-facing devices and systems, databases, and other systems that store, process, or transmit cardholder data.	●			
6.2 Ensure that all system components and software are protected from known vulnerabilities by installing applicable vendor-supplied security patches. Install critical security patches within one month of release. **Note:** Critical security patches should be identified according to the risk ranking process defined in Requirement 6.1.	●			

6.3 Develop internal and external software applications (including web-based administrative access to applications) securely, as follows:
  • In accordance with PCI DSS (for example, secure authentication and logging)
  • Based on industry standards and/or best practices
  • Incorporating information security throughout the software-development life cycle
 	
Note: This applies to all software developed internally as well as bespoke or custom software developed by a third party.
	●			

6.3.1 Remove development, test and/or custom application accounts, user IDs, and passwords before applications become active or are released to customers.	●			

Requirement 6: Develop and maintain secure systems and applications (cont.)	Control Reduction Automatically Provided			
	P2PE	E2EE	Tokenization	EMV
6.3.2 Review custom code prior to release to production or customers in order to identify any potential coding vulnerability (using either manual or automated processes) to include at least the following: • Code changes are reviewed by individuals other than the originating code author, and by individuals knowledgeable about code-review techniques and secure coding practices • Code reviews ensure code is developed according to secure coding guidelines • Appropriate corrections are implemented prior to release • Code-review results are reviewed and approved by management prior to release **Note:** This requirement for code reviews applies to all custom code (both internal and public-facing), as part of the system development life cycle. Code reviews can be conducted by knowledgeable internal personnel or third parties. Public-facing web applications are also subject to additional controls, to address ongoing threats and vulnerabilities after implementation, as defined at PCI DSS Requirement 6.6.	●			
6.4 Follow change control processes and procedures for all changes to system components. The processes must include the following:	●			
6.4.1 Separate development/test environments from production environments, and enforce the separation with access controls.	●			
6.4.2 Separation of duties between development/test and production environments.	●			
6.4.3 Production data (live PANs) are not used for testing or development.	●			
6.4.4 Removal of test data and accounts from system components before the system becomes active/goes into production.	●			
6.4.5 Change control procedures must include the following:	●			
6.4.5.1 Documentation of impact.	●			
6.4.5.2 Documented change approval by authorized parties.	●			
6.4.5.3 Functionality testing to verify that the change does not adversely impact the security of the system.	●			
6.4.5.4 Back-out procedures.	●			
6.4.6 Upon completion of a significant change, all relevant PCI DSS requirements must be implemented on all new or changed systems and networks, and documentation updated as applicable.	●			

Requirement 6: Develop and maintain secure systems and applications (cont.)	Control Reduction Automatically Provided			
	P2PE	**E2EE**	**Tokenization**	**EMV**
6.5 Address common coding vulnerabilities in software-development processes as follows: • Train developers at least annually in up-to-date secure coding techniques, including how to avoid common coding vulnerabilities • Develop applications based on secure coding guidelines **Note:** The vulnerabilities listed at 6.5.1 through 6.5.10 were current with industry best practices when this version of PCI DSS was published. However, as industry best practices for vulnerability management are updated (for example, the OWASP Guide, SANS CWE Top 25, CERT Secure Coding, etc.), the current best practices must be used for these requirements. **Note:** Requirements 6.5.1 through 6.5.6, below, apply to all applications (internal or external).	●			
6.5.1 Injection flaws, particularly SQL injection. Also consider OS Command Injection, LDAP and XPath injection flaws as well as other injection flaws.	●			
6.5.2 Buffer overflows	●			
6.5.3 Insecure cryptographic storage	●			
6.5.4 Insecure communications	●			
6.5.5 Improper error handling	●			
6.5.6 All "high risk" vulnerabilities identified in the vulnerability identification process (as defined in PCI DSS Requirement 6.1).	●			
Note: Requirements 6.5.7 through 6.5.10, below, apply to web applications and application interfaces (internal or external):				
6.5.7 Cross-site scripting (XSS)	●			
6.5.8 Improper access control (such as insecure direct object references, failure to restrict URL access, directory traversal, and failure to restrict user access to functions)	●			
6.5.9 Cross-site request forgery (CSRF)	●			
6.5.10 Broken authentication and session management	●			

Requirement 6: Develop and maintain secure systems and applications (cont.)	Control Reduction Automatically Provided			
	P2PE	**E2EE**	**Tokenization**	**EMV**
6.6 For public-facing web applications, address new threats and vulnerabilities on an ongoing basis and ensure these applications are protected against known attacks by either of the following methods: • Reviewing public-facing web applications via manual or automated application vulnerability security assessment tools or methods, at least annually and after any changes **Note:** This assessment is not the same as the vulnerability scans performed for Requirement 11.2. • Installing an automated technical solution that detects and prevents web-based attacks (for example, a web-application firewall) in front of public-facing web applications, to continually check all traffic	●			
6.7 Ensure that security policies and operational procedures for developing and maintaining secure systems and applications are documented, in use, and known to all affected parties.	●			

Requirement 7: Restrict access to cardholder data by business need to know	Control Reduction Automatically Provided			
	P2PE	**E2EE**	**Tokenization**	**EMV**
7.1 Limit access to system components and cardholder data to only those individuals whose job requires such access.	●			
7.1.1 Define access needs for each role, including: • System components and data resources that each role needs to access for their job function • Level of privilege required (for example, user, administrator, etc.) for accessing resources	●			
7.1.2 Restrict access to privileged user IDs to least privileges necessary to perform job responsibilities.	●			
7.1.3 Assign access based on individual personnel's job classification and function.	●			
7.1.4 Require documented approval by authorized parties specifying required privileges.	●			
7.2 Establish an access control system(s) for systems components that restricts access based on a user's need to know, and is set to "deny all" unless specifically allowed. This access control system(s) must include the following:	●			
7.2.1 Coverage of all system components	●			

Requirement 7: Restrict access to cardholder data by business need to know (cont.)	Control Reduction Automatically Provided			
	P2PE	E2EE	Tokenization	EMV
7.2.2 Assignment of privileges to individuals based on job classification and function.	●			
7.2.3 Default "deny-all" setting.	●			
7.3 Ensure that security policies and operational procedures for restricting access to cardholder data are documented, in use, and known to all affected parties.	●			

Requirement 8: Assign a unique ID to each person with computer access	Control Reduction Automatically Provided			
	P2PE	E2EE	Tokenization	EMV
8.1 Define and implement policies and procedures to ensure proper user identification management for non-consumer users and administrators on all system components as follows:	●			
8.1.1 Assign all users a unique ID before allowing them to access system components or cardholder data.	●			
8.1.2 Control addition, deletion, and modification of user IDs, credentials, and other identifier objects.	●			
8.1.3 Immediately revoke access for any terminated users.	●			
8.1.4 Remove/disable inactive user accounts within 90 days.	●			
8.1.5 Manage IDs used by third parties to access, support, or maintain system components via remote access as follows: • Enabled only during the time period needed and disabled when not in use • Monitored when in use	●			
8.1.6 Limit repeated access attempts by locking out the user ID after not more than six attempts.	●			
8.1.7 Set the lockout duration to a minimum of 30 minutes or until an administrator enables the user ID.	●			
8.1.8 If a session has been idle for more than 15 minutes, require the user to re-authenticate to re-activate the terminal or session.	●			
8.2 In addition to assigning a unique ID, ensure proper user-authentication management for non-consumer users and administrators on all system components by employing at least one of the following methods to authenticate all users: • Something you know, such as a password or passphrase • Something you have, such as a token device or smart card • Something you are, such as a biometric	●			

Requirement 8: Assign a unique ID to each person with computer access (cont.)	Control Reduction Automatically Provided			
	P2PE	E2EE	Tokenization	EMV
8.2.1 Using strong cryptography, render all authentication credentials (such as passwords/phrases) unreadable during transmission and storage on all system components.	●			
8.2.2 Verify user identity before modifying any authentication credential—for example, performing password resets, provisioning new tokens, or generating new keys.	●			
8.2.3 Passwords/passphrases must meet the following: • Require a minimum length of at least seven characters • Contain both numeric and alphabetic characters Alternatively, the passwords/passphrases must have complexity and strength at least equivalent to the parameters specified above.	●			
8.2.4 Change user passwords/passphrases at least once every 90 days.	●			
8.2.5 Do not allow an individual to submit a new password/passphrase that is the same as any of the last four passwords/passphrases he or she has used.	●			
8.2.6 Set passwords/passphrases for first-time use and upon reset to a unique value for each user, and change immediately after the first use.	●			
8.3 Secure all individual non-console administrative access and all remote access to the CDE using multi-factor authentication. Note: Multi-factor authentication requires that a minimum of two of the three authentication methods (see Requirement 8.2 for descriptions of authentication methods) be used for authentication. Using one factor twice (for example, using two separate passwords) is not considered multi-factor authentication.	●			
8.3.1 Incorporate multi-factor authentication for all non-console access into the CDE for personnel with administrative access.	●			
8.3.2 Incorporate multi-factor authentication for all remote network access (both user and administrator and including third party access for support or maintenance) originating from outside the entity's network.	●			
8.4 Document and communicate authentication policies and procedures to all users, including: • Guidance on selecting strong authentication credentials • Guidance for how users should protect their authentication credentials • Instructions not to reuse previously used passwords • Instructions to change passwords if there is any suspicion the password could be compromised	●			

Requirement 8: Assign a unique ID to each person with computer access (cont.)	Control Reduction Automatically Provided			
	P2PE	E2EE	Tokenization	EMV
8.5 Do not use group, shared, or generic IDs, passwords, or other authentication methods as follows: • Generic user IDs are disabled or removed • Shared user IDs do not exist for system administration and other critical functions • Shared and generic user IDs are not used to administer any system components	●			
8.5.1 Additional requirement for service providers only: Service providers with remote access to customer premises (for example, for support of POS systems or servers) must use a unique authentication credential (such as a password/phrase) for each customer. Note: This requirement is not intended to apply to shared hosting providers accessing their own hosting environment, where multiple customer environments are hosted.				
8.6 Where other authentication mechanisms are used (for example, physical or logical security tokens, smart cards, certificates, etc.), use of these mechanisms must be assigned as follows: • Authentication mechanisms must be assigned to an individual account and not shared among multiple accounts • Physical and/or logical controls must be in place to ensure only the intended account can use that mechanism to gain access	●			
8.7 All access to any database containing cardholder data (including access by applications, administrators, and all other users) is restricted as follows: • All user access to, user queries of, and user actions on databases are through programmatic methods • Only database administrators have the ability to directly access or query databases • Application IDs for database applications can only be used by the applications (and not by individual users or other non-application processes)	●			
8.8 Ensure that security policies and operational procedures for identification and authentication are documented, in use, and known to all affected parties.	●			
Requirement 9: Restrict physical access to cardholder data **Note:** For P2PE deployments, non-checked requirements (9.5, 9.5.1, 9.8 & 9.8) only apply for those merchants that have paper records with the Primary Account Number (PAN). For requirements 9.9 – 9.9.3, these requirements apply as they pertain to the physical protection of the ID Tech SREDKey POI device.	Control Reduction Automatically Provided			
	P2PE	E2EE	Tokenization	EMV
9.1 Use appropriate facility entry controls to limit and monitor physical access to systems in the cardholder data environment.	●			

Requirement 9: Restrict physical access to cardholder data (cont.) **Note:** For P2PE deployments, non-checked requirements (9.5, 9.5.1, 9.8 & 9.8) only apply for those merchants that have paper records with the Primary Account Number (PAN). For requirements 9.9 – 9.9.3, these requirements apply as they pertain to the physical protection of the ID Tech SREDKey POI device.	Control Reduction Automatically Provided			
	P2PE	**E2EE**	**Tokenization**	**EMV**
9.1.1 Use either video cameras or access control mechanisms (or both) to monitor individual physical access to sensitive areas. Review collected data and correlate with other entries. Store for at least three months, unless otherwise restricted by law. **Note:** "Sensitive areas" refers to any data center, server room or any area that houses systems that store, process, or transmit cardholder data. This excludes public-facing areas where only point-of-sale terminals are present, such as the cashier areas in a retail store.	●			
9.1.2 Implement physical and/or logical controls to restrict access to publicly accessible network jacks. For example, network jacks located in public areas and areas accessible to visitors could be disabled and only enabled when network access is explicitly authorized. Alternatively, processes could be implemented to ensure that visitors are escorted at all times in areas with active network jacks.	●			
9.1.3 Restrict physical access to wireless access points, gateways, handheld devices, networking/communications hardware, and telecommunication lines.	●			
9.2 Develop procedures to easily distinguish between onsite personnel and visitors, to include: • Identifying onsite personnel and visitors (for example, assigning badges) • Changes to access requirements • Revoking or terminating onsite personnel and expired visitor identification (such as ID badges)	●			
9.3 Control physical access for onsite personnel to sensitive areas as follows: • Access must be authorized and based on individual job function • Access is revoked immediately upon termination, and all physical access mechanisms, such as keys, access cards, etc., are returned or disabled.	●			
9.4 Implement procedures to identify and authorize visitors. Procedures should include the following:	●			
9.4.1 Visitors are authorized before entering, and escorted at all times within, areas where cardholder data is processed or maintained.	●			
9.4.2 Visitors are identified and given a badge or other identification that expires and that visibly distinguishes the visitors from onsite personnel.	●			
9.4.3 Visitors are asked to surrender the badge or identification before leaving the facility or at the date of expiration.	●			

Requirement 9: Restrict physical access to cardholder data (cont.) **Note:** For P2PE deployments, non-checked requirements (9.5, 9.5.1, 9.8 & 9.8) only apply for those merchants that have paper records with the Primary Account Number (PAN). For requirements 9.9 – 9.9.3, these requirements apply as they pertain to the physical protection of the ID Tech SREDKey POI device.	Control Reduction Automatically Provided			
	P2PE	**E2EE**	**Tokenization**	**EMV**
9.4.4 A visitor log is used to maintain a physical audit trail of visitor activity to the facility as well as computer rooms and data centers where cardholder data is stored or transmitted. Document the visitor's name, the firm represented, and the onsite personnel authorizing physical access on the log. Retain this log for a minimum of three months, unless otherwise restricted by law.	●			
9.5 Physically secure all media.				
9.5.1 Store media backups in a secure location, preferably an off-site facility, such as an alternate or backup site, or a commercial storage facility. Review the location's security at least annually.				
9.6 Maintain strict control over the internal or external distribution of any kind of media, including the following:	●			
9.6.1 Classify media so the sensitivity of the data can be determined.	●			
9.6.2 Send the media by secured courier or other delivery method that can be accurately tracked.	●			
9.6.3 Ensure management approves any and all media that is moved from a secured area (including when media is distributed to individuals).	●			
9.7 Maintain strict control over the storage and accessibility of media.	●			
9.7.1 Properly maintain inventory logs of all media and conduct media inventories at least annually.	●			
9.8 Destroy media when it is no longer needed for business or legal reasons as follows:				
9.8.1 Shred, incinerate, or pulp hard-copy materials so that cardholder data cannot be reconstructed. Secure storage containers used for materials that are to be destroyed.				
9.8.2 Render cardholder data on electronic media unrecoverable so that cardholder data cannot be reconstructed.	●			
9.9 Protect devices that capture payment card data via direct physical interaction with the card from tampering and substitution. **Note:** These requirements apply to card-reading devices used in card-present transactions (that is, card swipe or dip) at the point of sale. This requirement is not intended to apply to manual key-entry components such as computer keyboards and POS keypads.				

Requirement 9: Restrict physical access to cardholder data (cont.) **Note:** For P2PE deployments, non-checked requirements (9.5, 9.5.1, 9.8 & 9.8) only apply for those merchants that have paper records with the Primary Account Number (PAN). For requirements 9.9 – 9.9.3, these requirements apply as they pertain to the physical protection of the ID Tech SREDKey POI device.	Control Reduction Automatically Provided			
	P2PE	**E2EE**	**Tokenization**	**EMV**
9.9.1 Maintain an up-to-date list of devices. The list should include the following: • Make, model of device • Location of device (for example, the address of the site or facility where the device is located) • Device serial number or other method of unique identification				
9.9.2 Periodically inspect device surfaces to detect tampering (for example, addition of card skimmers to devices), or substitution (for example, by checking the serial number or other device characteristics to verify it has not been swapped with a fraudulent device). **Note:** Examples of signs that a device might have been tampered with or substituted include unexpected attachments or cables plugged into the device, missing or changed security labels, broken or differently colored casing, or changes to the serial number or other external markings.				
9.9.3 Provide training for personnel to be aware of attempted tampering or replacement of devices. Training should include the following: • Verify the identity of any third-party persons claiming to be repair or maintenance personnel, prior to granting them access to modify or troubleshoot devices • Do not install, replace, or return devices without verification • Be aware of suspicious behavior around devices (for example, attempts by unknown persons to unplug or open devices) • Report suspicious behavior and indications of device tampering or substitution to appropriate personnel (for example, to a manager or security officer)				
9.10 Ensure that security policies and operational procedures for restricting physical access to cardholder data are documented, in use, and known to all affected parties.				

Requirement 10: Track and monitor all access to network resources and cardholder data	Control Reduction Automatically Provided			
	P2PE	**E2EE**	**Tokenization**	**EMV**
10.1 Implement audit trails to link all access to system components to each individual user.	●			
10.2 Implement automated audit trails for all system components to reconstruct the following events:	●			
10.2.1 All individual user accesses to cardholder data	●			
10.2.2 All actions taken by any individual with root or administrative privileges	●			
10.2.3 Access to all audit trails	●			

Requirement 10: Track and monitor all access to network resources and cardholder data (cont.)	Control Reduction Automatically Provided			
	P2PE	E2EE	Tokenization	EMV
10.2.4 Invalid logical access attempts	●			
10.2.5 Use of and changes to identification and authentication mechanisms—including, but not limited to, creation of new accounts and elevation of privileges—and all changes, additions, or deletions to accounts with root or administrative privileges.	●			
10.2.6 Initialization, stopping, or pausing of the audit logs.	●			
10.2.7 Creation and deletion of system-level objects.	●			
10.3 Record at least the following audit trail entries for all system components for each event:	●			
10.3.1 User identification	●			
10.3.2 Type of event	●			
10.3.3 Date and time	●			
10.3.4 Success or failure indication	●			
10.3.5 Origination of event	●			
10.3.6 Identity or name of affected data, system component, or resource	●			
10.4 Using time-synchronization technology, synchronize all critical system clocks and times and ensure that the following is implemented for acquiring, distributing, and storing time. **Note:** One example of time synchronization technology is Network Time Protocol (NTP).	●			
10.4.1 Critical systems have the correct and consistent time.	●			
10.4.2 Time data is protected.	●			
10.4.3 Time settings are received from industry-accepted time sources.	●			
10.5 Secure audit trails so they cannot be altered.	●			
10.5.1 Limit viewing of audit trails to those with a job-related need.	●			
10.5.2 Protect audit trail files from unauthorized modifications.	●			
10.5.3 Promptly back up audit trail files to a centralized log server or media that is difficult to alter.	●			

Requirement 10: Track and monitor all access to network resources and cardholder data (cont.)	Control Reduction Automatically Provided			
	P2PE	**E2EE**	**Tokenization**	**EMV**
10.5.4 Write logs for external-facing technologies onto a secure, centralized, internal log server or media device.	●			
10.5.5 Use file integrity monitoring or change detection software on logs to ensure that existing log data cannot be changed without generating alerts (although new data being added should not cause an alert).	●			
10.6 Review logs and security events for all system components to identify anomalies or suspicious activity. **Note:** Log harvesting, parsing, and alerting tools may be used to meet this Requirement.	●			
10.6.1 Review the following at least daily: • All security events • Logs of all system components that store, process, or transmit CHD and/or SAD • Logs of all critical system components • Logs of all servers and system components that perform security functions (for example, firewalls, intrusion-detection systems/intrusion-prevention systems (IDS/IPS), authentication servers, e-commerce redirection servers, etc.)	●			
10.6.2 Review logs of all other system components periodically based on the organization's policies and risk management strategy, as determined by the organization's annual risk assessment.	●			
10.6.3 Follow up exceptions and anomalies identified during the review process.	●			
10.7 Retain audit trail history for at least one year, with a minimum of three months immediately available for analysis (for example, online, archived, or restorable from backup).	●			
10.8 Additional requirement for service providers only: Implement a process for the timely detection and reporting of failures of critical security control systems, including, but not limited to, failure of: • Firewalls • IDS/IPS • FIM • Anti-virus • Physical access controls • Logical access controls • Audit logging mechanisms • Segmentation controls (if used)				

Requirement 10: Track and monitor all access to network resources and cardholder data (cont.)	Control Reduction Automatically Provided			
	P2PE	**E2EE**	**Tokenization**	**EMV**
10.8.1 Additional requirement for service providers only: Respond to failures of any critical security controls in a timely manner. Processes for responding to failures in security controls must include: • Restoring security functions • Identifying and documenting the duration (date and time start to end) of the security failure • Identifying and documenting cause(s) of failure, including root cause, and documenting remediation required to address root cause • Identifying and addressing any security issues that arose during the failure • Performing a risk assessment to determine whether further actions are required as a result of the security failure • Implementing controls to prevent cause of failure from reoccurring • Resuming monitoring of security control				
10.9 Ensure that security policies and operational procedures for monitoring all access to network resources and cardholder data are documented, in use, and known to all affected parties.	●			

Requirement 11: Regularly test security systems and processes	Control Reduction Automatically Provided			
	P2PE	**E2EE**	**Tokenization**	**EMV**
11.1 Implement processes to test for the presence of wireless access points (802.11), and detect and identify all authorized and unauthorized wireless access points on a quarterly basis. **Note:** Methods that may be used in the process include, but are not limited to, wireless network scans, physical/logical inspections of system components and infrastructure, network access control (NAC), or wireless IDS/IPS. Whichever methods are used, they must be sufficient to detect and identify both authorized and unauthorized devices.	●			
11.1.1 Maintain an inventory of authorized wireless access points including a documented business justification.	●			
11.1.2 Implement incident response procedures in the event unauthorized wireless access points are detected.	●			
11.2 Run internal and external network vulnerability scans at least quarterly and after any significant change in the network (such as new system component installations, changes in network topology, firewall rule modifications, product upgrades). **Note:** Multiple scan reports can be combined for the quarterly scan process to show that all systems were scanned and all applicable vulnerabilities have been addressed. Additional documentation may be required to verify non-remediated vulnerabilities are in the process of being addressed. For initial PCI DSS compliance, it is not required that four quarters of passing scans be completed if the assessor verifies 1) the most recent scan result was a passing scan, 2) the entity has documented policies and procedures requiring quarterly scanning, and 3) vulnerabilities noted in the scan results have been corrected as shown in a re-scan(s). For subsequent years after the initial PCI DSS review, four quarters of passing scans must have occurred.	●			

Requirement 11: Regularly test security systems and processes (cont.)	Control Reduction Automatically Provided			
	P2PE	E2EE	Tokenization	EMV
11.2.1 Perform quarterly internal vulnerability scans. Address vulnerabilities and perform rescans to verify all "high risk" vulnerabilities are resolved in accordance with the entity's vulnerability ranking (per Requirement 6.1). Scans must be performed by qualified personnel.				
11.2.2 Perform quarterly external vulnerability scans, via an Approved Scanning Vendor (ASV) approved by the Payment Card Industry Security Standards Council (PCI SSC). Perform rescans as needed, until passing scans are achieved. **Note:** Quarterly external vulnerability scans must be performed by an Approved Scanning Vendor (ASV), approved by the Payment Card Industry Security Standards Council (PCI SSC). Refer to the ASV Program Guide published on the PCI SSC website for scan customer responsibilities, scan preparation, etc.	●			
11.2.3 Perform internal and external scans, and rescans as needed, after any significant change. Scans must be performed by qualified personnel.	●			
11.3 Implement a methodology for penetration testing that includes the following: • Is based on industry-accepted penetration testing approaches (for example, NIST SP800-115) • Includes coverage for the entire CDE perimeter and critical systems • Includes testing from both inside and outside the network • Includes testing to validate any segmentation and scope-reduction controls • Defines application-layer penetration tests to include, at a minimum, the vulnerabilities listed in Requirement 6.5 • Defines network-layer penetration tests to include components that support network functions as well as operating system • Includes review and consideration of threats and vulnerabilities experienced in the last 12 months • Specifies retention of penetration testing results and remediation activities results.	●			
11.3.1 Perform external penetration testing at least annually and after any significant infrastructure or application upgrade or modification (such as an operating system upgrade, a sub-network added to the environment, or a web server added to the environment).	●			
11.3.2 Perform internal penetration testing at least annually and after any significant infrastructure or application upgrade or modification (such as an operating system upgrade, a sub-network added to the environment, or a web server added to the environment).	●			
11.3.3 Exploitable vulnerabilities found during penetration testing are corrected and testing is repeated to verify the corrections.	●			
11.3.4 If segmentation is used to isolate the CDE from other networks, perform penetration tests at least annually and after any changes to segmentation controls/methods to verify that the segmentation methods are operational and effective, and isolate all out-of-scope systems from systems in the CDE.	●			

Requirement 11: Regularly test security systems and processes (cont.)	Control Reduction Automatically Provided			
	P2PE	**E2EE**	**Tokenization**	**EMV**
11.3.4.1 Additional requirement for service providers only: If segmentation is used, confirm PCI DSS scope by performing penetration testing on segmentation controls at least every six months and after any changes to segmentation controls/methods.				
11.4 Use intrusion detection and/or intrusion prevention techniques to detect and/or prevent intrusions into the network. Monitor all traffic at the perimeter of the cardholder data environment as well as at critical points in the cardholder data environment, and alert personnel to suspected compromises. Keep all intrusion detection and prevention engines, baselines, and signatures up to date.	●			
11.5 Deploy a change detection mechanism (for example, file-integrity monitoring tools) to alert personnel to unauthorized modification (including changes, additions, and deletions) of critical system files, configuration files, or content files; and configure the software to perform critical file comparisons at least weekly. **Note:** For change detection purposes, critical files are usually those that do not regularly change, but the modification of which could indicate a system compromise or risk of compromise. Change detection mechanisms such as file integrity monitoring products usually come pre-configured with critical files for the related operating system. Other critical files, such as those for custom applications, must be evaluated and defined by the entity (that is, the merchant or service provider).	●			
11.5.1 Implement a process to respond to any alerts generated by the change detection solution.	●			
11.6 Ensure that security policies and operational procedures for security monitoring and testing are documented, in use, and known to all affected parties.	●			

Requirement 12: Maintain a policy that addresses information security for all personnel	Control Reduction Automatically Provided			
	P2PE	**E2EE**	**Tokenization**	**EMV**
12.1 Establish, publish, maintain, and disseminate a security policy.				
12.1.1 Review the security policy at least annually and update the policy when the environment changes.				
12.2 Implement a risk-assessment process that: • Is performed at least annually and upon significant changes to the environment (for example, acquisition, merger, relocation, etc.), • Identifies critical assets, threats, and vulnerabilities, and • Results in a formal, documented analysis of risk. Examples of risk-assessment methodologies include but are not limited to OCTAVE, ISO 27005 and NIST SP 800-30.	●			

Requirement 12: Maintain a policy that addresses information security for all personnel (cont.)	Control Reduction Automatically Provided			
	P2PE	**E2EE**	**Tokenization**	**EMV**
12.3 Develop usage policies for critical technologies and define proper use of these technologies. **Note:** Examples of critical technologies include, but are not limited to, remote access and wireless technologies, laptops, tablets, removable electronic media, e-mail usage and Internet usage. Ensure these usage policies require the following:	●			
12.3.1 Explicit approval by authorized parties.	●			
12.3.2 Authentication for use of the technology.	●			
12.3.3 A list of all such devices and personnel with access.	●			
12.3.4 A method to accurately and readily determine owner, contact information, and purpose (for example, labeling, coding, and/or inventorying of devices)	●			
12.3.5 Acceptable uses of the technology.	●			
12.3.6 Acceptable network locations for the technologies.	●			
12.3.7 List of company-approved products.	●			
12.3.8 Automatic disconnect of sessions for remote access technologies after a specific period of inactivity.	●			
12.3.9 Activation of remote access technologies for vendors and business partners only when needed by vendors and business partners, with immediate deactivation after use.	●			
12.3.10 For personnel accessing cardholder data via remote access technologies, prohibit the copying, moving, and storage of cardholder data onto local hard drives and removable electronic media, unless explicitly authorized for a defined business need. Where there is an authorized business need, the usage policies must require the data be protected in accordance with all applicable PCI DSS Requirements.	●			
12.4 Ensure that the security policy and procedures clearly define information security responsibilities for all personnel.				

12.4.1 Additional requirement for service providers only: Executive management shall establish responsibility for the protection of cardholder data and a PCI DSS compliance program to include:
  • Overall accountability for maintaining PCI DSS compliance
  • Defining a charter for a PCI DSS compliance program and communication to executive management				

Requirement 12: Maintain a policy that addresses information security for all personnel (cont.)	Control Reduction Automatically Provided			
	P2PE	E2EE	Tokenization	EMV
12.5 Assign to an individual or team the following information security management responsibilities:				
12.5.1 Establish, document, and distribute security policies and procedures.	●			
12.5.2 Monitor and analyze security alerts and information and distribute to appropriate personnel.	●			
12.5.3 Establish, document, and distribute security incident response and escalation procedures to ensure timely and effective handling of all situations.				
12.5.4 Administer user accounts, including additions, deletions, and modifications.	●			
12.5.5 Monitor and control all access to data.	●			
12.6 Implement a formal security awareness program to make all personnel aware of the cardholder data security policy and procedures.				
12.6.1 Educate personnel upon hire and at least annually. Note: Methods can vary depending on the role of the personnel and their level of access to the cardholder data.				
12.6.2 Require personnel to acknowledge at least annually that they have read and understood the security policy and procedures.				
12.7 Screen potential personnel prior to hire to minimize the risk of attacks from internal sources. (Examples of background checks include previous employment history, criminal record, credit history, and reference checks.) **Note:** For those potential personnel to be hired for certain positions such as store cashiers who only have access to one card number at a time when facilitating a transaction, this requirement is a recommendation only.	●			
12.8 Maintain and implement policies and procedures to manage service providers, with whom cardholder data is shared, or that could affect the security of cardholder data, as follows:				
12.8.1 Maintain a list of service providers including a description of the service provided.				
12.8.2 Maintain a written agreement that includes an acknowledgement that the service providers are responsible for the security of cardholder data the service providers possess or otherwise store, process or transmit on behalf of the customer, or to the extent that they could impact the security of the customer's cardholder data environment. **Note:** The exact wording of an acknowledgement will depend on the agreement between the two parties, the details of the service being provided, and the responsibilities assigned to each party. The acknowledgement does not have to include the exact wording provided in this requirement.				

Requirement 12: Maintain a policy that addresses information security for all personnel (cont.)	Control Reduction Automatically Provided			
	P2PE	E2EE	Tokenization	EMV
12.8.3 Ensure there is an established process for engaging service providers including proper due diligence prior to engagement.				
12.8.4 Maintain a program to monitor service providers' PCI DSS compliance status at least annually.				
12.8.5 Maintain information about which PCI DSS requirements are managed by each service provider, and which are managed by the entity.				
12.9 Additional requirement for service providers only: Service providers acknowledge in writing to customers that they are responsible for the security of cardholder data the service provider possesses or otherwise stores, processes, or transmits on behalf of the customer, or to the extent that they could impact the security of the customer's cardholder data environment. **Note:** The exact wording of an acknowledgement will depend on the agreement between the two parties, the details of the service being provided, and the responsibilities assigned to each party. The acknowledgement does not have to include the exact wording provided in this requirement.				
12.10 Implement an incident response plan. Be prepared to respond immediately to a system breach.				
12.10.1 Create the incident response plan to be implemented in the event of system breach. Ensure the plan addresses the following, at a minimum: • Roles, responsibilities, and communication and contact strategies in the event of a compromise including notification of the payment brands, at a minimum • Specific incident response procedures • Business recovery and continuity procedures • Data backup processes • Analysis of legal requirements for reporting compromises • Coverage and responses of all critical system components • Reference or inclusion of incident response procedures from the payment brands				
12.10.2 Review and test the plan, including all elements listed in Requirement 12.10.1, at least annually.	●			
12.10.3 Designate specific personnel to be available on a 24/7 basis to respond to alerts.	●			
12.10.4 Provide appropriate training to staff with security breach response responsibilities.	●			
12.10.5 Include alerts from security monitoring systems, including but not limited to intrusion-detection, intrusion-prevention, firewalls, and file-integrity monitoring systems.	●			
12.10.6 Develop a process to modify and evolve the incident response plan according to lessons learned and to incorporate industry developments.	●			

Requirement 12: Maintain a policy that addresses information security for all personnel (cont.)	Control Reduction Automatically Provided			
	P2PE	E2EE	Tokenization	EMV
12.11 Additional requirement for service providers only: Perform reviews at least quarterly to confirm personnel are following security policies and operational procedures. Reviews must cover the following processes: • Daily log reviews • Firewall rule-set reviews • Applying configuration standards to new systems • Responding to security alerts • Change management processes				
12.11.1 Additional requirement for service providers only: Maintain documentation of quarterly review process to include: • Documenting results of the reviews • Review and signoff of results by personnel assigned responsibility for the PCI DSS compliance program				