RSA 2020 Interop Demonstration Event

Tony Cox
Feb 2020
Rationale

• Requirement to show testing value
  – Participants
  – Industry expectations
  – Spec & Profile development

• Commitment to members
What actually happened...

• Per previous years – we’re using the abbreviated process until the OASIS Board approve something else.
• 1 week connectivity Test
• 2 weeks interop testing
• 1 late server entry – accommodated without fuss
• New results collection system in play – made the process much smoother (no spreadsheets)
• Results review was quick and very collegial/cooperative
• Results collation and review was relatively straightforward
• Good results for the group overall
Testing Process

- 7 Clients
- 7 Servers
- 7 Participating organisations
- ~51,000 successful test runs
- Testing scope was significantly higher than last year
- Same point to point testing setup as in previous years
- Limited (small) number of tests needed a subjective adjustment through analysis
- Specific Connectivity Test period test again eliminated some delays we’ve seen in the past
Testing Process
Testing Process
KMIP TC Interop Results
Feb 2020

Tony Cox

Graphs based on verified results from the OASIS KMIP RSA2020 Interoperability Demonstration Testing
Profile Conformance by Server

Profiles Passed

Cryptosoft KMIP C Server SDK
Cryptosoft KMIP Java Server SDK
PrimeKey SEE Key Manager Server
Quintessence Labs qCrypt
Utimaco Enterprise Secure Key Manager (ESKM)

- Tape Library v21
- Symmetric Key Lifecycle v21
- Symmetric Key Foundry v21
- Storage Array with Self-Encrypting Drives v21
- Quantum Safe v21
- PKCS#11 v21
- Opaque Managed Object v21
- RNG Cryptographic v21
- Basic Cryptographic v21
- Advanced Cryptographic v21
- Baseline v21
- AES XTS v21
- Asymmetric Key Lifecycle v21
- Tape Library v20
- Symmetric Key Lifecycle v20
- Symmetric Key Foundry v20
- Storage Array with Self-Encrypting Drives v20
- Quantum Safe v20
- PKCS#11 v20
- Opaque Managed Object v20
- RNG Cryptographic v20
- Basic Cryptographic v20
- Advanced Cryptographic v20
- Baseline v20
- AES XTS v20
- Asymmetric Key Lifecycle v20
Summary

- Most successful test yet – very cooperative
- The abbreviated Interop Process works
- Test Cases & Profiles were well tested and some adjustments made
- New results system worked well and aided clearer communication between participants
- Still minimal use of the Interop Identifier – consider use for future interops
- Thank you for everyone who contributed towards making this a flagship event for OASIS