

Which specific EMVCo Security Guidelines document and version should I use? For example: - EMVCo



What it is

EMVCo Security Guidelines is an industry framework that helps organizations implement robust security controls for payment card transactions and protect sensitive cardholder data. These guidelines provide a common security baseline for the design and deployment of card payment systems, addressing emerging cybersecurity threats and regulatory requirements.

Published by EMVCo, a consortium managed by leading payment networks including Visa, Mastercard, and American Express, the guidelines are widely referenced by payment service providers, device manufacturers, and financial institutions. The framework covers areas such as cryptographic security, data protection, device integrity, and secure transaction processing, supporting compliance with global payment security standards.

At a glance

PUBLISHER EMVCo, LLC	TYPE Guidance	VERSION Current EMVCo Security Guidelines
EFFECTIVE 2016	DOMAIN Cybersecurity	FAMILY PCI Security Standards
REGION United States	INDUSTRY Payment & FinTech	ADOPTION MODEL Industry Requirement
IMPLEMENTATION COMPLEXITY High		

Source: <https://www.emvco.com/>

Why it matters

- **Strengthen payment system security** Enables organizations to implement robust controls that mitigate risks across payment devices, networks, and cardholder data flows.
- **Enhance data protection practices** Supports comprehensive data confidentiality and integrity measures, reducing the likelihood of unauthorized cardholder information access or theft.
- **Improve regulatory compliance efforts** Aligns security measures with global standards, facilitating compliance with industry and regional payment security regulations.
- **Increase certification and audit readiness** Provides a structured framework that helps organizations streamline internal assessments and succeed in external audits and product certifications.

How SmartSuite supports EMVCo Security Guidelines

Security Requirement Mapping

Translate EMVCo expectations into operational controls with ownership.

Cryptographic and Key Management Governance

Track key management processes, approvals, and evidence of operation.

Secure Processing and Access Controls

Manage access governance and control evidence for payment environments.

Monitoring, Detection, and Incident Workflows

Capture monitoring proof, incident timelines, and corrective actions.

Vendor and Ecosystem Oversight

Track third-party dependencies, contract safeguards, and monitoring evidence.

Compliance Reporting

Report posture, gaps, and evidence coverage for stakeholder reviews.

Common framework mappings

CIS Controls v8.1

ISO 27001:2022

ISO 27002:2022

NIST CSF 2.0

NIST 800-53 Rev.5

PCI DSS 4.0.1

SWIFT CSCF

Official resources

EMVCo Security Requirements

Defines security requirements for card payment systems to protect sensitive cardholder data.

emvco.com/approved-products/?type=security_evaluation

EMVCo Security Evaluation Processes

Outlines processes for evaluating and certifying payment products' security in compliance with EMVCo standards.

emvco.com/approved-products/?type=security_evaluation

EMVCo Security Guidelines Overview

Provides an overview of the security guidelines for implementing robust controls in card transactions.

emvco.com/about-us/overview-of-emvco

EMVCo Data Protection Techniques

Describes techniques for protecting data in card payment environments according to EMVCo standards.

emvco.com/emv-technologies

Frequently asked questions

What are EMVCo Security Guidelines used for?

EMVCo Security Guidelines are used to help organizations implement robust security controls for payment card transactions and to protect sensitive cardholder data. They provide a common security baseline for developing and deploying card payment technologies in alignment with industry best practices and evolving cybersecurity threats.

Are EMVCo Security Guidelines mandatory or certifiable?

EMVCo Security Guidelines themselves are not legally mandatory or certifiable in the form of an official certification. However, many payment networks require compliance with these guidelines as part of product approval processes, and EMVCo operates evaluation programs that assess product conformance to its security requirements.

Who must comply with EMVCo Security Guidelines?

Organizations that design, manufacture, or deploy payment products or infrastructures supporting EMV technology, such as financial institutions, payment service providers, and device manufacturers, are expected to follow EMVCo Security Guidelines. Adherence is particularly significant for those seeking payment network acceptance and participation in the global payment ecosystem.

What are the key security controls outlined in EMVCo Security Guidelines?

EMVCo Security Guidelines require organizations to implement controls in areas such as cryptographic key management, secure authentication mechanisms, transaction security, tamper resistance, and data protection. These controls are designed to prevent

How do organizations implement EMVCo Security Guidelines?

Implementation typically involves mapping security requirements to lifecycle stages of payment solutions, integrating controls into the design and development process, and conducting risk assessments and security evaluations. Documentation of compliance and alignment with guideline requirements is often necessary for participating in EMVCo's security evaluation programs.

How do EMVCo Security Guidelines relate to other standards like PCI DSS?

EMVCo Security Guidelines complement other payment security standards such as PCI DSS by focusing on the security of payment device design and transaction processes, while PCI DSS is primarily concerned with cardholder data environments. Organizations often use both sets of requirements to achieve comprehensive payment security compliance.

What ongoing compliance activities are required for EMVCo Security Guidelines?

Maintaining compliance involves continuous risk monitoring, updating controls in response to new security threats, participating in periodic product evaluations, and ensuring that payment systems remain aligned with the latest EMVCo requirements. Ongoing documentation and evidence of security activities are essential for successful compliance.

How would SmartSuite support EMVCo Security Guidelines?

SmartSuite enables organizations to operationalize EMVCo Security Guidelines by mapping payment security controls to internal policies, tracking risk assessments, and managing evidence collection for audits. It provides centralized control management, supports ongoing compliance monitoring, and generates reports to demonstrate audit readiness and regulatory due diligence.

License included / downloadable: Yes EMVCo security guidelines are published by EMVCo and are publicly available through official EMVCo resources.

Full framework page and mappings: smartsuite.com/frameworks/emvco-security-guidelines-update