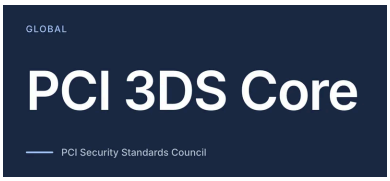
SmartSuite

Framework / Cybersecurity / PCI Security Standards

PCI 3DS Security Requirements and Assessment Procedures for EMV 3-D Secure Core Components: ACS, DS, and 3DS Server, v1.0 (October 2017)

PCI 3DS Core Security Standard v1.0 (October 2017) sets PCI SSC's Part 1 baseline and Part 2 3DS-specific requirements for operators of EMV 3-D Secure ACS, DS and 3DS Server functions.



What it is

The PCI 3DS Core Security Standard, in full the PCI 3DS Security Requirements and Assessment Procedures for EMV 3-D Secure Core Components: ACS, DS, and 3DS Server, is the PCI Security Standards Council's standard for the entities that perform or provide 3DS Server (3DSS), 3DS Directory Server (DS) and 3DS Access Control Server (ACS) functions as defined in the EMVCo 3DS Core Specification; version 1.0 was released in October 2017 and remains the published version, with a draft v2.0 taken through a request for comments from December 6, 2023 to January 19, 2024. Whether an entity must validate compliance is defined by the individual payment brand compliance programs, not by PCI SSC.

At a glance

PUBLISHER
Payment Card Industry Security Standards Council (PCI SSC)

TYPE
Standard

VERSION
v1.0 (October 2017) with Technical FAQs (April 2021, revised September 2023); v2.0 draft in request for comments December 2023 to January 2024

EFFECTIVE
October 2017 (v1.0)

DOMAIN
Cybersecurity

FAMILY
PCI Security Standards

REGION
Global

INDUSTRY
Payment & FinTech

ADOPTION MODEL
Industry Requirement

IMPLEMENTATION COMPLEXITY
High

Source: pcisecuritystandards.org/standards/pci-3ds-core/

Why it matters

- **One standard for three components** The same requirements apply to 3DS Server, Directory Server and Access Control Server functions as defined in the EMVCo 3DS Core Specification, with the HSM and data center requirements concentrated on the DS and ACS.
- **Baseline plus 3DS-specific controls** Part 1 carries technical and operational requirements that reflect general information security principles; Part 2 adds the controls specific to 3DS data, technologies and processes (FAQ Q3).
- **A defined data set to protect** The PCI 3DS Data Matrix names the EMVCo-defined data elements, the 3DS sensitive data and the key types the requirements cover, so scoping starts from a published list (FAQ Q5).
- **Reuse of PCI DSS work where environments overlap** Where the 3DS environment and the cardholder data environment are one, validated PCI DSS controls may be used toward the Part 1 requirements under Appendix B of the standard; Part 2 is always assessed on its own (FAQ Q12, Q13).

 © 2026 SmartSuite Inc. All rights reserved.

How SmartSuite supports PCI 3DS Core

3DS Component Inventory

Record every 3DS Server, Directory Server and Access Control Server instance, the facilities and HSMs that serve it, and whether its environment is also a cardholder data environment (FAQ Q12).

Part 1 and Part 2 Requirement Register

Hold the Baseline Security Requirements and the 3DS Security Requirements as separate records per component, with the Implementation Guidance kept as notes rather than as requirements.

3DS Sensitive Data and Key Inventory

List the Data Matrix elements and cryptographic key types in use, where the Authentication Value is stored, and the HSM that protects each key (P2-5.4.2, P2-6.1.2).

Assessment Evidence by Requirement

Attach the evidence a PCI 3DS Assessor will test, and mark where validated PCI DSS controls are relied on for Part 1 under Appendix B.

Technical FAQ Tracking

Link each Technical FAQ, including the September 2023 revision of Q3 on HSM access, to the requirements it interprets so assessments use the current reading.

Service Provider Responsibility Matrix

Use Third Party Risk Management to record which requirements an outsourced HSM host or other provider covers and which stay with the 3DS entity (Technical FAQ Q4).

Common framework mappings

CIS Controls v8.1 | ISO 27001:2022 | NIST CSF 2.0 | PCI DSS 4.0.1 | SOC 2

Official resources

PCI 3DS Core Security Standard

Defines the requirements for securing EMV 3-D Secure transactions.

pcisecuritystandards.org/standards/pci-3ds-core

PCI 3DS Core Security Standard Implementation Guide

Provides guidance on implementing security controls within 3DS environments.

pcisecuritystandards.org/document_library

PCI Security Standards Council Resources

Outlines additional resources and supporting documents for PCI 3DS.

pcisecuritystandards.org/standards/pci-3ds

PCI 3DS Risk Assessments

Describes risk assessment procedures for maintaining compliance with PCI 3DS.

pcisecuritystandards.org/document_library/?category=3ds

Frequently asked questions

Who has to comply with the PCI 3DS Core Security Standard?

It applies to entities that perform or provide 3DS Server, 3DS Directory Server or 3DS Access Control Server functions as defined in the EMVCo 3DS Core Specification, and third-party service providers that can affect those functions or their environments may be required to meet the applicable requirements (FAQ Q2). Whether an entity must validate compliance is defined by the individual payment brand compliance programs; PCI SSC does not list validated 3DS entities and refers compliance questions to the brands (FAQ Q7).

How are the requirements of PCI 3DS Core organized?

Part 1 Baseline Security Requirements set technical and operational requirements for environments where 3DS functions are performed, reflecting general information security principles; Part 2 3DS Security Requirements add controls specific to 3DS data, technologies and processes (FAQ Q3). The Implementation Guidance column explains how a requirement could be met but is not itself a requirement (FAQ Q4), and the separate PCI 3DS Data Matrix identifies the data elements, 3DS sensitive data and key types the requirements cover (FAQ Q5).

Updated Oct 15, 2026 · © 2026 SmartSuite Inc. All rights reserved.

Which 3DS components need an HSM under PCI 3DS?

Requirement P2-6 covers cryptography and key management for all 3DS components, but P2-6.1.2 requires an HSM, FIPS 140-2 Level 3 (overall) or higher certified or PCI PTS approved, only for environments housing DS and ACS systems; the related requirements P2-6.2 and P2-6.3 also apply only to the ACS and DS, and an HSM is recommended but not required where only a 3DS Server is present (Technical FAQ Q2). A 3DS entity may outsource HSM hosting and management but remains responsible for the requirements being met (Technical FAQ Q4).

Can a PCI DSS assessment be used for a PCI 3DS assessment?

Partly. Where the 3DS environment and the cardholder data environment are combined and PCI DSS controls have been applied and validated for all 3DE system components, the entity may be able to use its PCI DSS assessment results to validate the Part 1 Baseline Security Requirements, under the conditions in Appendix B of the standard and with the acquirer's or payment brand's agreement (FAQ Q12, Q13). PCI DSS results cannot be used to validate Part 2, and a PCI 3DS assessment cannot be used for PCI DSS validation.

Is there a PCI 3DS Core Security Standard v2.0?

Not as a published standard on the PCI SSC pages read. PCI SSC ran a request for comments on draft PCI 3DS Core Security Standard v2.0 and draft PCI 3DS Data Matrix v2.0 from December 6, 2023 to January 19, 2024, with the draft covering the ACS, DS, 3DS Server and Split-SDK Server. Version 1.0 of October 2017 remains the published standard, read together with the Technical FAQs of April 2021 and the September 29, 2023 revision of Technical FAQ Q3 on HSM access.

License included / downloadable: Yes The PCI 3DS Core Security Standard, the PCI 3DS Data Matrix and the FAQs are published by PCI SSC and available through the PCI SSC Document Library.

Full framework page and mappings: smartsuite.com/frameworks/pci-3ds-core