There is No Cloud
There is Just Someone Else's Regulator

David Mortman @mortman

Bank of America

Bank of America Merrill Lynch U.S. Trust Bank of America Merrill Lynch

Cryptography

Cloud and Crypto: Asymmetric/TLS Keys

Asymmetric/TLS (for data in motion RSA Key pair (created and stored inside at least a FIPS HSM)

- Minimum of 2048 bits, 4096 preferred
- During TLS Handshake: -
  - All RSA signing (or decryption) mechanisms offloaded to and performed by the HSM
- PFS Symmetric session keys can be handled by Server

Cloud and Crypto: Symmetric Keys

Symmetric keys (for data at rest)

- Must Be:
  - AES, minimum of 128 bits, 256 bits preferred
  - MASTER Keys (e.g. CMK)
    - must be created and stored in a FIPS approved HSM
    - MUST be for customer tenants ONLY
  - Data level Keys
    - can be outside the HSM, but MUST be encrypted by Master

Cloud and Crypto: Background

- Key AWS services are not HSM enabled:
  - Elastic Load Balancer
  - API Gateway
  - AWS Certificate Manager
- Google and others have similar issues

Key Management

Data Destruction

Audit

Identity

There is No Cloud
There is Just Someone Else's Regulator

David Mortman @mortman

Bank of America

Bank of America Merrill Lynch U.S. Trust Bank of America Merrill Lynch