NIST Key Management Workshop

Cross-Domain Security Interactions: Scenarios and Solutions

Bob Griffin, RSA
John Leiseboer, Quintessence Labs
Saikat Saha, SafeNet

Agenda

- Cross-domain use cases and issues
  - Cloud key management
  - Hardware Security Modules
  - Quantum Key Distribution
- Discussion

Common Security Issues in Cross-Domain Key Interactions

- Trust establishment (contractual and on-line)
- Ownership of keys
- Protection of keys at rest
- Protection of keys in transit
- Propagating key policy
- Negotiating key policy
- Managing access to keys
- Managing key life-cycle
- Visibility of key-related services and infrastructure
- Proof of possession

Defining Cloud Key Management Models

Enterprise

- Keys created, used, stored and managed by enterprise

Hybrid

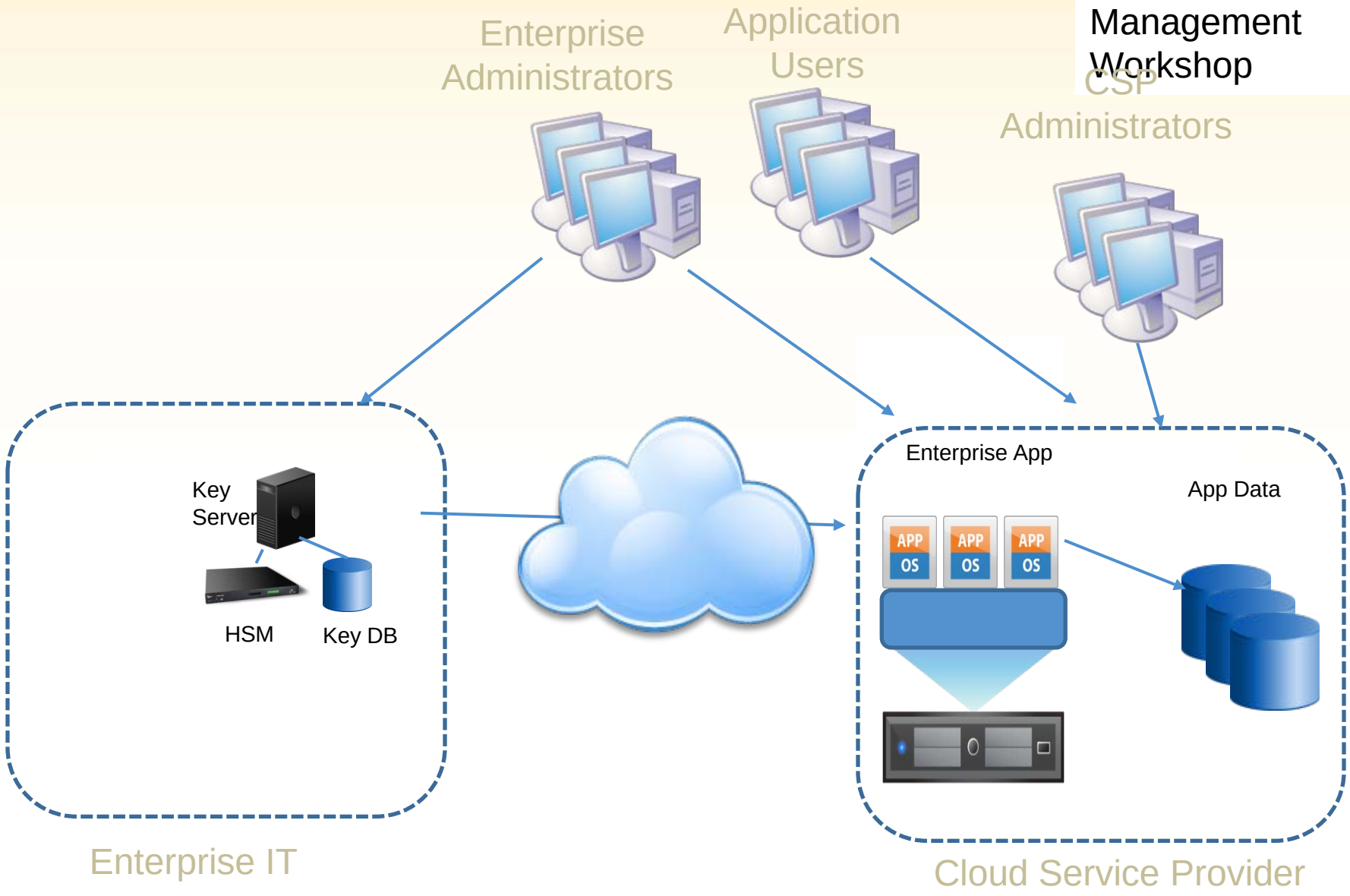
- Keys created, stored and managed by enterprise, but used by CSP

CSP

- Keys created, used, stored and managed by CSP

Hybrid Key Management

NIST Key Management Workshop

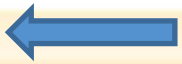


Cross-Domain Security Issues in Cloud Key Interactions

NIST Key Management Workshop

- Trust establishment (contractual and on-line)
- Ownership of keys
- Protection of keys at rest
- Protection of keys in transit
- Propagating key policy
- Negotiating key policy
- Managing access to keys
- Managing key life-cycle
- Visibility of key-related services/infrastructure
- Proof of possession



Agenda

- Cross-domain use cases and issues
  - Cloud key management
  - Hardware Security Modules
  - QKD
- Discussion

A Hardware Security Module is…

…a dedicated crypto processor…

…designed for protection of the crypto key lifecycle…

…validated for security by third parties…

…a Trust Anchor…

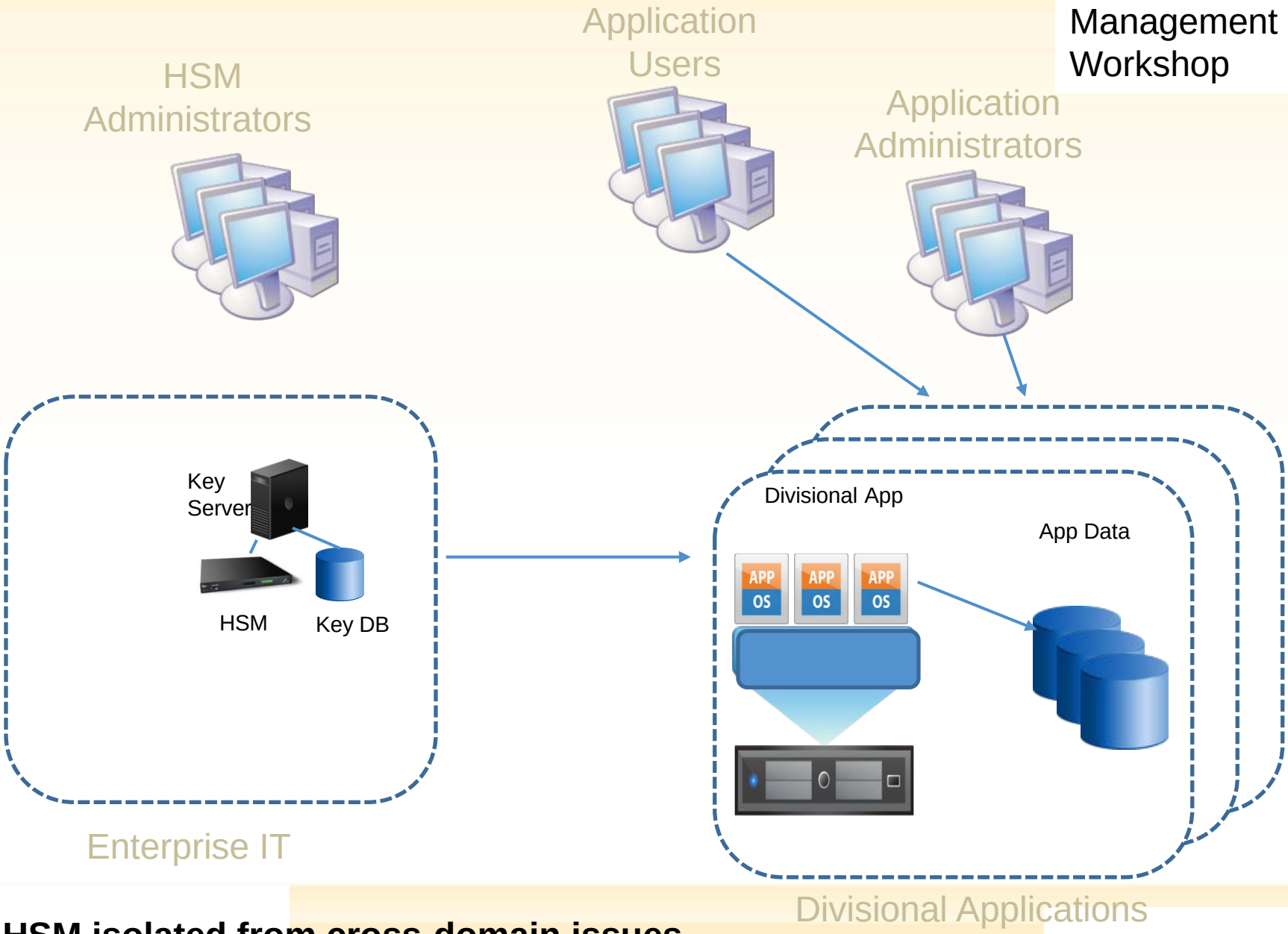
Virtualized Hardware Security Modules

Designed for Multi-tenancy

NIST Key Management Workshop

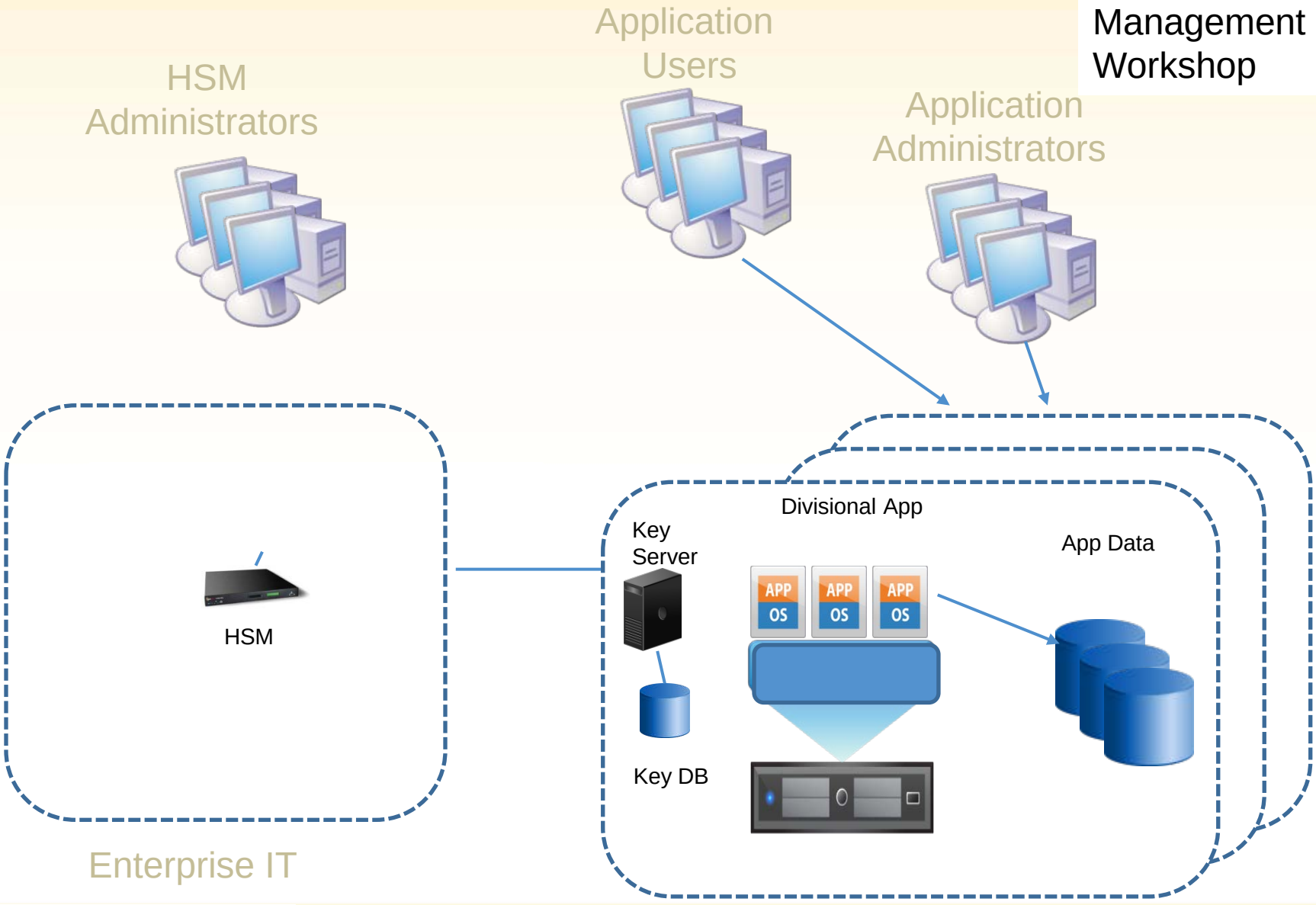
HSM/KM in Separate Domain from Apps

NIST Key Management Workshop



HSM isolated from cross-domain issues

HSM in Separate Domain from KM



Cross-Domain Security Issues in HSM Interactions

NIST Key Management Workshop

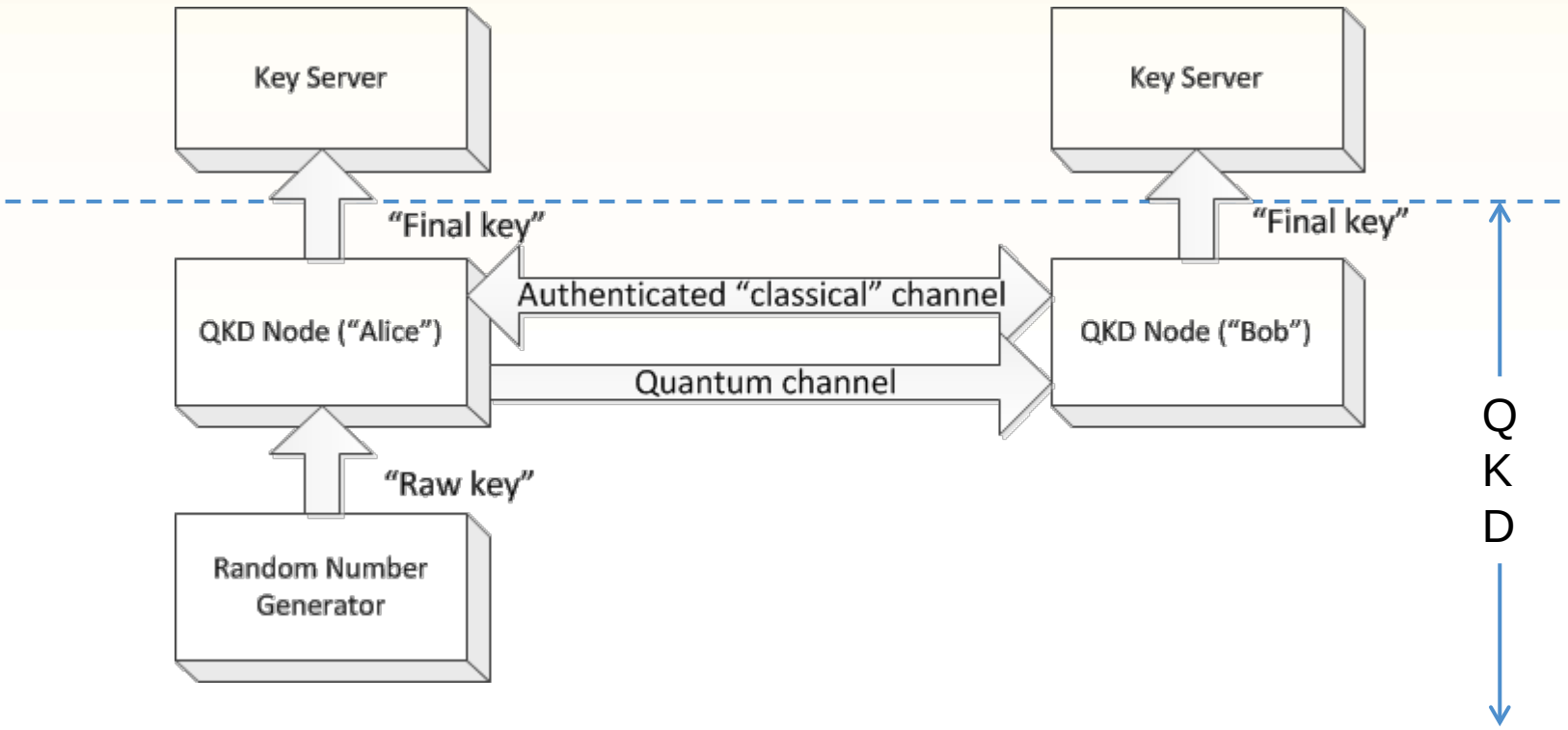
- Trust establishment (contractual and on-line)
- Ownership of keys 
- Protection of keys at rest 
- Protection of keys in transit 
- Propagating key policy 
- Negotiating key policy
- Managing access to keys
- Managing key life-cycle
- Visibility of key-related services and infrastructure
- Proof of possession

Agenda

- Cross-domain use cases and issues
  - Cloud key management
  - Hardware Security Modules
  - QKD
- Discussion

Quantum Key Distribution

NIST Key Management Workshop

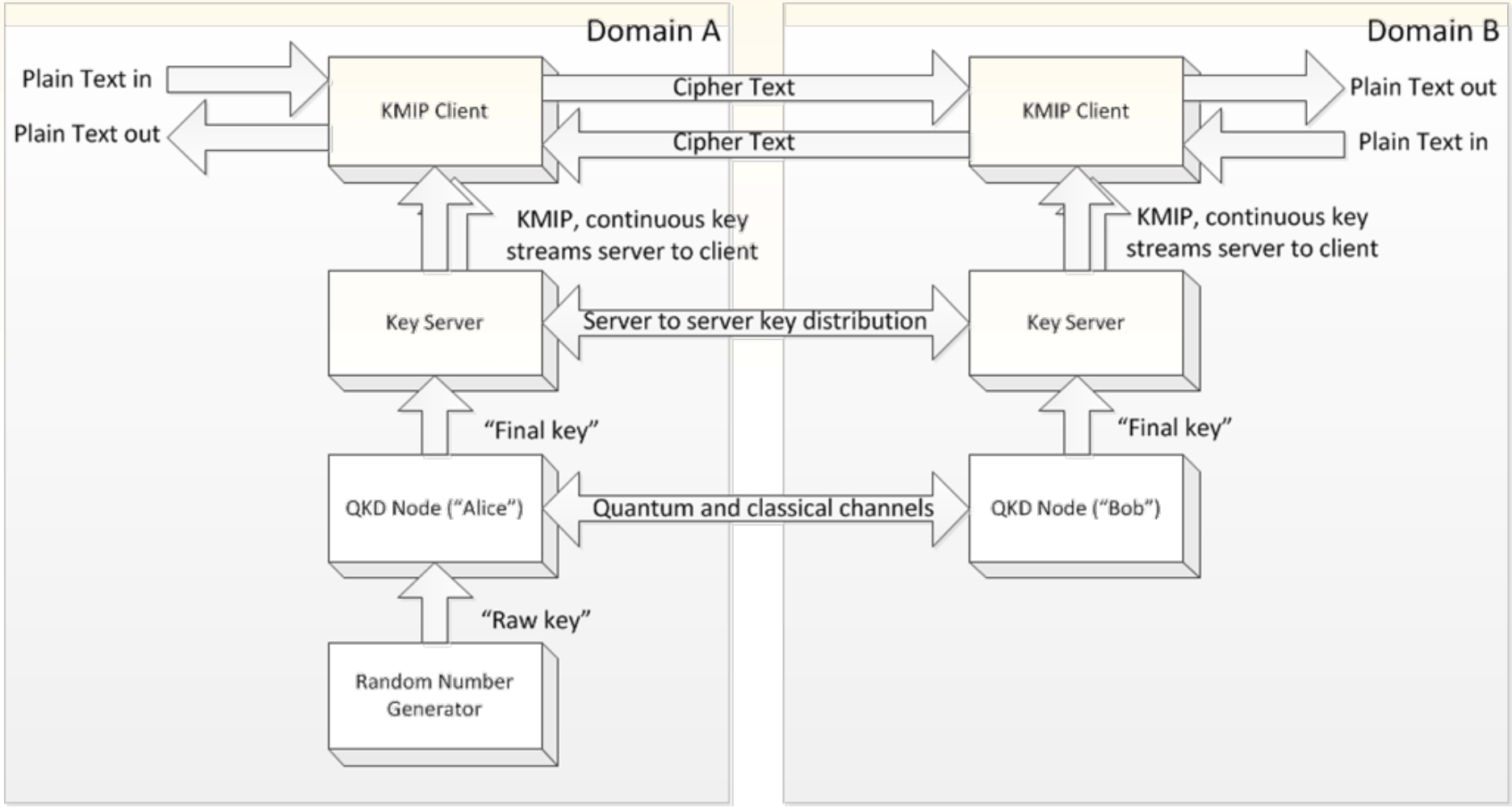


Raw key: True random

Final key: Secure, secret, replicated, synchronised true random

Key Streams and Periodic Keys

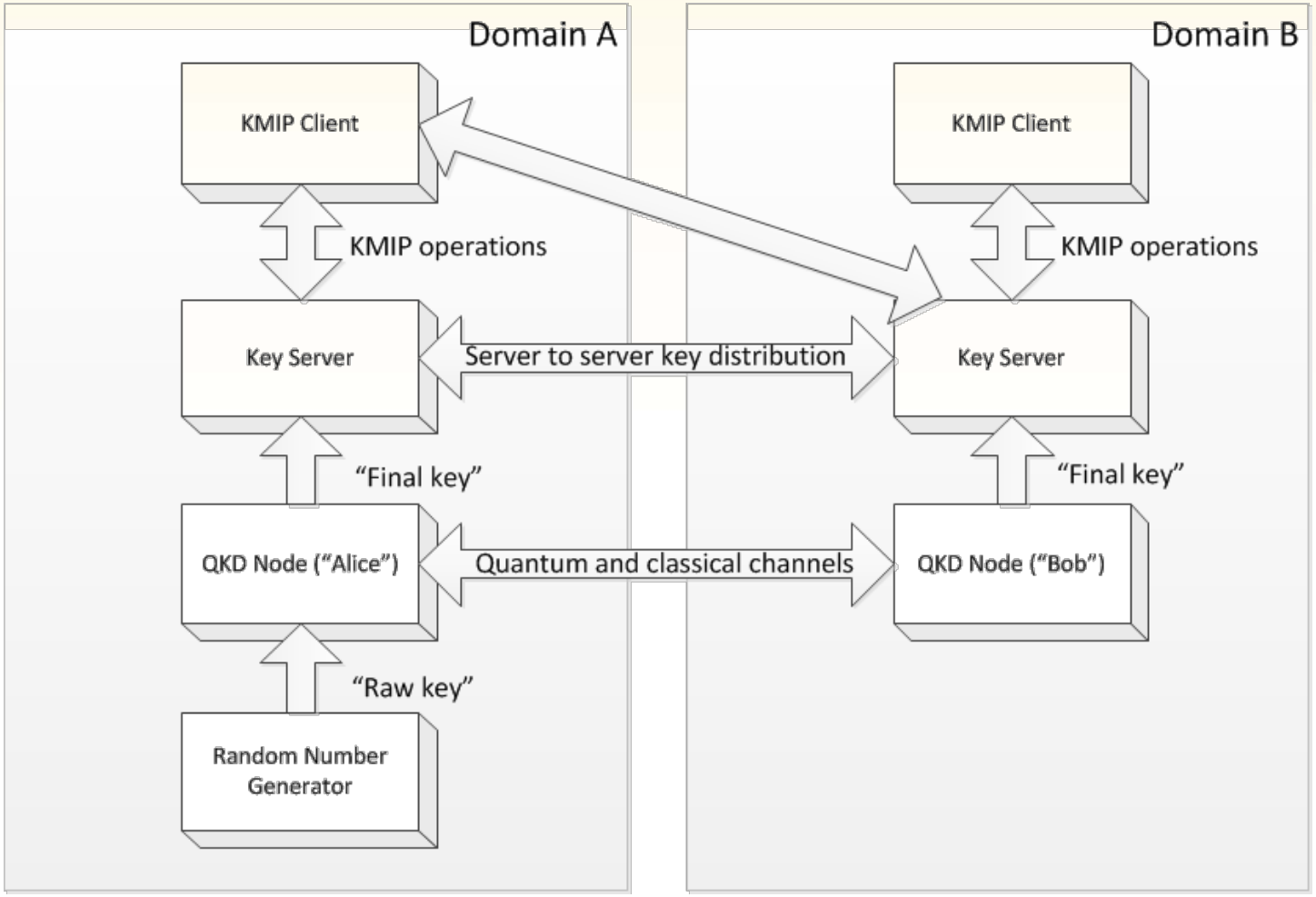
NIST Key Management Workshop



Server: Replicated, synchronised keys across domain boundaries
Client: KMIP operations with key server in same domain

Individual Keys

NIST Key Management Workshop



Server: Replicated, synchronised keys across domain boundaries
Client: KMIP operations with key servers in different domains

Cross-Domain Security Issues in QKD Interactions

NIST Key Management Workshop

- Trust establishment (contractual and on-line)
- Ownership of keys
- Protection of keys at rest
- Protection of keys in transit
- Propagating key policy
- Negotiating key policy
- Managing access to keys
- Managing key life-cycle
- Visibility of key-related services and infrastructure
- Proof of possession

Open Discussion of Cross-Domain Security Issues

- Trust establishment (contractual and on-line)
- Ownership of keys
- Protection of keys at rest
- Protection of keys in transit
- Propagating key policy
- Negotiating key policy
- Managing access to keys
- Managing key life-cycle
- Visibility of key-related services / infrastructure
- Proof of possession

Thank you!