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

---

Technical FAQs for use with Version 1.x

September 2023

Introduction

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.

PCI 3DS: Technical FAQs

These Technical FAQs provide answers to questions regarding the application of the Security Requirements defined in the PCI 3DS Core Security Standard. Technical FAQs may contain information on how to interpret requirements and, in some cases, may add new or extend existing requirements. Technical FAQs are an integral and mandatory part of the PCI 3DS Core Security Standard and must be considered during a PCI 3DS Core Security Assessment.

New questions or questions updated for clarity are in **red**.

Requirement P2-5

Q 1 April 2021: Does the Authentication Value (AV) need to be encrypted per PCI 3DS Core Requirement P2-5.4.2 if it is a cryptographically generated value (e.g., a "cryptogram")?

A *Whether a cryptographically generated Authentication Value (AV) may be stored without being encrypted (again) will depend on how each payment system (i.e., payment brand) generates the Authentication Value and how that value is used.*

The EMV® 3-D Secure Protocol and Core Functions Specification does not specify a method or algorithm that is required to generate an Authentication Value and enables each payment system to determine which method(s) and/or algorithm(s) to use. The PCI 3DS Core Security Standard, however, assumes that these values are static values that are used directly in the course of 3DS transaction processing and, therefore, must be encrypted along with other 3DS sensitive data per the PCI 3DS Data Matrix and in accordance with PCI 3DS Core Requirement P2-5.4.2 prior to any permitted storage.

Where the Authentication Value is a dynamic (i.e., a single use) value that cannot be reused after generation or is already encrypted using strong cryptography and requires the value to be decrypted prior to use, then it may be possible to store the Authentication Value where permitted without encrypting it again. 3DS entities should contact the applicable payment system(s) for more information on whether the Authentication Value for that payment system is generated and used in a way that would permit it to be stored without having to encrypt it further.

Requirement P2-6

Q 2 April 2021: What types of 3DS components are required to use an HSM for protecting and managing cryptographic keys?

A *Requirement P2-6 covers Cryptography and Key Management for all 3DS components (ACS, DS, and 3DS Server); however, P2-6.1.2 clearly notes that only environments housing DS and ACS systems require the use of an FIPS 140-2 Level 3 (overall) or higher certified, or a PCI PTS approved HSM for all key management activity. Other HSM related requirements such as Requirements P2-6.2 and P2-6.3 also apply only to the ACS and DS.*

The use of an HSM is recommended, but not required, for locations where only a 3DS Server is present.

Q 3 September 2023: Can compensating controls be used to meet Requirement P2-6.2.1?

A *No. Requirement P2-6.2.1 requires personnel with logical access to HSMs to access those HSMs either using the HSM console or using a non-console access solution.*

However, effective upon the publication of this Technical FAQ, it is no longer exclusively required of a non-console HSM access solution to be evaluated by an independent laboratory to verify compliance with ISO 13491.

An alternative set of requirements for a non-console HSM access solution are as follows. Note these requirements below, if met in their entirety, can be used to satisfy the currently published requirements P2-6.2.1 through P2-6.2.5. If using these alternative requirements, make a note of this Technical FAQ in the ROC for each respective requirement and include the appropriate assessment & documentation to validate the requirements as stated have been satisfied.

- *(P2-6.2.1) Non-console HSM access for the purposes of management and configuration requires the use of MFA.*
- *(P2-6.2.2) Non-console HSM access for the purposes of management and configuration is performed using a secure channel.*
- *(P2-6.2.3) Secret or private cryptographic keys, key components, and/or key shares input to or output from the HSM are secured through dual control and split knowledge.*
- *(P2-6.2.4) Non-console access used for the loading of clear-text key components or key shares originates from a Secure Cryptographic Device (SCD), that is either:*
  - *Listed on the NIST Cryptographic Module Validation Program (CMVP) list and approved to FIPS 140-2 Level 3 or 140-3 Level 3 (overall) or higher. Refer to* http://csrc.nist.gov.

  Or,

  - *Listed on the PCI SSC website, with a valid PCI SSC listing number, as an Approved PCI PTS Device.*
- *(P2-6.2.5) When loaded through a non-console interface, key components and key shares are encrypted using a key encryption key that is specific for the purposes of key transport. Use of encryption provided by a secure channel is not sufficient to meet this requirement.*

Q 4 December 2020: Can a 3DS entity outsource the hosting and management of its HSMs to a third-party service provider?

A *Yes, a 3DS entity may choose to outsource the hosting and management of its HSM infrastructure to a third-party service provider as long as all applicable requirements are met. The 3DS entity should work with their service provider to determine which requirements are covered by the service provider and which are covered by the 3DS entity. The 3DS entity remains ultimately responsible for ensuring that all applicable requirements regarding the hosting and management of HSMs are met. Please refer to the "Use of Third-Party Service Providers / Outsourcing" section in the PCI 3DS Core Security Standard for more information.*

Requirement P2-7

Q 5 December 2020: What types of 3DS components are in scope for Requirement P2-7 in the PCI 3DS Core Security Standard?

A *Requirements P2-7.1 and P2-7.2, which relate to data center and CCTV security, apply to DS and ACS systems.*

As noted in the Overview section of Requirement P2-7, the DS and ACS systems are critical components of the 3DS infrastructure that require a secure facility with elevated physical security controls to restrict, manage, and monitor all physical access.

The requirements in P2-7 are recommended, but not required, for locations where only a 3DS Server is present. Refer to the PCI 3DS Core Security Standard for information about the different 3DS components.

Note*: This FAQ has been imported from the General FAQs on the PCI SSC website.*