PCI Security Standards Council

PIN Processing in the Cloud

Ryan Day

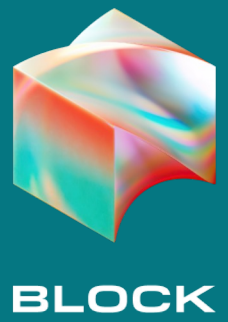
Product Security GRC Lead
Block, Inc.

Tim Winston

Principal Industry Specialist – Payments
Amazon Web Services

Skyler Ferran

Principal | Payments – Solution Validation
COALFIRE



TIDAL

What do you think Square sells?

PCI Security Standards Council®

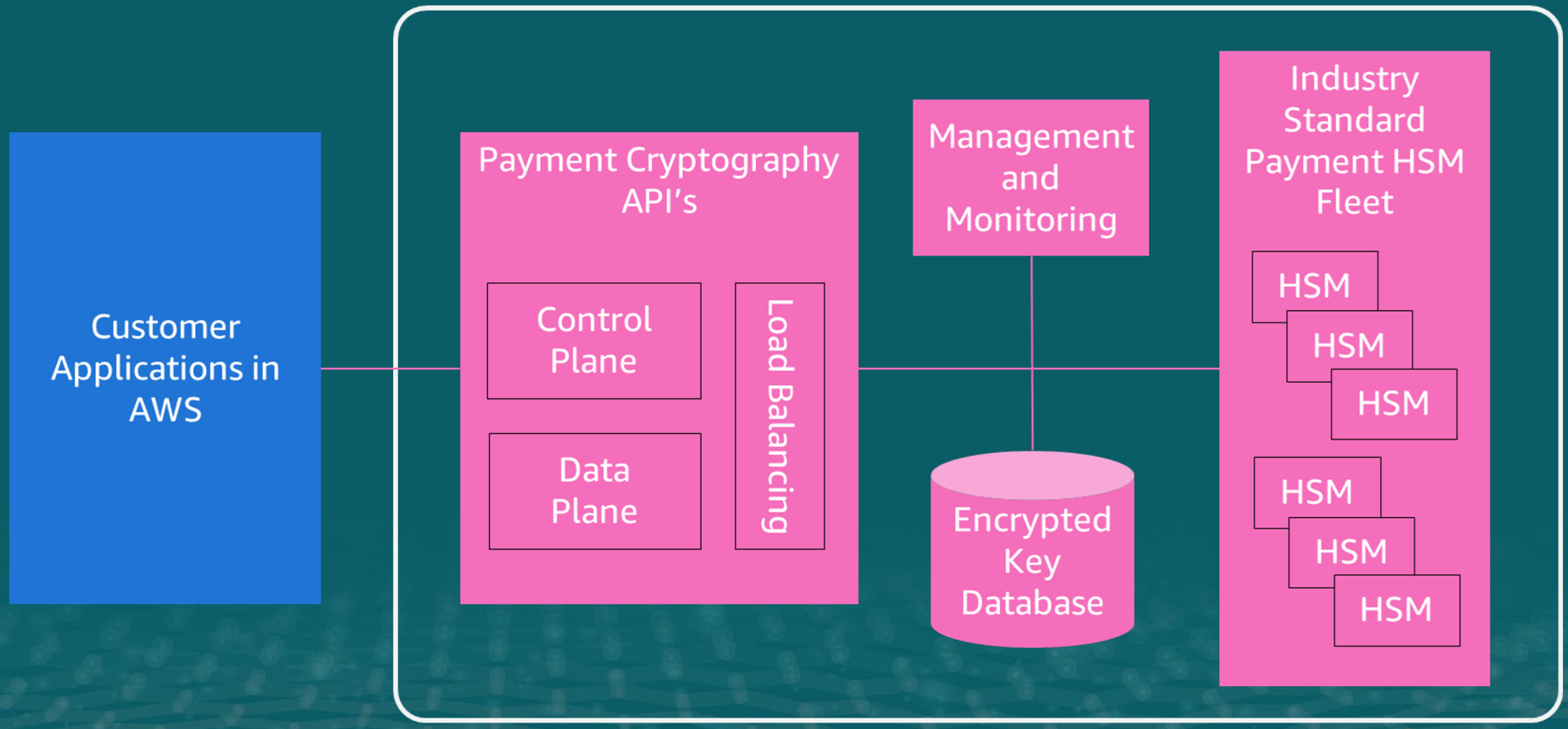
AWS Payment Cryptography: Cryptography-as-a-Service

- Shift maximum responsibility to the CSP
- HSM lifecycle, key management, and PIN protection
- Service owns HSMs and holds all keys
- Application requests functions via a web service API
- AWS-level security with payments compliance
- Visa definition of PIN-Acquiring Third-Party Servicer (TPS)

PCI Security Standards Council®

AWS Payment Cryptography:
Ownership of HSM, Key Management, and PIN Protection

- CreateKey
- DeleteKey
- ImportKey
- TranslatePinData
- VerifyPinData



PCI Security Standards Council

AWS Payment Cryptography:
Maximize CSP Responsibility

AWS Payment Cryptography

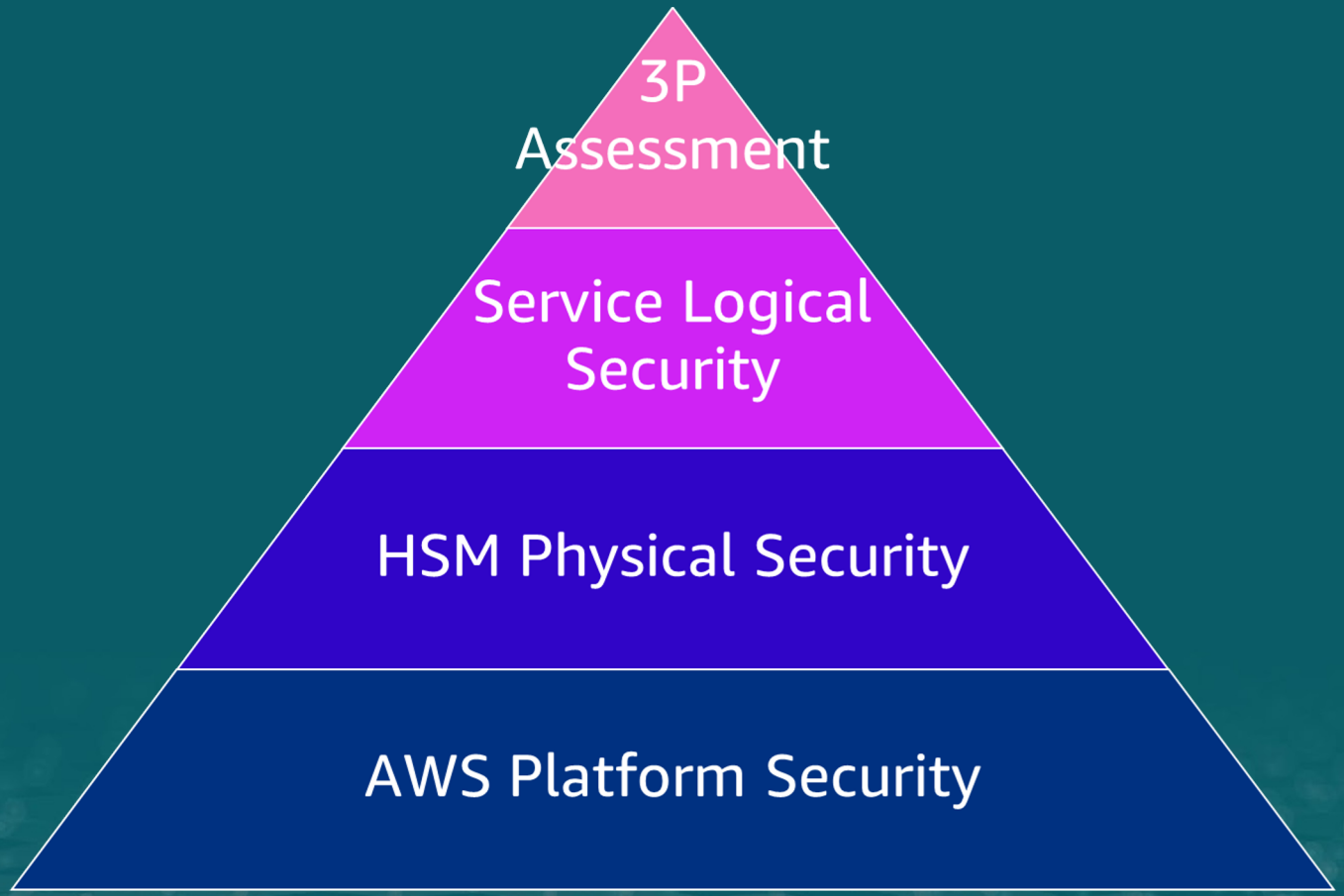
Feature	Responsibility
Physical HSM security	Service
HSM MK management	Service
Access control configuration of the HSM	Service
Functional HSM configuration	Service
Key storage, including access to MK protected keys	Service
Maintenance of key "ownership"	Service
Enforcement of key compliance	Service
Native HSM interface	Service
Requests specific cryptographic functions	Customer, as defined by use agreement
Receives results of individual or sequences of HSM commands	Customer, if defined by use agreement

HSM-as-a-Service

Feature	Responsibility
Physical HSM security	Service
HSM MK management	Customer, including sync with HSM outside the service
Access control configuration of the HSM	Customer
Functional HSM configuration	Customer
Key storage, including access to MK protected keys	Customer
Maintenance of key "ownership"	Customer
Enforcement of key compliance	Customer
Native HSM interface	Customer
Requests specific cryptographic functions	Customer
Receives results of individual or sequences of HSM commands	Customer

PCI Security Standards Council®

AWS Payment Cryptography:
Security and PIN Compliance



PCI Security Standards Council®

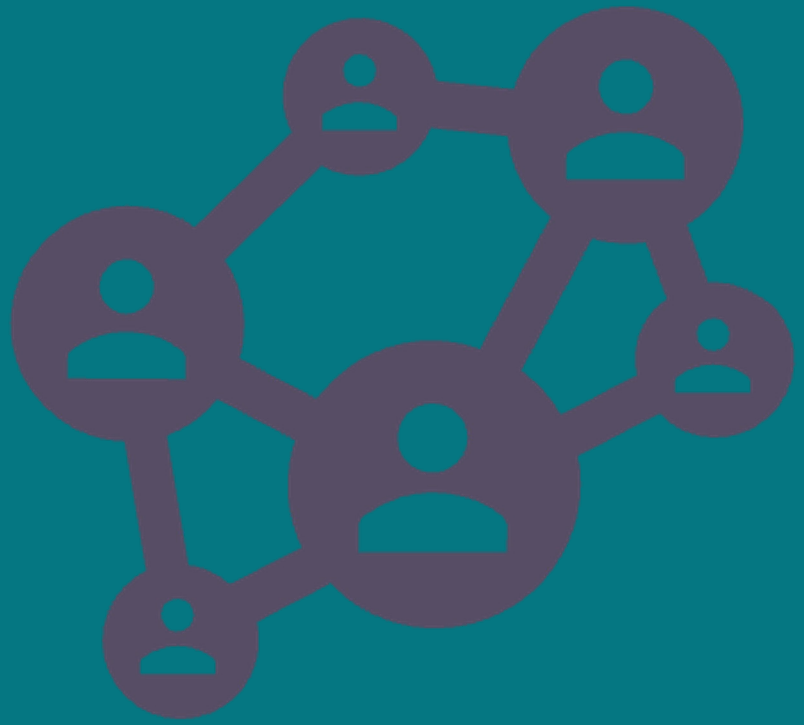
Assessing PIN for Amazon Payment Cryptography: Approach and Concerns

- A service, not another virtual hardware/cloud-based HSM
- Identifying appropriate controls and shared responsibility structure
- Key management; How are top-level keys established?
- HSM lifecycle in an inherently elastic and automated environment

PCI Security Standards Council®

Assessing PIN for Amazon Payment Cryptography: Solutions

- Building hybrid/logical controls to meet traditionally physical controls
- Key conveyance
- HSM inspections



What is the result of this collaboration?

Thank you