

PCI 3-D Secure (3DS) Core Security Standard v2.2.1

PCI 3DS Core Security Standard defines security controls to protect data and processes in EMV 3-D Secure online payment authentication.



What it is

The PCI 3DS Core Security Standard is a cybersecurity framework that helps organizations protect the confidentiality, integrity, and availability of data involved in EMV® 3-D Secure (3DS) transactions. This standard establishes technical and operational requirements to reduce the risk of data breaches and support secure online payment authentication processes.

Published by the PCI Security Standards Council (PCI SSC), the framework applies to organizations that operate 3DS environments, such as payment service providers, issuers, and merchants. It addresses areas including network security controls, data protection, access management, incident response, and ongoing compliance oversight within 3DS ecosystems.

At a glance

PUBLISHER Payment Card Industry Security Standards Council (PCI SSC)	TYPE Standard	VERSION PCI 3DS Core Security Standard (current PCI SSC published edition)
EFFECTIVE October 2020	DOMAIN Cybersecurity	FAMILY PCI Security Standards
REGION United States	INDUSTRY Payment & FinTech	ADOPTION MODEL Industry Requirement
IMPLEMENTATION COMPLEXITY High		

Source: <https://www.pcisecuritystandards.org/standards/pci-3ds-core/>

Why it matters

- **Strengthen data protection practices** Safeguard the confidentiality and integrity of sensitive authentication and transaction data throughout the 3DS payment process.
- **Enhance cybersecurity governance** Establish clear security roles and responsibilities that improve oversight, accountability, and control throughout the payment authentication lifecycle.
- **Improve incident detection and response** Enable rapid identification and reporting of security incidents to better contain threats and reduce potential impacts.
- **Support regulatory compliance** Align 3DS security practices with broader PCI requirements, facilitating regulatory adherence and ongoing compliance efforts.

How SmartSuite supports PCI 3DS Core

3DS Scope and Component Inventory Define 3DS components, boundaries, and supporting infrastructure in scope.	Requirement Library and Ownership Track 3DS requirements with owners, procedures, and implementation evidence.	Key Management and Cryptography Evidence Centralize key management procedures and cryptographic control proof.
Testing and Monitoring Cadence Schedule scans, testing, monitoring checks, and evidence capture.	Change Management and Release Control Manage changes to 3DS components with approvals and validation evidence.	Audit-Ready Reporting Report requirement coverage, open gaps, and readiness for assessments.

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

- What is the PCI 3DS Core Security Standard used for?**
The PCI 3DS Core Security Standard is used to protect the confidentiality, integrity, and availability of data in EMV® 3-D Secure (3DS) payment authentication transactions. It establishes security requirements for organizations that process, store, or transmit 3DS transaction data to reduce the risk of data breaches and ensure secure online payment experiences.
- Is PCI 3DS Core Security Standard certification required?**
Certification to the PCI 3DS Core Security Standard is required for certain organizations, such as payment service providers, 3DS issuers, and merchants operating 3DS environments, by card brands or acquirers. Compliance is validated through regular assessments by Qualified Security Assessors (QSAs) as directed by the PCI Security Standards Council or your payment brand.
- What organizations are in scope for PCI 3DS Core Security Standard?**
The standard applies to all organizations that operate 3DS transaction environments, including payment service providers, issuers, acquirers, and merchants who facilitate or process 3DS data. Third-party service providers involved in 3DS ecosystems are also in scope if they impact the security of authentication data.
- What are the key requirements or controls in PCI 3DS Core Security Standard?**
Key controls include network security architecture, encryption of sensitive authentication data, robust access management, monitoring and logging, incident response, and periodic security assessments. Organizations must also manage cryptographic keys, assess third-party providers, and document compliance evidence.

How is the PCI 3DS Core Security Standard implemented in practice?

Organizations implement the standard by understanding its security control domains, mapping requirements to their 3DS payment environments, developing security policies and procedures, and integrating these controls with existing risk management and governance practices. Regular training, monitoring, and review activities are also part of the implementation process.

How does PCI 3DS Core Security Standard relate to other PCI standards?

The PCI 3DS Core Security Standard complements other PCI frameworks, such as PCI DSS, but focuses specifically on the secure processing of 3DS authentication data. It addresses unique risks and authentication elements in 3DS, while PCI DSS covers broader payment card data environments.

What are the ongoing compliance requirements for PCI 3DS Core Security Standard?

Ongoing compliance involves maintaining all required security controls, conducting periodic risk assessments, documenting procedures, monitoring for security incidents, and undergoing regular PCI SSC assessments. Continuous improvement, remediation of findings, and up-to-date evidence collection are also expected.

How would SmartSuite support PCI 3DS Core Security Standard?

SmartSuite supports PCI 3DS Core Security Standard compliance by enabling organizations to track risks, manage required security controls, and automate evidence collection for audit purposes. It provides tools for maintaining policy documentation, managing remediation workflows, and monitoring compliance status through real-time dashboards and reporting, facilitating continuous audit readiness and oversight.

License included / downloadable: Yes The PCI 3DS Core Security Standard is published by the PCI Security Standards Council and is publicly available through official PCI SSC resources.

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