KMIP Cryptographic Services

February 2013
Tim Hudson – tjh@cryptsoft.com
History

Previously:
- worked on multiple drafts with “interested” vendors
- presented at last F2F with general agreement to proceed as major work item for KMIP 1.2

Post-F2F:
- Updated to incorporate feedback on:
  - Streaming operations
  - Random Number Generators
  - MAC operations
- Competing non-compatible proposal from JohnL
History

Current:
- Based on other vendor feedback have backed out most post-F2F items
- Core Working Draft 5 - enc/dec/sign/verify/RNG
- Usage of RNG for nonce remains for Attestation
- Classification of RNG removed
- Prototype implementation completed
- Private interop testing soon
- Post F2F items for a subsequent version
Implementation of non-persistent operations as managed objects

- fundamentally these are different to what we currently have in KMIP

- As a TC we still have not reached agreement on adding in new managed objects for things like User/Client/Entity

- Adding managed objects for enc/dec/sign/verify/rng/etc – would these be one new object type or multiple? Lifecycle? Redefining existing operations? Adding new parameters for each operation? Persistence handling?
Discussion

Specification additions
- Require statements of use from at least three vendors which requires a level of commitment from vendors to implement/use

Suggested path (which we have adopted):
- Work out amongst like-minded vendors and develop an approach first
- Tackle a smaller scope initially and don’t accept helpful scope additions from other participants who are less committed to implementing