KMIP Interop

December 2013
Tim Hudson – tjh@cryptsoft.com
Expanded Tests

Need test cases for increased interop coverage

- Verify
- Derive Key
- Attestation
Variable Interpretation

Variable interpretation with:
- Locate
- Destroy
- Get on wrapped key where no (un-)wrapping key available
- Register with Key Value containing Attributes
- Register with Attributes and Value where they match but are duplicated
- Register with Attributes and Value where they do not match but are duplicated
Locate Interpretation

Variable interpretation with:

- Locate
  - Should objects which have been destroyed be returned?
    - One vendor returns destroyed objects in Locate, most vendors do not.
  - Should objects which are not returned in Locate be valid for other operations?
    - Some vendors that don’t return destroyed objects in Locate allow retrieval of attributes and performance of operations on objects which have been destroyed if the Unique Identifier is known.
Get Interpretation

Variable interpretation with:

- Register a key that is wrapped without wrapping key being available:
  - What does Get return
    - It cannot return a non-wrapped form of the key if it is unable to unwrap
  - What does Get with a wrapping key return when wrapped (unwrap/re-wrap?)

- Register allows for plaintext and wrapped keys
  - Not having the wrapping key is permitted which implies that the server is not expected to (always) unwrap what is provided

- Get allows for optionally specifying a wrapping key
  - Because a wrapped key without the unwrapping key can be registered then Get can return a wrapped key (as it cannot unwrap) without being asked to explicitly wrap.
Server Capability

Vendor choices for implementation vary and a client needs to be aware of it:

- Types supported for custom attributes
  - Non-interoperable for some vendors if non-TextString

- Number or instance count for custom attributes
  - Non-interoperable for some vendors if multi-instance

- Length limitations for custom attributes
  - Non-interoperable for some vendors if TextString > 64 bytes

Query interface does not yet return any information that helps here.
Other Interop Items

Vendor choices for implementation vary and a client needs to be aware of it:

- Setting of dates (and hence state) for objects associated with registered certificates based on NotBefore, NotAfter
  - Specification does not indicate to do this; nor does it preclude it being done
  - Side-effect is that the state after registration can be different between vendors and that is non-interoperable
  - Should it be left undefined (vendor-specific) variable interpretation?

- Revoke on linked objects
  - Should the action be propagated or precluded or left undefined?

- Destroy linked objects
  - Should the action be propagated or precluded or left undefined?