

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

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

- Three deployment models for payment cryptography
- Myth #1: Physical controls are always stronger
- Myth #2: You can’t trust and you can't verify what you don’t physically control
- Myth #3: Cloud migration increases PCI scope
- Reducing compliance burden: 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.

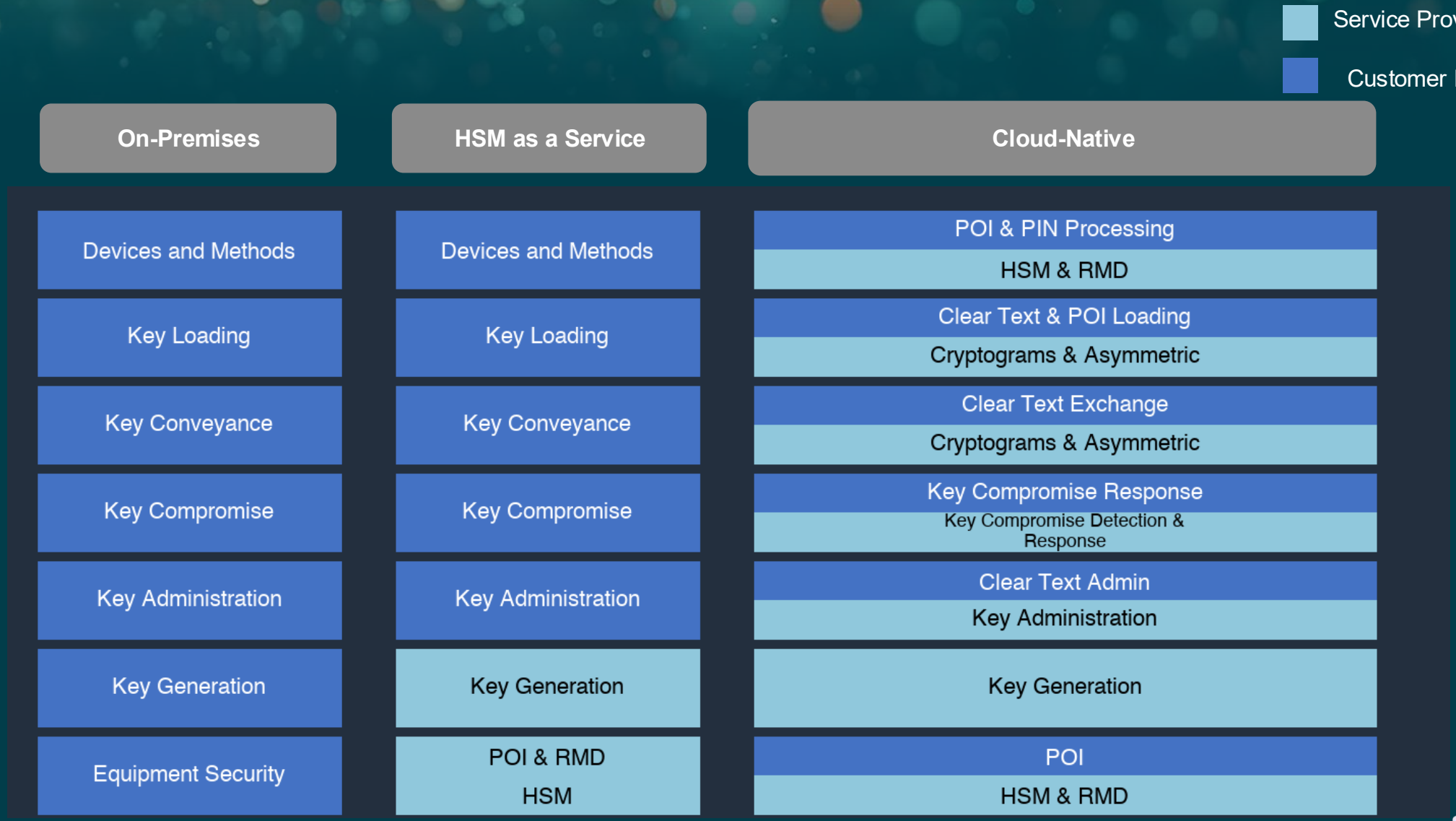
Dedicated or shared HSM Processing Elements. Virtualization system segregates tenant domains.

Suited for organizations prioritizing operational simplicity and scalability.

Best Practice: Service providers must define these boundaries in coordination with their assessor

20 YEARS OF SECURING PAYMENT DATA
PCI Security Standards Council

Comparing Compliance Responsibility Models



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 (CSP Owns)
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: 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. Evaluate control effectiveness, not control type
2. Require full identity context on every cryptographic operation
3. Map shared responsibility to your assessment scope before engagement
4. Scope reduction is real — Customers are taking advantage of it now
5. Cloud-native key management adds value: it takes responsibility off your plate while providing greater visibility

20 YEARS OF SECURING PAYMENT DATA
PCI Security Standards Council

Thank You

Rob Faba & Balaji Palanisamy
Amazon Web Services



Scan here for blog post

Simplify payment flows with cloud-based payment cryptography

Connect with us

Rob Faba
Fabarob@amazon.com
https://www.linkedin.com/in/rob-faba/

Balaji Palanisamy
Palanisa@amazon.com
https://www.linkedin.com/in/balajipalani/