Payment Card Industry (PCI)

Additional Security Requirements for Token Service Providers (EMV Payment Tokens)

Frequently Asked Questions

December 2015

Introductory Note

This document addresses frequently asked questions (FAQs) related to the PCI SSC *Additional Security Requirements and Assessment Procedures for Token Service Providers (EMV Payment Tokens), Version 1.0*. Throughout this FAQ document:

- The use of "PCI TSP Security Requirements" refers to the *Additional Security Requirements and Assessment Procedures for Token Service Providers (EMV Payment Tokens) Version 1.0*, as published on the PCI SSC website (www.pcisecuritystandards.org).
- The use of "EMVCo Technical Framework" refers to the *EMV® Payment Tokenisation Specification – Technical Framework*, as published by EMVCo (www.emvco.com).
- "TSP" is a PCI SSC-defined acronym that refers to and aligns with the EMVCo-defined term "Token Service Provider"

Further information about use and applicability of the PCI TSP Security Requirements can be found in the "Introduction", "Terminology", and "Scope of Requirements" sections within the document itself.

FAQs for PCI TSP Security Requirements

Q 1. Who is required to comply with the PCI TSP Security Requirements?

A: *Compliance programs for the PCI TSP Security Requirements, including which entities need to validate and validation procedures, are managed by the payment brands. Entities that are registered as Token Service Providers by EMVCo should confirm their compliance and validation requirements with the applicable payment brand(s).*

Q 2. When are the PCI TSP Security Requirements effective?

A: *The TSP Security Requirements are active upon publication. Effective dates for compliance to TSP Security Requirements are defined by the payment brands. Any queries about validating compliance to the TSP Security Requirements should be directed to the applicable payment brand(s).*

Q 3. What is the relationship between PCI DSS and the PCI TSP Security Requirements?

A: *The PCI TSP Security Requirements build on and are additional to those in PCI DSS. Both the PCI DSS and TSP Security Requirements apply to the TSP's token data environment.*

Q 4. What is the relationship between the EMVCo Technical Framework and the PCI TSP Security Requirements?

A: *The EMVCo Technical Framework defines technical requirements for interoperable tokenization solutions for Payment Tokens. The specification defines the key roles and data fields associated with Payment Token requests, issuance, provisioning, transaction processing, and application programming interfaces (APIs).*

The PCI TSP Security Requirements define physical and logical security controls to protect the environments where Token Service Providers (as defined by the EMVCo Technical Framework) perform tokenization services.

During development of the PCI TSP Security Requirements, PCI SSC consulted with EMVCo to produce requirements that support and complement the EMVCo Technical Framework. Supporting programs for the PCI TSP Security Requirements and EMVCo Technical Framework are managed by PCI SSC and EMVCo respectively, and each entity defines its own processes and procedures related to their own program. The documents are independently maintained, and neither document replaces or supersedes the other.

Q 5. Do the PCI TSP Security Requirements apply to acquiring tokens?

A: *No. The PCI TSP Security Requirements are intended for entities that have registered with EMVCo as a Token Service Provider for Payment Tokens. The PCI TSP Security Requirements cover Payment Tokens as defined by EMVCo, and do not address acquiring tokens or other types of tokens. While entities that provide services for acquiring tokens (for example, by tokenizing PAN after it is received from the cardholder during a transaction) may choose to implement the PCI TSP Security Requirements, they are not required to do so.*

For guidance on acquiring token solutions, the PCI Tokenization Product Security Guidelines document is available on the PCI SSC website.

Q 6. What is the difference between "acquiring tokens", "issuer tokens", and "Payment Tokens"?

A: *Each of these types of tokens replace the PAN with an alternative or surrogate value.*

Acquiring tokens are created by the acquirer, merchant, or a merchant's service provider after the cardholder presents their PAN and/or other payment credentials. Acquiring tokenization solutions are proprietary and are not based on an industry-standard approach to token generation, format, request or provisioning[1]. Acquiring Tokens cannot be used for new authorizations. They can be used for card-on-file and recurring payments. The PCI Tokenization Product Security Guidelines offers guidance on acquiring tokens.

Issuer tokens, also known as virtual card numbers, are created by issuers and provide the means to reduce risk in specific use cases, including commercial card applications, as well as consumer-oriented services. These tokens resemble the PAN, so merchants and acquirers are unlikely to know that they are using a token[2].

Payment tokens are created by TSPs that are registered with EMVCo. Payment Tokens and their usage are defined by EMVCo in the EMVCo Technical Framework. Payment Tokens are issued to a cardholder in lieu of a PAN, and the cardholder presents the Payment Token to the merchant when making a purchase. During a Payment Token transaction, the merchant and acquirer do not receive or have access to the corresponding PAN.

[1] U.S. Payments Security Evolution and Strategic Road Map. Developed by the working groups of the Payments Security Taskforce, December 11, 2014.

[2] U.S. Payments Security Evolution and Strategic Road Map. Developed by the working groups of the Payments Security Taskforce, December 11, 2014.

Q 7. How do the PCI TSP Security Requirements differ from the PCI Tokenization Product Security Guidelines?

A: *The PCI TSP Security Requirements is a standard for Payment Tokens, while the PCI Tokenization Product Security Guidelines provide guidance and best practices for acquiring tokens*

The PCI TSP Security Requirements are intended for entities designated by EMVCo as Token Service Providers, to protect the environments where the Token Service Provider performs tokenization services. Assessment and validation against the TSP Security Requirements may be required by payment brands for registered Token Service Providers.

The Tokenization Product Security Guidelines were published by PCI SSC in April 2015 to *provide technical best practices for the development of tokenization solutions for acquiring tokens. The Tokenization Product Security Guidelines do not apply to Payment Tokens and are not intended for use by Payment Token TSPs. The Tokenization Product Security Guidelines are intended as guidance only; there is no program or validation associated with the Guidelines.*

Q 8. Where do the PCI TSP Security Requirements apply within a TSP's environment?

A: *The PCI TSP Security Requirements apply to the TSP's token data environment, which is a dedicated, secure area within which the TSP performs the tokenization services defined in the EMVCo Technical Framework. The token data environment is described further within the PCI TSP Security Requirements. Payment Tokens that exist outside of the token data environment are not subject to the PCI TSP Security Requirements.*

Q 9. How does a TSP validate to the PCI TSP Security Requirements?

A: *Entities wishing to become Token Service Providers must first register with EMVCo and meet all requirements defined in the EMVCo Technical Framework.*

To validate to the PCI TSP Security Requirements, the TSP engages a QSA (P2PE) to evaluate the token data environment against the PCI TSP Security Requirements. The TSP submits validation documentation (ROC and AOC) to the applicable payment brand(s). Templates for the TSP ROC and TSP AOC are provided on the PCI SSC website.

Q 10. Who is qualified to assess the PCI TSP Security Requirements?

A: *When assessing the TSP's token data environment, only QSA (P2PE)s that have undergone TSP training are qualified to assess the PCI TSP Security Requirements. PCI DSS Requirements 1 through 12 (which also apply to the token data environment) may be validated by a QSA.*

Q 11. Why is a QSA (P2PE) required to assess the PCI TSP Security Requirements?

A: *The PCI TSP Security Requirements include cryptographic key management, physical security and logical access controls that are more stringent than PCI DSS. Assessment of these requirements requires a level of knowledge and skill comparable to that required for performing P2PE assessments. Qualification as a QSA (P2PE) requires a level of prerequisite experience and knowledge that is also suitable for assessing the more stringent controls defined in the PCI TSP Security Requirements.*

Q 12. How can a QSA that is not also a QSA (P2PE) become qualified to assess the PCI TSP Security Requirements?

A: *QSAs that wish to assess the PCI TSP Security Requirements, and that meet all the requisite personnel and company requirements defined in the "PCI Qualification Requirements For Point-to-Point Encryption (P2PE) Qualified Security Assessors – QSA (P2PE) and PA-QSA (P2PE)", can follow the qualification path to become a QSA (P2PE) in order to perform such assessments.*

Q 13. When will qualified assessors be available to perform TSP Security Requirements assessments?

A: *PCI SSC will publish reporting templates and provide QSA (P2PE)s with supplemental training in early 2016. Additional announcements and communications will be provided when these are available.*

Q 14. Does PCI SSC list validated TSPs?

A: *There are currently no plans for PCI SSC to list Token Service Providers that have been assessed to the PCI TSP Security Requirements. Any queries about TSP compliance should be directed to the applicable payment brand(s).*