Key Management Automation

KMIP F2F 2020 Day 1
Tim Chevalier, NetApp
The Problem

• Security Best Practice via manual configuration fails
• Customers are demanding both secure and simple systems
• Manual configuration failures are common
• Poor security outcomes in deployment scenarios
• Different customers with different levels of “security”
Requirements

The user experience must be:
• Simple
• Automatic
• Verifiable

The underlying solution must be:
• Cross-vendor
• Secure
History

Remember the journey to the cloud and the **FUD**:

- *Only a toy*
- *No one will ever use it for anything serious*
- *It is inherently insecure*
- *You cannot trust the storage*
- *The CSPs will lose your data / steal your data*
- *HSMs / KMSs will never work in the cloud*
History

Today’s reality overcame the **FUD**:

- **Only a toy**
  - many major businesses are cloud only
- **No one will ever use it for anything serious**
  - cloud usage is mainstream and increasing
- **It is inherently insecure**
  - it is good enough for most needs
- **You cannot trust the storage**
  - the same storage reliability is available
- **The CSPs will lose your data / steal your data**
  - the same backup and recovery options are available no reports of CSP’s being responsible for data exfiltration
- **HSMs / KMSs will never work in the cloud**
  - most CSPs offer hosted HSM solutions and virtual KMS solutions and own KMS solutions
KMIP origins

- Primarily simple devices
- Primarily simple security requirements
- Capability for rich solutions
- Missing automation interfaces for configuration
- Client provisioning remains weakness despite
KMIP origins

- KMIP-1.1 fixed up minor issues
- KMIP-1.2 added cryptographic services
- KMIP-1.3 added streaming and client provisioning
- KMIP-1.4 client provisioning
- KMIP-2.0 fixed base protocol issues
- KMIP-2.1 adds new capabilities
KMIP gaps

Setup:
• Cannot create a user
• Cannot create a group
• Locked to client PKI

Verification:
• Cannot see what users exist
• Cannot see what groups exist
• Cannot see what security configuration is in place (permissions etc)
• Cannot check client PKI
Conclusion

- Automation is a major missing capability
- We have partial solutions to parts of the problem
- All the major CSPs have tackled this
- KMIP-3.0 needs to cover at least the basics
- We can no longer exclude automation from the problem domain