Payment Card Industry 3-D Secure (PCI 3DS)

Security Requirements and Assessment Procedures for EMV® 3-D Secure Core Components: ACS, DS, and 3DS Server

Frequently Asked Questions

October 2019

Introductory Note

This document addresses frequently asked questions (FAQs) related to the *PCI 3DS Security Requirements and Assessment Procedures for EMV® 3-D Secure Core Components: ACS, DS, and 3DS Server* (hereafter referred to as the PCI 3DS Core Security Standard). Throughout this FAQ document:

- The use of "PCI 3DS Core Security Standard" or "PCI 3DS" refers to the current version of the *PCI 3DS Security Requirements and Assessment Procedures for EMV® 3-D Secure Core Components: ACS, DS, and 3DS Server*, as published on the PCI SSC website (www.pcisecuritystandards.org).
- The use of "EMVCo 3DS Core Specification" refers to the *EMV® 3-D Secure Protocol and Core Functions Specification*, as published by EMVCo (www.emvco.com).

Further information about use and applicability of the PCI 3DS Core Security Standard can be found in the "Introduction", "Terminology", and "Scope of Requirements" sections within the standard itself, as well as in the general PCI Glossary on the PCI SSC website: https://www.pcisecuritystandards.org/pci_security/glossary.

The FAQs in this document are organized as follows:

1. General FAQs
2. Relationship between PCI 3DS Core Security Standard and other PCI standards

1. General FAQs

Q 1: What is 3-D Secure?

A: *EMV® Three-Domain Secure (3-D Secure, or 3DS) is a messaging protocol that enables consumers to authenticate themselves with their card issuer when making card-not-present (CNP) e-commerce purchases. The additional security layer helps prevent unauthorized CNP transactions and protects the merchant from exposure to CNP fraud. The three domains consist of the merchant/acquirer domain, issuer domain, and the interoperability domain (for example, Payment Systems). For details about EMV® 3-D Secure, refer to https://www.emvco.com/emv-technologies/3d-secure/.*

Q 2: To whom does the PCI 3DS Core Security Standard apply?

A: *The PCI 3DS Core Security Standard applies to entities that perform or provide the following functions, as defined in the EMVCo 3DS Core Specification:*

- *3DS Server (3DSS)*
- *3DS Directory Server (DS)*
- *3DS Access Control Server (ACS)*

Where a third-party service can impact 3DS functionality or the security of the 3DS Environment (3DE), the applicable PCI 3DS requirements will need to be identified and implemented for that service. While the ultimate responsibility for the security of the 3DE and 3DS Data lies with the 3DS entity, service providers may be required to demonstrate compliance with the applicable PCI 3DS requirements based on the service provided. Refer to the section "Use of Third-Party Service Providers / Outsourcing" in the PCI 3DS Core Security Standard for further details on the use of third-party service providers.

Whether an entity is required to validate compliance with the PCI 3DS Core Security Standard is defined by the individual payment brand compliance programs. Contact information for the payment brands can be found in FAQ #1142, "How do I contact the payment brands?" on the PCI SSC website.

Q 3: How are the PCI 3DS requirements structured?

A: *The requirements in the PCI 3DS Core Security Standard are organized into the following sections:*

- *Part 1: Baseline Security Requirements, which provide technical and operational security requirements designed to protect environments where 3DS functions are performed. These requirements reflect general information security principles and practices common to many industry standards, and should be considered for any type of environment.*
- *Part 2: 3DS Security Requirements, which provide security controls specifically intended to protect 3DS data, technologies, and processes.*

Q 4: Does the Implementation Guidance have to be met in order for a requirement to be considered "in place"?

A: *No. The intent of the Implementation Guidance is to provide additional information to help entities and assessors understand how a requirement could be met. The examples and practices in the Implementation Guidance column are not requirements and do not preclude other methods that may be used to meet a requirement. While the Implementation Guidance contains recommendations and best practices that should be considered, this guidance does not replace or extend the requirement to which it refers. Assessors and 3DS entities should work together to ensure clear understanding of how implemented controls meet the intent of the requirements.*

Q 5: What is the PCI 3DS Data Matrix and how does it fit in with the PCI 3DS Core Security Standard?

A: *The PCI 3DS Data Matrix is a separate document that supports the PCI 3DS Core Security Standard. The PCI 3DS Data Matrix identifies a number of data elements common to 3DS transactions, as defined by EMVCo, that are also subject to requirements in the PCI 3DS Core Security Standard. The data elements identified in the PCI 3DS Data Matrix include those considered to be 3DS sensitive data, which are subject to specific data protection requirements, and certain cryptographic key types that are subject to HSM requirements.*

Q 6: Who is qualified to assess the PCI 3DS Core Security Requirements?

A: *Only 3DS Assessors who have satisfied all 3DS Core Assessor Qualification Requirements applicable to employees of 3DS Assessor Companies and are listed on the PCI SSC 3DS assessor website are qualified to assess the PCI 3DS Core Security Requirements.*

The 3DS Core Program qualification involves both the qualification of the company and the employee who will be performing and/or managing PCI 3DS Core Assessments. QSA Employees wishing to become a 3DS Core Assessor will require at least three years' QSA experience and at least one industry-recognized certification in both information security and IT audit (as defined in QSA Qualification Requirements section 3.2). QSA Employees will also be required to attend training and pass an examination. A grandfathering arrangement for P2PE Assessors and existing 3-D Secure v1 Visa assessors that are also QSAs will be in place until 1 January 2020. Details of the qualification requirements are further described in the 3DS Core Qualification Requirements available in the PCI SSC Document Library.

Q 7: Does PCI SSC provide a list of 3DS entities that are validated to the PCI 3DS Core Security Standard?

A: *There are currently no plans for PCI SSC to list 3DS entities that have been assessed to the PCI 3DS Core Security Standard. Any queries about PCI 3DS Core Security Standard compliance should be directed to the applicable payment brand(s).*

Q 8: Are 3DS entities that support v1 of the 3-D Secure protocol required to migrate to EMV® 3-D Secure?

A: *Whether an entity is required to use and/or support a specific version of 3DS is determined by the payment brands. 3DS entities should contact the applicable payment brand and/or issuer to whom they provide 3DS services for further information.*

Q 9: Are 3DS entities that currently meet the *Visa 3-D Secure Security Requirements for Enrollment Servers and Access Control Servers* also required to meet the PCI 3DS Core Security Standard?

A: *All queries related to validating compliance should be directed to the applicable payment brand.*

2. Relationship between PCI 3DS Core Security Standard and other PCI standards

Q 10: What is the relationship between the PCI 3DS Core Security Standard and the PCI 3DS SDK Security Standard?

A: *The PCI 3DS Core Security Standard and PCI 3DS SDK Security Standard are independent standards that define security controls covering different areas of the 3DS ecosystem.*

- *The PCI 3DS Core Security Standard supports the EMVCo 3DS Core Specification, and applies to entities that perform or provide specific 3DS functions; namely 3DS Server (3DSS), 3DS Directory Server (DS), or 3DS Access Control Server (ACS) functions.*
- *The PCI 3DS SDK Security Standard applies to entities that develop 3DS Software Development Kits (SDK), as defined in the EMV® 3-D Secure SDK Specification.*

While these two PCI standards define consistent levels of security for respective 3DS components, they are distinct standards with separate requirements and programs, and validation against one standard does not imply or result in validation against the other.

Q 11: What is the relationship between the PCI 3DS Core Security Standard and the PCI DSS?

A: *The PCI 3DS Core Security Standard and PCI DSS are separate, independent standards each intended for specific types of entities. The PCI 3DS Core Security Standard applies to 3DS environments where 3DSS, ACS, and/or DS functions are performed, while PCI DSS applies wherever payment card account data is stored, processed or transmitted. Details of each standard's applicability are provided within the introductory sections of that standard.*

Where an entity meets the applicability for both standards, the entity should consult with their acquirer and/or payment brand, as applicable, to determine whether they are required to validate to either or both standards.

While many 3DS entities may have both PCI 3DS and PCI DSS responsibilities, there may be cases where a 3DS entity does not store, process, or transmit any payment card account data–for example, where the 3DS entity is involved only in 3DS transactions for EMVCo payment tokens. In this scenario, the 3DS entity may not be subject to PCI DSS. In all cases, entities should refer to their acquirer and/or the payment brand(s) to determine their compliance obligations to a PCI standard.

Q 12: How should a 3DS entity manage an environment covered by both PCI 3DS and PCI DSS?

A: *3DS entities that store, process, or transmit payment card account data will have a defined 3DS environment (3DE) and a defined cardholder data environment (CDE). If account data is present in the environment where 3DS functions are performed, that environment would be considered both a 3DE and a CDE.*

Where the 3DE and CDE are combined in the same environment, the 3DS entity may be able to implement security controls that meet requirements in both standards. As the PCI 3DS Part 1: Baseline Security Requirements cover many of the security objectives required by PCI DSS, additional controls may not be needed to meet the PCI 3DS Part 1 Requirements if PCI DSS is fully implemented.

Where a requirement in one standard requires more stringent security controls than what is implemented or required by the other standard, the entity may need to implement the more stringent controls throughout the environment to ensure the applicable requirements from both standards are met.

An alternative scenario is where the 3DS entity has a CDE that is separate and segmented from the 3DE. In this scenario, the 3DS entity may choose to apply different controls to each environment as appropriate for the applicable standard.

Whether a 3DS entity is required to validate compliance with the PCI 3DS Core Security Standard and/or PCI DSS is defined by the individual payment brand compliance programs.

Q 13: Can an entity use their PCI DSS assessment results for their 3DS assessment?

A: *As noted in Q12, additional controls may not be needed to meet the PCI 3DS Part 1: Baseline Security Requirements if PCI DSS is fully implemented to protect the 3DE and all 3DS system components. In circumstances where the 3DE and CDE are combined in the same environment, and PCI DSS controls have been applied and validated for all 3DE system components, the 3DS entity may be able to leverage the results of their PCI DSS assessment to validate the PCI 3DS Part 1 Requirements. 3DS entities wishing to use the results of a PCI DSS assessment for this purpose should confirm this approach with their acquirer and/or the payment brand(s). PCI DSS assessment results cannot be leveraged to validate 3DS Part 2 Requirements.*

Refer to Appendix B: Alignment between PCI 3DS and PCI DSS Requirements, in the PCI 3DS Core Security Standard, for details on requirements for leveraging PCI DSS for PCI 3DS Part 1. The 3DS assessor will need to document PCI DSS coverage of the 3DE in the 3DS Report on Compliance and Attestation documents.

There is currently no option for entities to leverage results of a PCI 3DS assessment for their PCI DSS validation. Validation to PCI 3DS Part 1 does not impact or replace PCI DSS compliance obligations.