HSM Virtualization for Payments and Enterprise: Compliance Strategies and Considerations

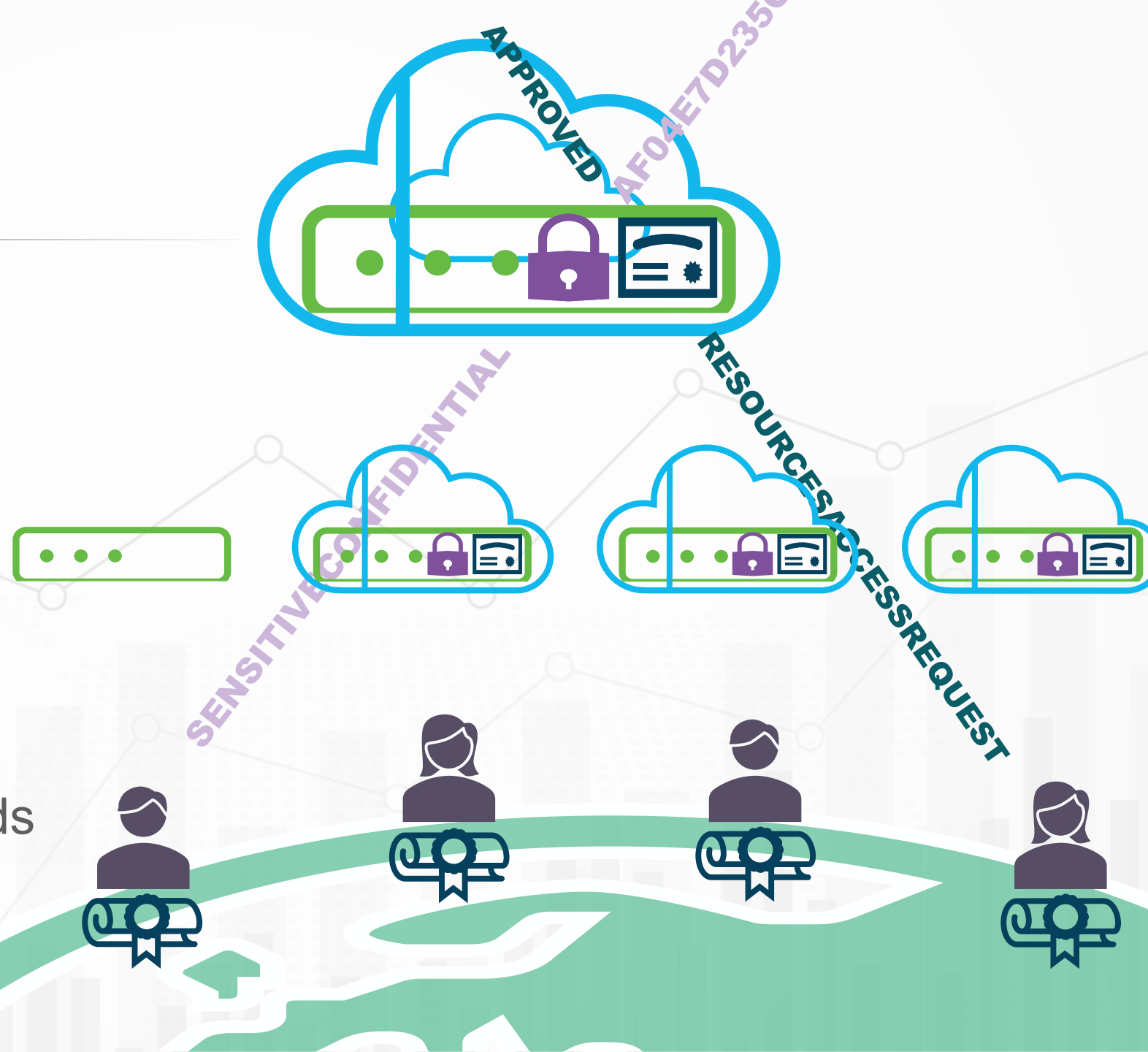
Adam Cason; Vice President, Global and Strategic Alliances, Futurex
Sam Pfanstiel, PhD; Principal, Coalfire (QSA, QSA(P2PE), QPA, 3DSA, SSF SSA & SSLCA)

State of the Industry

Industry Drivers for HSM Virtualization

Growth in:

- Cloud and Hyperscale
- Virtualization
- Data Protection
- Distributed Workforce
- Digital Trust
- Edge Cloud Security
- HSMs in Security Standards



PCI Security Standards Council

Cryptographic Use Cases for HSMs

- Data Encryption (P2PE, CHD Storage)
- Payments-specific (DUKPT, PIN, Issuing)
- Key Generation
- Key Management
- Signing of Public Certificates
- Code Signing
- Hardware Root of Trust (CA/RA)

All within a purpose-built, hardened, tamper-protected, lab-tested device

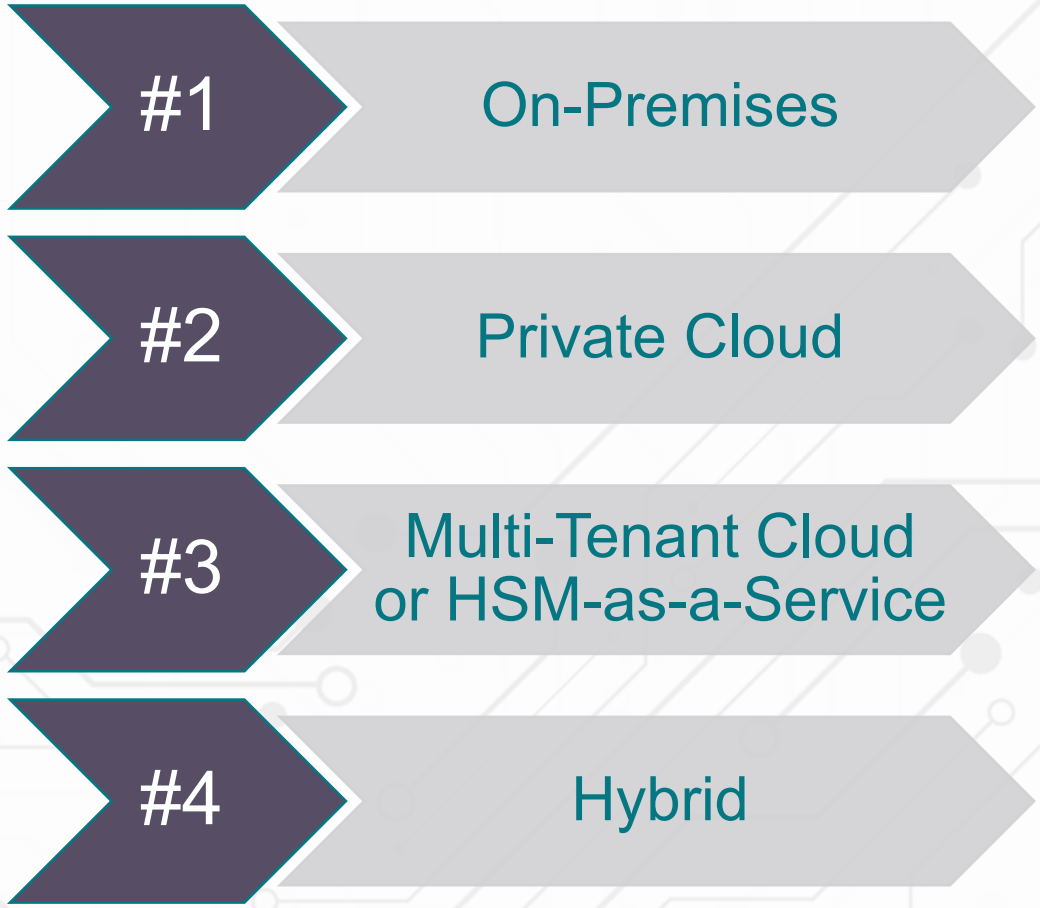
How Are Multitenant and Virtualized HSMs Deployed?

What are virtualized HSMs?

- Logically separated and isolated instances of HSM firmware, running on a single physical HSM, or across multiple cloud HSMs
- Indistinguishable from a standard HSM to the host application

What is HSM virtualization *not*?

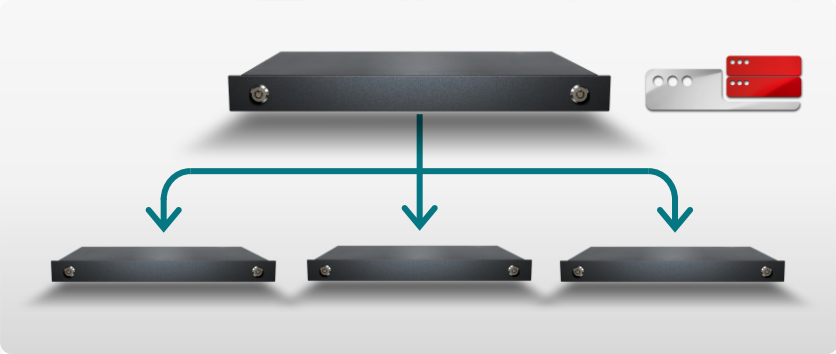
- Partitioning – although it does have its uses!
- Software-only HSMs – they still need to be operated from within PCI PTS HSM approved hardware security modules



PCI Security Standards Council

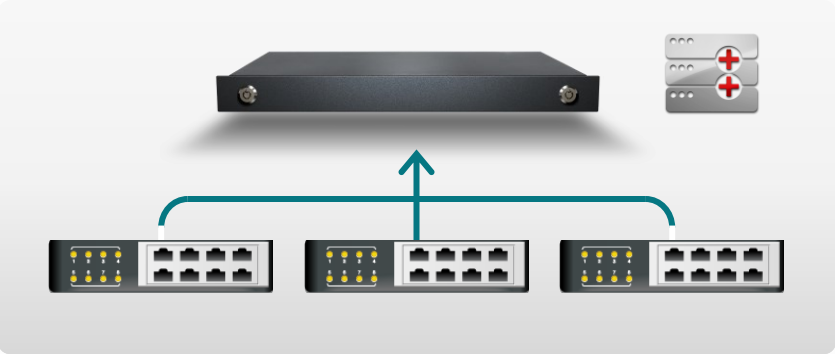
Overview of Common HSM Multitenancy Modes

HSM Virtualization



- Each virtual HSM is isolated from others
- Unique attributes per virtual HSM: firmware, security policies, configuration, keys, users, processing power, and network stack

Partitioning



- Relies on segmenting the HSM's internal key storage space
- Requires authentication to the HSM, which is tricky for payment applications
- Shared major keys between all partitions
- Each application has unique permissions, function blocking, and working keys

PCI Security Standards Council

Why Use HSM Virtualization and Multitenancy?

Cost Optimization

- Large enterprises often have distributed teams managing products from multiple vendors, often even running different firmware versions on devices that are part of a single fleet
- HSM virtualization enables consolidation without sacrificing utility or security
- Single teams are being tasked with HSM and key management infrastructure management
- End users can increase their security profile while reducing maintenance overhead

Revenue Generation

- HSM virtualization has actively created new revenue streams, particularly for payment application providers
- Virtual HSMs can form the basis for a cloud/SaaS offering for Payments-as-a-Service

PCI Security Standards Council®

Markets for HSM Virtualization

What organizations benefit from this technology?

Payments Enterprises

- Business Unit Isolation
- Scale
- Security

Cloud Service Provider (CSP)

- Customer Isolation
- Hyperscale
- Security Policies

PCI Security Standards Council®

How Does Implementation Look in the Real World?

- Data residency and other regional considerations
- The technology may be great, but who's going to manage it?
- Alignment with overall IT strategy and cloud migration
- Payment and general-purpose HSMs: together at last?

PCI Security Standards Council®

How PCI SSC is Responding

Community Involvement and Program Changes

2020 – Cloud Cryptographic Services SIG

- Update to Cloud Guidance
- PTS HSM Recommendations

2021 – PTS HSM v4

- Cloud-based HSMs as a Service
  - HSM Solution Providers
  - HSM Solution Customers
  - Multi-tenant HSMs
- Remote-managed HSMs

HSM Virtualization Compliance Considerations

Addressing Growing Needs within PCI Standards

- PCI DSS v4.0
  - HSM Option for Key Storage *(3.6.1.2)*
  - Targeted Risk Analysis and Strength of Customized Cryptographic Controls
  - TPSP must detail shared responsibilities for HSMs *(12.9.2)*
  - Appendix A1 for “Multi-Tenant Service Providers” - Logical Separation *(A1.1)*
- PCI SSF Secure Software 1.1
  - Where HSM is relied upon to provides cryptographic controls vendor security guidance must reflect configuration *(6.3)*

PCI Security Standards Council

HSM Virtualization Compliance Considerations

HSM Virtualization for PCI Standards with HSM Requirements

Virtualization

- Firmware Dependencies
  (P2PE, PIN, 3DS, TSP)
- Isolated Cryptosystem
  (PCI DSS 4 A1)

Physical Security

- Physically separating devices
  (CP-P 2.3.5.5, TSP 2.2.3, 2.6, 6.2.8)

Remote Access (“Non-console”)

- PTS HSM 4.x Module 3
  (TBD)
- ISO 13491 required
  (3DS, TSP)
- Clear-text key prohibited
  (3DS, TSP)
- Clear-text key loading in SCD
  (P2PE, PIN)

PCI Security Standards Council®

Conclusion

HSM Virtualization and Compliance Considerations

- Industry Trends That Led Us Here
- Business Drivers for HSM Virtualization
- Compliance Complexities Warrant Further Research

PCI Security Standards Council®