Emerging Technology Whitepaper

Initial Roadmap: Point-to-Point Encryption Technology and PCI DSS Compliance

For Transmissions of Cardholder Data and Sensitive Authentication Data

Program Guide
Version 1.0

October 5, 2010

Table of Contents

Preface

Intended Audience

This document is written for the merchant perspective but is applicable to any payment industry stakeholder, including merchants, payment processors, acquirers, service providers, assessors, and solution vendors. It provides guidance for considering point-to-point encryption (P2PE) solutions and how they may simplify compliance efforts with the Payment Card Industry Data Security Standard (PCI DSS).

This document discusses P2PE solutions as applied to the payments industry. It provides an overview of the relevant components of a P2PE solution and the threat landscape that still exists with those solutions, including current challenges for validation. As a Program Guide, it does not cover every permutation of P2PE. The document concludes by suggesting future opportunities to enhance confidence in the validation of P2PE solutions for cardholder data environments.

Description of Document	
What this document IS	**What this document IS NOT**
An overview of the subject of P2PE offered to the community for critical consideration.	A detailed and exhaustive analysis of P2PE and how to validate proper deployment with specific testing criteria for laboratories and assessors.
An initial inspection of the P2PE components and how they may affect the encrypted cardholder data as it is *transmitted* through a cardholder data environment.	An analysis of how P2PE components may affect *stored* encrypted cardholder data.
A document written from the perspective of merchants who may be considering P2PE to improve their security posture and potentially reduce their compliance effort.	A document written from a vendor's point of view, although vendors and other stakeholders will benefit from understanding the merchant perspective.

The Payment Card Industry Security Standards Council (PCI SSC) is drafting an additional document tentatively titled *Validation Requirements for Point-to-Point Encryption*. It will define requirements and the process for validating effective P2PE solutions. Its intended audience is vendors, assessors, and labs that may evaluate the testing procedures associated with key management, segregation of duties, access controls, and other necessary criteria.

1 Executive Summary

1.1 Objective

This is the first in a series of documents to cover the use of encryption as it relates to PCI DSS and scope reduction. This roadmap document identifies common components involved in point-to-point encryption (P2PE) technology that may simplify the PCI DSS compliance validation process. It proposes how this technology may reduce the cardholder data environment (CDE) by enumerating both security principles and implementation risks involved from the point of encryption to the point of decryption.

The purpose of this document is to help payment industry stakeholders in critically evaluating whether point-to-point encryption solutions may simplify PCI DSS compliance for their environment. The scope of this document relates only to *transmitted* cardholder or sensitive authentication data, and the impact on PCI DSS scope for a P2PE solution that encrypts this transmitted data. It does not cover or address *stored* encrypted cardholder data (CHD).

This document also does not detail the requirements any given P2PE solution should satisfy. This document must not be used to validate current P2PE solutions. A companion document entitled *Validation Requirements for Point-to-Point Encryption* will describe the validation requirements for P2PE solutions; it will be released for comment to Participating Organizations in 2011.

1.2 Description and Definition of Point-to-Point Encryption

Encryption is the algorithmic process of transforming plaintext into unreadable ciphertext, and is the core technology for solutions discussed in this paper. Point-to-point encryption (P2PE) includes people, processes and technology in place to encrypt and decrypt transmitted cardholder or sensitive authentication data.

Encryption occurs at one designated and independently validated encryption device or location in a card transaction (the source or encryption point), and the data is subsequently sent as unreadable ciphertext for decryption to another designated and independently validated decryption device or location (the destination or decryption point). The data remains encrypted between the source and the destination, with no decryption of the data feasible at any point between the source and the destination.

The presumption of P2PE is that cardholder data in transit is protected when it is encrypted to the extent that an entity in possession of the ciphertext alone cannot reverse the encryption process.

1.3 Scope of Point-to-Point Encryption

A P2PE solution that encrypts CHD transmissions throughout the merchant environment and uses comprehensive cryptographic and key management systems results in a scenario where the merchant has limited or no access to plaintext CHD. This may simplify the merchant's PCI DSS compliance effort by reducing the system components considered part of the cardholder data environment. As part of this redefined scope, it is essential that merchants understand their entire card transaction environment and ensure that all cardholder and sensitive authentication data is identified, that there is a realistic understanding of the threats, and that the organizational security posture and risk management are appropriate.

For a merchant to adequately determine scoping considerations, it is essential that data discovery methods are part of the design and implementation of a P2PE solution. The result of the data discover exercise must demonstrate no leakage of CHD between system components classified as part of the newly defined P2PE cardholder data environment and those system components that are no longer required to validate PCI DSS compliance.

Note: In reading this document, it is important that scope reduction in the context of P2PE does not imply that a merchant's networks should no longer implement protective controls outside of those provided by the P2PE solution itself. PCI DSS should still be considered as a security best practice to effectively secure a merchant environment.

To maximize the benefit of P2PE, the transmissions should be encrypted in a secure and tamper-resistant module at the initial Point of Interaction (POI) device in the merchant environment with these provisions:

- Encryption is performed immediately after reading the data through contact-based (EMV), magnetic stripe, contactless, PAN key entry or Near Field Communication [NFC] methods.
- The portions of the merchant environment that no longer require validation have no access to: plaintext CHD, cryptographic keys, or a decryption function that would allow encrypted data to be decrypted.
- CHD (including any sensitive authentication data) cannot be decrypted until received by a validated decryption point such as a segmented portion of the merchant network or processor/acquirer network.
- P2PE solutions including devices, key management practices, and encryption and decryption environments are independently validated.

1.4 Conclusions

This paper provides four conclusions for the use of P2PE and compliance with PCI DSS:

- Methods of validating P2PE solutions and implementations are immature. This presents opportunity for standardization of the technology and validation processes to ensure consistent and robust security practices are followed by developers, implementers, and administrators.
- A properly deployed P2PE solution will simplify PCI DSS compliance for transmissions of cardholder data within a merchant environment so long as it meets well defined and validated testing procedures.
- P2PE solutions will not eliminate the need to maintain and validate PCI DSS compliance, but may simplify validation efforts by reducing the number of system components to which PCI DSS applies.
- Independent validation of P2PE solutions is required and will be based on additional guidance and/or testing criteria for the encryption and decryption environments to be provided by PCI SSC.

1.5 Future Actions by PCI SSC

The PCI SSC is positioned to provide additional guidance and will consider the following:

- Provide additional guidance and awareness opportunities such as webinars, Internal Security Assessor (ISA) and Qualified Security Assessor (QSA) training, face-to-face meetings and speaking events
- Develop and promote standards to determine appropriate parameters and testing procedures for the points of encryption and decryption
- Extend the PCI PTS POI Modular Security Requirements to allow assessment and approval of non-PIN-based POI devices via independent lab validation
- Formalize testing criteria based on new standards for independent lab validation or qualified assessment of implementation
- Consider tools for merchants, such as a list of qualified P2PE solutions and/or revised Self-Assessment Questionnaires
- Train assessors to evaluate all relevant P2PE elements, including components, documentation, and implementation
- Identify and qualify independent third party evaluators, if applicable

2 Roles and Responsibilities

Depending on the specific architecture and implementation of a particular P2PE solution, there may be transference of responsibilities between the various stakeholders described below.

2.1 P2PE Solution Providers

The P2PE solution provider has the overall responsibility for the design of an effective P2PE solution appropriate for a specific merchant environment. This could include integration concerns over compatibility with currently deployed technologies within the merchant environment. In addition, the solution provider is ultimately responsible for ensuring: validation of device security, point of decryption security, device management, cryptographic considerations have been met, that appropriate monitoring is in place and that a P2PE supplementary document is developed to assist merchants deploying the technology and assessors validating the implementation. Any security-related function that a solution provider implements or outsources in support of the P2PE solution must be assessed by an independent party.

2.2 Vendors

A vendor submits a POI device for evaluation to an independent PCI or card scheme-approved security laboratory. Vendors must develop a supplement document describing the secure operation and administration of their equipment to assist merchants and solution providers.

2.3 Merchants

The entity implementing a P2PE solution must ensure that the device is physically and logically secured consistent with the P2PE solution provider's implementation guidance. If the solution provider permits the entity to configure the device, the entity must follow configuration change control guidance provided by the solution provider and validate appropriate deployment.

If network segmentation controls are not part of the vendor-supplied device, the merchant is responsible for the segmentation controls and to ensure that they are implemented consistent with PCI DSS. Any device not segmented from the point of encryption shall remain in scope for PCI DSS. The adequacy of the segmentation controls and the validation of the devices' continued physical and logical security are to be validated by an independent and approved assessor in accordance with the forthcoming *Validation Requirements for Point-to-Point Encryption.*

3 How P2PE Can Simplify PCI DSS Compliance

3.1 Establishing Parameters of Scope Reduction

The PCI DSS applies to all system components within the cardholder data environment (CDE). The CDE includes every system that may store, process, or transmit cardholder data and other systems connected to these systems. To limit the scope of a PCI DSS assessment, many organizations seek to minimize the number of system components within a given network that have access to cardholder data. This may be achieved by eliminating and consolidating unnecessary data or through the use of appropriate network segmentation to isolate a properly defined CDE from other system components. As a result, the other system components cannot negatively affect the security of the CDE.

Similarly, encryption may help minimize the accessibility to cardholder data; however, encryption alone is not sufficient for PCI DSS compliance.

Encryption solutions are only as good as the industry-approved algorithms and key management practices used, including security controls surrounding the encryption/decryption keys ("Keys"). If Keys are left unprotected and accessible, anyone can decrypt the data. The PCI DSS has specific encryption key management controls (PCI DSS Requirements 3.5 and 3.6), however, other PCI DSS controls such as firewalls, user access controls, vulnerability management, scanning, logging and application security provide additional layers of security to prevent malicious users from gaining privileged access to networks or cardholder data environments that may grant them access to Keys. It is for this reason that encrypted cardholder data is in scope for PCI DSS.

3.2 Can a P2PE Solution Simplify PCI DSS Compliance?

Many stakeholders are seeking to implement a P2PE solution where system components that simply process and transmit encrypted data, are adequately isolated from the encryption and decryption environments, and have no ability to decrypt the data be excluded from the scope of a PCI DSS review.

The PCI SSC has previously clarified that encrypted data is out of scope if, and only if, it has been validated that the entity that possesses encrypted cardholder data does not have the means to decrypt it.[1] However, if an entity can validate that the encryption and decryption environments and methods used meet industry best practices included in the forthcoming *Validation Requirements for Point-to-Point Encryption,* then an entity may consider their CDE reduced to the encryption and/or decryption environments, subject to validation.

3.3 Scope for Networks that Transmit Encrypted Cardholder Data

As encrypted data flows over a network, a primary risk is that someone might decrypt it by either accessing secret or private keys or gaining access to the decryption function. Encrypted data in transit and system components over which it flows may be excluded from a PCI DSS assessment provided that the risk is addressed and the testing procedures in the forthcoming *Validation Requirements for Point-to-Point Encryption* have been met. Requirements include but are not limited to adequate segregation of duties, network segmentation, and strong access control.

[1] *Article #10359 on the PCI-SSC FAQ website.*

4 Components of P2PE Technology

When critically examining any P2PE solution, it is important for the merchant to consider all P2PE components. These include the technologies and mechanisms enabling how the cardholder data is accepted, and how the transaction progresses through the merchant environment – including transmission to the processor/acquirer. The P2PE solution must address potential attack vectors against each component and provide the merchant with the ability to confirm with confidence that associated risks have been addressed.

4.1 P2PE Domains

P2PE domains are the areas where specific controls need to be applied and validated. These domains may be managed and controlled by separate entities.

The forthcoming *Validation Requirements for Point-to-Point Encryption* will specify requirements and validation procedures for at least the following key domains:

- Encryption device
- Payment Application if applicable
- Merchant encryption environment, which includes all elements still subject to PCI DSS validation
- Encryption and decryption operations and key management
- Decryption environment
- Enhanced key management practices for the decryption environment

These domains are introduced below; further details will appear in the forthcoming *Validation Requirements for Point-to-Point Encryption*.

4.2 Encryption Device

In general, the data that must be encrypted includes the full primary account number (PAN) and sensitive authentication data (SAD).

Implementing an encryption function within the POI device requires security against both physical and logical compromise – including properly managing, storing, and protecting cryptographic keys. The considerations applicable to any device performing encryption of CHD or sensitive authentication data with the goal of simplifying PCI DSS validation scope include but are not limited to the following:

- Appropriateness of algorithm choice, key size, key lifetime, etc.
- How the confidentiality of secret and private keys is ensured
- How integrity and authenticity of public keys are maintained
- Physical security and tamper resistance of the device
- How integrity of software components and services is maintained (including integrity of any updates)
- Generation of audit events
- Physical penetration testing
- How side channel analysis is prevented

- Verification that plaintext data is not output from the device
- How access to plaintext account data prior to encryption is prevented by the POI device
- Device administration, including administration of cryptographic keys
- Thorough documentation by the developer to assure appropriate installation

4.3 Payment Application (if applicable)

An application that has access to plaintext data would still require validation. For example, consider when the secure controller within a POI device operating in encryption mode releases plaintext account data to an authenticated application within the device. In this example, the application with access to plaintext account data should undergo validation, such as a PA-DSS assessment.

4.4 Merchant Encryption Environment

Within the context of a given solution, the merchant, in consultation with its acquirer, should ensure the adequacy of physical or logical controls and any segmentation controls if these controls are not part of the supplied solution.

Where possible, the merchant should ensure that its devices are inspected on a regular basis for signs of tampering in-line with the guidance provided by the P2PE solution provider. The encryption environment would be required to satisfy the *Validation Requirements for Point-to-Point Encryption* and undergo an annual PCI DSS assessment.

4.5 Encryption and Decryption Operations (if applicable)

Encryption and decryption operations must be validated if merchants make the business decision to both encrypt and decrypt the data for use within their own networks.

4.6 Decryption Environment

A critical point of security is the environment where cardholder data is returned to plaintext by decryption. To ensure that any systems responsible for key management operations are developed and implemented securely, the key management function and the environment into which it is deployed must satisfy the *Validation Requirements for Point-to-Point Encryption* and undergo an annual PCI DSS assessment.

4.7 Enhanced Key Management Practices

Management of cryptographic keys is fundamental to the security of a P2PE solution. An exploit of a single POI device should not compromise the security of all encrypted data originating from a merchant environment. For example, cryptographic keys used to protect account data cannot be used to verify the authenticity of a software update.

In the *Validation Requirements for Point-to-Point Encryption,* PCI SSC will include enhanced key management procedures derived from existing industry standards for PIN key management. These procedures will include criteria for managing keys and performing decryption functions, including but not limited to key: generation, loading, distribution, usage, administration, injection, revocation, retirement, and archival.

5 Considerations for Compliance

5.1 Selection of a Point-to-Point Encryption Solution

The processing of encrypted cardholder data should be as simple for a merchant as selecting an independently tested solution and validating that the solution has been implemented according to set requirements. However, several factors should be considered as the merchant selects a P2PE solution. Note that many of these are the same factors that must be considered prior to selecting and implementing any major new technology.

5.1.1 **POI device selection**

Independent laboratories should evaluate the effectiveness of the encryption solution and the ability to attack the physical and logical characteristics inherent in POI devices. This can simplify the merchant selection process and minimizes the cost associated with validation for merchants. It also provides a consistent approach to determining an appropriate level of preventative controls.

The POI devices should have tamper-resistant protection and prevent the processing of transactions if the integrity of the algorithm or key length, or key authenticity cannot be verified. The POI device should also have undergone penetration testing for physical and logical threats.

5.1.2 **Method of encryption**

In maintaining the operational security of a P2PE solution, the method of encryption requires close consideration. For instance, where encryption is carried out using asymmetric techniques, knowledge of the public key does not provide access to the decryption capability; however, the solution must ensure the integrity and authenticity of such keys. Where encryption is carried out using symmetric encryption, the solution must additionally ensure the confidentiality of these keys.

5.1.3 **Vendor lock-in**

As with any new technology, there is risk of non-interoperability with a variety of acquirer and/or processor systems. Prior to selecting a solution, a merchant should evaluate its migration plans, including potential corporate acquisitions or mergers. The solution should offer flexibility and mobility for the various types of transactions within the organization.

5.1.4 **Enterprise architecture and operations**

Similar to vendor lock-in are the architectural design and operations of the enterprise. Selection of the solution should include future business operations such as loyalty programs and technology upgrades that may affect the encryption and transmission of cardholder data. Note how the solution deals with operational issues such as the treatment of truncated PANs.

5.1.5 **Industry standards**

The lack of industry standards poses challenges for selecting a P2PE solution today. The *Validation Requirements for Point-to-Point Encryption* will set requirements in the selection of a solution that meets the expected level of security and validation confidence.

5.2 Threats to P2PE Solutions

To ensure that a P2PE solution effectively minimizes risk, it is important to first understand the risk to cardholder data within these environments, including:

- The risk that plaintext CHD will be intercepted prior to encryption by circumventing security controls at the point of interaction (POI)
- The risk that plaintext CHD will be intercepted after decryption by circumventing security controls at the point of decryption
- The risk that an attacker will obtain decryption keys. This risk grows when an organization retains keys to decrypt ciphertext
- The risks posed by inadequate key management. Encryption and decryption keys must be protected with robust key management practices including key generation, loading, distribution, usage, administration, and injection

The potential for exposure of cardholder data via a breach remains as long as the PAN and other sensitive cardholder data is of value and is present – even in encrypted form.

The following summarizes merchant transaction processing or storage scenarios that pose risks even for P2PE solutions, since access to plaintext data can occur. Merchants should evaluate their environments carefully for these types of scenarios and ensure that any plaintext cardholder data is adequately protected.

5.2.1 Technical fallback to non-encrypted transactions

If the POI device falls back to non-encrypted output for payment card transactions, any part of the merchant environment that transmits, processes or stores the plaintext CHD is still a part of the CDE and is in scope for PCI DSS compliance.[2]

5.2.2 Legacy cardholder data

Any legacy data and processes (such as billing, loyalty, or marketing databases) within the merchant's environment that may still store, process or transmit plaintext CHD remain in scope for PCI DSS. Entities should have an ongoing data discovery methodology to demonstrate that legacy information is not resident in the environment before considering whether the footprint of the CDE can be reduced by a P2PE implementation.

5.2.3 Card white-listing

In cases where a merchant issues a pre-paid “gift” card or where a non-card scheme card is used, that card’s account data may need to be exported in plaintext form. A device may implement a white-listing approach to prevent these cards from being encrypted prior to output.

White-listing presents a significant threat to the security of a P2PE solution, should the white-listing process be subverted. For this reason, the entity operating the white-listing should be subject to PCI DSS review.

[2] In a P2PE scenario, the point of decryption should have appropriate auditing and detection capabilities in place such that improper (e.g., unencrypted) output from a POI device is detected and appropriate action is taken.

5.2.4 Transaction conducted using physical impression from embossed card

The physical impression taken during a card-present transaction must at some point be converted to electronic data for transmission to the acquirer/processor. Use of encryption at the point of data entry and electronic conversion can produce benefits and significantly reduce the scope of the CDE, but there will still be points at which CHD is available in plaintext form. PCI DSS validation scope is unchanged until the data is encrypted.

5.2.5 Merchant obtains CHD through other means

Should a merchant later obtain plaintext CHD from an acquirer/processor as part of dispute resolution or chargeback processing, this data remains in scope of PCI DSS.

6 Roadmap for Future Validation

Point-to-point encryption provides the ability for merchants to simplify their PCI DSS compliance effort by limiting the system components that transmit plaintext cardholder data. However, confidence must exist that the tools, processes, systems, and/or the third-party providers that offer these services can be trusted.

The summary of future steps below creates a framework for validating the effectiveness of point-to-point encryption solutions. The steps will help simplify PCI DSS compliance efforts and provide criteria to demonstrate appropriate security.

Separately, in an effort to demonstrate transparency, the PCI SSC will publish an associated timeline for all activities referenced in this section and update the projected deliverables regularly. Note that many items in this section are currently under consideration, with future developments and project deliverables yet to come.

For merchants deploying a P2PE solution, several opportunities exist for PCI SSC to work with key stakeholders to develop requirements, programs and processes that can help assure that merchants have minimized risk to cardholder data within their environment. These opportunities include:

- Guidance and awareness
- Use of standards as basis for P2PE criteria
- Independent technology validation
- Environmental validation of implementation

6.1 Guidance and Awareness

In order to make informed decisions, merchants need appropriate information to determine whether their unique environments may benefit from P2PE. The following will help improve P2PE awareness and solution selection in the future.

6.1.1 SRED/P2PE guidelines

This paper, the forthcoming *Validation Requirements for Point-to-Point Encryption,* and the Secure Read and Exchange of Data (SRED) POI module within the PIN Transaction Security framework will provide guidance for merchants, vendors, and QSAs to understand the requirements for securing the point of interaction. Additional guidance will be considered for laboratories that assess SRED, and for QSAs that may assess the security of P2PE implementations and relevant components such as key management. The SRED module requirements can be found on the PCI SSC website at https://www.pcisecuritystandards.org/.

6.1.2 Additional training – merchants

PCI SSC will develop additional training to provide context around point-to-point encryption and opportunities for discussion – possibly as an extension of the Internal Security Assessor or the Standards Training program currently offered.

6.1.3 Additional training – labs and assessors

PCI SSC may develop additional training for both PTS labs and QSAs to ensure that they fully understand the intent of the P2PE requirements and can execute their portion of the overall compliance assessment. PCI SSC will evaluate training that allows assessors to demonstrate knowledge of not only P2PE but fundamental cryptography knowledge as well.

6.1.4 Revised Self-Assessment Questionnaire (SAQ)

Merchants who use a P2PE solution to simplify their PCI DSS validation will potentially have a different set of concerns than what is addressed in current SAQ forms. Accordingly, PCI SSC will review and revise merchant SAQs as needed to facilitate assessments of common P2PE implementations.

6.2 Standards

To create consistency of implementation for any P2PE solution, there must be standards that help set parameters for the technology and provide procedures for testing that requirements have been achieved. PCI SSC will consider the following standards for ongoing development and/or for coordination with other recognized standards bodies.

6.2.1 Point of encryption (SRED)

The SRED module will be a validation requirement for all POI devices as originating endpoints.

6.2.2 Point of encryption (non-PIN acceptance device)

The PCI SSC will consider an evaluation option (similar to the SRED module) to allow non-PIN acceptance devices that do not currently qualify for SRED evaluation.

6.2.3 Enhanced key management

Based on analysis of PCI DSS key management requirements and existing standards for PIN key management, PCI SSC will develop a key management standard and attestation of compliance to be required for each P2PE deployment.

6.2.4 Expanded scope of PTS and PA-DSS

The PCI SSC will consider additional security requirements for POI devices and embedded payment applications as needed to facilitate P2PE solutions within the PTS and PA-DSS standards.

6.2.5 Changes in acceptable cryptographic algorithms

The PCI SSC will continue to review the current acceptable symmetric and asymmetric algorithms as well as key bit lengths to provide new guidance well in advance of any changes. This is necessary so that both producers and consumers/users of encryption technology can ensure that the equipment that is in use and planned for new deployment will be sufficiently resistant to attack for the duration of its planned deployment.

6.3 Technology Certification

For merchants and other entities to have confidence in the selection of a P2PE solution designed to minimize the scope of the CDE, independent validation of P2PE technology may be required. Some potential areas for independent validation under consideration include:

6.3.1 **Validation program for originating endpoint**

The PTS POI SRED module establishes security requirements for POI devices to protect account data through encryption. PCI SSC will monitor SRED in coordination with the PTS laboratories evaluating the criteria to determine whether the requirements have exhaustively addressed all security concerns or whether additional requirements should be included in future releases. POI devices listed on the PCI SSC website will indicate whether the SRED module has been approved as part of the lab evaluation.

6.3.2 **P2PE solution validation**

After the development of validation requirements for point-to-point encryption, the PCI SSC will consider establishing a program for validating comprehensive P2PE solutions. This "complete package" program may include existing programs such as PCI DSS, PA-DSS, or PTS POI (or expansions of these standards if needed). The PCI SSC will evaluate publishing a list of compliant solutions, where PTS labs, QSAs and possibly other assessors each validate components (devices, processors, termination points, etc.) of the solution.

6.4 Environment

Technology is not the only area requiring validation. The environment where the technology is deployed should also be evaluated. Potential areas for environmental validation include:

6.4.1 **QSA training to validate P2PE environments**

QSAs should receive training for evaluating any P2PE deployment to determine whether system components can be removed from validation scope. The PCI SSC will consider potential additional course material regarding how to appropriately assess certain technology that may simplify compliance. This effort may result in a separate qualification for those professionals that specialize in these technologies.

6.4.2 **Validation of implementers**

The PCI SSC is considering training and qualification of those entities that implement P2PE solutions on behalf of another entity. One example is an implementer that provides appropriate key management and CHD security on behalf of another entity. Implementers may be required to demonstrate understanding of the PCI DSS and relevant requirements prior to installation in new environments.