

Cloud-Native Key Management for PCI PIN & P2PE: Busting Myths and Reducing Compliance Burden

October 22, 2026

Rob Faba, QSA
Senior Security Assurance Consultant, AWS

Balaji Palanisamy
Principal, AWS Payment Cryptography





20 YEARS OF SECURING PAYMENT DATA
PCI Security Standards Council

Agenda

01

- Three deployment models for payment cryptography

02

- Physical controls are always stronger
- Trust requires physical control
- Cloud migration increases PCI scope

03

- What shifts to the CSP
- Real-world case study
- Key takeaways

20 YEARS OF SECURING PAYMENT DATA
PCI Security Standards Council

Suggested Models for Payment HSM Deployment

On-Premises

Traditional model. Organization owns, manages, and operates HSM hardware.

Full control over physical security, key management, firmware.

Single tenant by design.

HSM as a Service / Bare Metal

CSP provides HSM hardware then hands over control to the customer.

Customer responsible for key management and HSM security policy.

Single tenant. Tamper keys managed by customer. HSM proprietary API.

Cloud-Native Cryptography as a Service

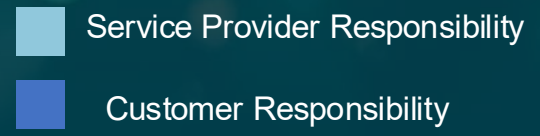
CSP manages HSM infrastructure and operations per Shared Responsibility Model.

Dedicated or shared HSM Processing Elements. Virtualization system segregates tenant domains.

Suited for organizations prioritizing operational simplicity and scalability.

20 YEARS OF SECURING PAYMENT DATA
PCI Security Standards Council

Comparing Compliance Responsibility Models



On-Premises	HSM as a Service	Cloud-Native
Devices and Methods	Devices and Methods	POI & PIN Processing HSM & RMD
Key Loading	Key Loading	Clear Text & POI Loading Cryptograms & Asymmetric
Key Conveyance	Key Conveyance	Clear Text Exchange Cryptograms & Asymmetric
Key Compromise	Key Compromise	Key Compromise Response Key Compromise Detection & Response
Key Administration	Key Administration	Clear Text Admin Key Administration
Key Generation	Key Generation	Key Generation
Equipment Security	POI & RMD HSM	POI HSM & RMD

20 YEARS OF SECURING PAYMENT DATA
PCI Security Standards Council

Myth #1: Physical Controls Are Always Stronger

Reality: Logical controls can be more granular, consistent, and demonstrable

- Procedural dual control depends on people following process correctly every time
- Logical dual control is service-enforced – the system will not allow bypass
- Example: IAM policies, MFA, and Multi-Party Approval for sensitive key actions
- ***Best Practice: Ask "Is this control more or less effective?" not "Is it physical or logical?"***





Myth #2: You Can’t Trust And Can’t Verify What You Don’t Physically Control

Reality: In a cloud model, you trust because you can verify

- Every cryptographic operation logged with full identity context: Who? What? When? Frome Where? Which Key? What was the Result?
- Transparency replaces physical inspection
- ***Best Practice: Require full identity context on every cryptographic operation log and verify third party attestations***



Myth #3: Cloud Migration Increases PCI Scope

Reality: Scope reduction is achievable with upfront documentation

- Provider attestations cover: PCI PTS HSM, PCI PIN, P2PE, DSS, 3DS
- Inherited controls are third-party attested, not self-assessed
- Customer scope narrows too: access control, key lifecycle, application accuracy
- ***Best Practice: Engage assessors early — walk through shared responsibility before assessment***



Reducing Compliance Burden: What Shifts to the CSP

Responsibility Area	On-Premises (You Own)	Cloud-Native
HSM physical lifecycle	Customer manages installation, inspection, decommissioning	→ CSP manages with additional cryptographic device identity validation
Master Key management	Customer creates, stores, and rotates master keys	→ CSP manages; keys never leave service HSMs
Firmware updates	Customer tests and deploys; regression risk causes delays	→ CSP manages transparently; API shields application from changes
Fleet capacity & resilience	Customer provisions 2× peak; manages regional failover	→ CSP manages elastic fleet across 3+ availability zones
Dual-control key ceremonies	Procedural — depends on people following process	→ Service-enforced via IAM + Multi-Party Approval
Cryptographic function enforcement	HSM PCI mode; limited granularity	→ CSP IAM fine-grained per API call, per role
Audit evidence	Manual collection for assessors	→ Programmatic; every operation logged with full identity context

You still own: Access control configuration | Key lifecycle policy | Application accuracy | Exception governance | Compliance program

20 YEARS OF SECURING PAYMENT DATA PCI Security Standards Council

Case Study: Established Payment Service Provider (25 years in the industry)

Challenge

- Multiple services dependent on on-premises HSMs for payment terminal key injection and decryption
- Duplicated key management across injection and decryption workflows
- Manual HSM provisioning slowed payment terminal onboarding
- High operational cost of maintaining physical HSM infrastructure

What Shifted to the CSP

- Adopted AWS Payment Cryptography for next-gen payment network platform
- Unified Remote Key Injection (RKI) and decryption onto a single cloud-native service
- PCI P2PE decryption component responsibility shifted to AWS

Outcomes

- Significant reduction in HSM operational burden
- Up to 40% cost reduction vs. in-house HSM operations
- Improved scalability and availability
- Accelerated regional expansion and business growth

PCI P2PE compliant solution built on AWS Payment Cryptography

20 YEARS OF SECURING PAYMENT DATA PCI Security Standards Council

Case Study: European POS Platform (global payment provider)

Challenge

- HSMs Only remaining on-prem systems
- Small team running manual key ceremonies
- Could not quickly expand to new regions
- Heavy audit overhead from HSMs

What Shifted to the CSP

- Physical security and key management
- 99% of transactions instantly cloud-native
- Nearly two thirds of audit responsibility shifted to CSP

Outcomes

- Significant reduction in audit time
- New regions in a click
- Team refocused on product
- PCI PIN and P2PE certification maintained throughout

20 YEARS OF SECURING PAYMENT DATA
PCI Security Standards Council

Key Takeaways

1

Effectiveness over type

Judge controls by what they enforce, not whether they're physical or logical.

2

Identity on every operation

Require full context on every cryptographic call. No anonymous access, ever.

3

Map scope before you audit

Define the shared responsibility boundary with your assessor upfront.

4

Scope reduction is real

Organizations are achieving it today. Cloud-native shifts compliance burden to the CSP.

5

Visibility up, burden down

Cloud-native key management gives you more audit evidence, not less.

20 YEARS OF SECURING PAYMENT DATA
PCI Security Standards Council

Thank You

Rob Faba

QSA, Senior Security Assurance Consultant

Fabarob@amazon.com

linkedin.com/in/rob-faba/

Balaji Palanisamy

AWS Payment Cryptography

Palanisa@amazon.com

linkedin.com/in/balajipalani/

Scan for the blog post

How AWS Payment Cryptography Raises the Cryptographic Security Bar

aws.amazon.com/blogs/industries/

20 YEARS OF SECURING PAYMENT DATA

PCI Security Standards Council

Certified & Compliant