## Meeting Minutes KMIP Face-to-Face (F2F) Day One

## 27 February 2019

Meeting Commenced at 9:05 AM PDT

**Roll Call** (Tony C)

* Quorum achieved

**Approve F2F Day One Agenda**

***Motion to approve F2F Day One Agenda***

* Bruce R moves, Chuck W seconds, No objections, abstentions, or comments. Agenda approved

**Approve Previous Meeting Minutes (21 February 2019)**

***Motion to approve minutes from the 21 February 2019 KMIP TC Meeting***

* Tim C moves, Tim H seconds, No objections, abstentions, or comments. Minutes for 21 February 2019 are approved

**KMIP 2.0 Completion**

**Usage Guide Review (Judy F)**

* Judy F reviewed [Working Draft 01 of the Usage Guide](https://www.oasis-open.org/committees/document.php?document_id=64764&wg_abbrev=kmip) with the TC and discussed changes she made in this draft as well as changes she plans for the next working draft.
* Based on this discussion additional editorial changes were captured; Appendix B and D will be removed from the UG; and Section 4.10 on AES-XTS will be moved into section 3 and combined into the key encoding section (3.29).

**Usage Guide Editing (Judy F)**

* Reviewed list of outstanding KMIP 2.0 Usage Guide Content from the KMIP 2.0 proposals found on the TC Wiki (<https://wiki.oasis-open.org/kmip/2.0>)
* TC decided to work through the list in order and get the necessary UG text developed.

***Key Format Type (Bruce R)***

* Content developed during meeting

***Login (Tim H)***

* Content developed during meeting

***Delegated Login (Tim H)***

* Content developed during meeting

***Client Provisioning (Anthony B)***

* Anthony B to review Client Registration section in UG and provide redlines to accommodate for 2.0 changes.

***Client Re-Provisioning (Chuck W)***

* Chuck W to review Client Registration section in UG and determine if re-provisioning can be worked into this section (Chuck provide redlines) or if a separate section is needed (Chuck to provide new section content).

***Protection Storage Security (Bruce R)***

* Content developed during meeting

***MultipleIDPlaceholders (Tim H)***

* Content developed during meeting

**Break**

**KMIP 2.0 Completion (Continued)**

**Interop Test Review (Tony C)**

[KMIP Interop RSA2019](https://www.oasis-open.org/committees/document.php?document_id=64783&wg_abbrev=kmip)

* Tony C presented an overview of the 2019 Interop event and its results to the TC.
* TC discussed some of the alternative graphs that Tony C created with the interop data and what other analytics could be done
* Mark J asked if the interop data could be assessed to determine where test coverage for new functionality is weak. This information can be used to determine where additional test cases are needed. Tony C, Tim H, Mark J will work on figuring out how to assess the interop data.
* While Test Case contributions are greater than Usage Guide text it’s not by much so the Test Cases Co-editors welcome new test case contributions.

***Motion that all vendors have qualified for participation in the KMIP Interop Event at RSA Conference 2019***

* Tim H moves, Mark J seconds, No objections, abstentions, or comments. Motion approved.

**Specification Updates (Tony C)**

* Tony C walked the TC through a redlined copy of the Specification to review the updates which he recently made. Most of the updates were raised during the recent Interop event, but a few were outstanding review comments.
* Tony C asked the TC if there were other changes needed in the Spec. The following items were raised:
* In Authorization section where there is a list of credentials the Ticket structure needs to be added and the Ticket Type/Ticket Value should be removed.
* Resolve inconsistency in text and content between Digest (4.21) and Key Format Type (4.26) regarding how to handle digests for certificates and opaque objects. Key Format type is always required for objects, so it would be the easiest change.
  + Add Certificate, Opaque Object, Secret Data, PGP Key, Certificate Request to the Key Format type in 2.26
  + Also edit the enumerations for Key Format type
* Tony C will make the additional changes to the Spec and post the updated copy to the OASIS site.

**Test Case Updates (Tim H)**

[Test Case Items](https://www.oasis-open.org/committees/document.php?document_id=64781&wg_abbrev=kmip)

* Tim H took TC through the changes that need to be made to the Test Cases which came out of the Interop testing.
* TC agreed to all the changes that Tim H presented. He will post updated test cases to the reflector.
* An additional change to the Spec was also raised during this presentation regarding Fresh (section 4.24). For 2.0 the TC agreed to limit Fresh to only objects obtained via the Get operation and not the Export operation.
  + Also apply Fresh to all types of objects (not just cryptographic objects).
  + In KMIP 2.1 we can add a new attribute to address John L’s question about how to indicate if a key/object is new/not used.

**Statements of Use (SoUs) & 2020 Interop**

* The six vendors who participated in the KMIP Interop event are eligible to make the Statements of Use that required for the OASIS standards process. A minimum of three are required.
* Requests for a mid-year interop event have been made to Tony C. This will be considered if there is sufficient interest from the TC.
* Bruce R gave an update on the OASIS Board Interop discussion.
* Board pushed the definition of the interop policy back to the board subcommittee
* KMIP TC will be able to use our Interop policy until the OASIS one gets published
* Today there is one document on public OASIS events which covers both demos and showcases. Going forward, this document will be broken out into two documents one for show cases and one for demos. The KMIP Interop policy is being used as the basis for the demo policy
* OASIS Board election is being held May/June 2019, which might affect the momentum on the Interop policy. Bruce R’s seat is up for election.
* RSA Conference 2020 will be held February 24-28, 2020.
* Tony C asked if the TC was still interested in doing an interop event at this conference and there was overwhelming agreement that the TC should continue to do this. Folks did note that more time is needed to properly plan the event and the test cases need to be available well before the start of the Interop event.
* Tony C noted that we have new members to the TC who are interested in being involved in the Interop event. Tony would like to get back up to eight (or more) vendors participating in the event again.
* Tony C noted that the TC needs to give Jane H clear direction as to whether to reserve a booth for RSA 2020.

***Motion to run a KMIP Interop event at RSAC 2020, using the existing KMIP Interop Policy***

* Mark J moves, Tim H seconds, No objections or abstentions. Motion approved
* One comment from Chuck W that the TC should review the success of this year’s event (RSAC 2019) and look at alternative venues. The TC should revisit the topic within 30 days from the F2F meeting.
* TC Co-chairs will draft a note to the OASIS Board to state the TC stance that we are assuming that the Interop event at RSAC 2020 will use the existing KMIP Interop Policy. If that changes (and a different Interop Policy is required) then the participating vendors reserve right to back out from the RSAC 2020 event.

***Motion to (re)elect Tony Cox as the Interop Lead***

* Mark J moves, Jeff B seconds, No objections or abstentions, Tony C reelected Interop Lead.
* Jeff B offered to assist Tony C with Interop events. No objections to having Jeff B assist Tony C were voiced by the TC.

***Lunch***

**All afternoon discussions focused on KMIP 2.1**

* Tim H started a new table on the wiki to list the KMIP 2.1 F2F proposal decisions, owners and which KMIP documentations are affected. Please see the last table on this wiki page: <https://wiki.oasis-open.org/kmip/2.1>

**Name**

**Name Domain Definition (Tony C)**

[Name Domain Definition Proposal](https://www.oasis-open.org/committees/document.php?document_id=64784&wg_abbrev=kmip)

* Problem: Names need to be unique in a “Key Management Domain” but we never defined the boundaries of the “Key Management Domain and there is a lot of different approaches.
* Recommendation: Replace Server domain with a Logical Partition which is independent of hardware implementation
* TC discussed the proposal and its objectives
* Tim H felt this was more of a candidate for Usage Guide than Spec changes.
* Chuck W felt that the partitioning seemed analogous to a FIPS 140 cryptographic boundary. He proposed going with a local boundary (irrespective of implementation)
* After a long discussion TC agreed that the objective of the proposal was to find a way to support multi-tenancy. So given that could we not use a well-accepted definition of multi-tenancy and adapt it to address the logical separation of name.
* Tony C will take the multi-tenancy definition, adapt it to add in logical separation and make the KMIP Spec deltas and will present this at a future KMIP TC meeting.

***Motion for Tony C to bring forward an updated definition for Name Domain***

* Jim B moves, Bruce R seconds. No objections, abstentions, or comments. Motion approved.

**Namespaces (Anthony B)**

[Namespaces Proposal](https://www.oasis-open.org/committees/document.php?document_id=64785&wg_abbrev=kmip)

* Anthony walked the TC though the proposal around how to address the diversity in the different conventions that implementations are used for names and namespaces.
* Multiple solutions to the problem were presented, discussed and modified during the discussion.
* Do we need a separate namespace attribute or put the namespace within the name attribute?
* Anthony is going to go back and revise the proposal and present a new one at a future KMIP TC meeting.

**Rights for Object Groups (Bruce R)**

[Rights Object Groups Proposal](https://www.oasis-open.org/committees/document.php?document_id=64789&wg_abbrev=kmip)

Bruce R took the TC through his presentation

* Problem: Delegation is very popular and you like to restrict rights on delegation, but enumerating access on each group is very impractical.
* Solution: Allow groups of objects to be defined and assign access at a group level to simplify things.
* John L asked was there anything in Bruce R proposal which would break an implementation which was using groups already. No – This proposal is an addition, you can still assign rights individually.
* Discussion on how to figure out what object groups exist. We need a way to query a list of objects. Some discussion that this query of groups is more complex than just this access control case. Mark J and Jim B will bring forward a proposal to address query of groups.

***Motion to proceed with the Rights for Object Group proposal for KMIP 2.1***

* Mark J moves, Judy F seconds. No objections, abstentions, or comments. Motion approved.

***Break***

**Defaults**

**Query Defaults (Bruce R)**

[Query Defaults Proposal](https://www.oasis-open.org/committees/document.php?document_id=64905&wg_abbrev=kmip)

* Bruce R reviewed the Query Default presentation with the TC.
* In KMIP 2.0 we added one global default for all objects of a type (group). It would be good to have different defaults for different groups of objects. Use existing Object Group mechanism to differentiate between defaults.
* This may help with crypto agility, where one could use this to determine who was using a deprecated key algorithm and who migrated to use new key algorithms.

***Motion to proceed with the Query Defaults proposal for KMIP 2.1***

* Anthony B moves, Tim H seconds. No objections, abstentions, or comments. Motion approved.

***Motion for the co-chairs to request TC Admin provide the KMIP 2.1 documentation templates.***

* Tim H moved, Mark J seconds. No objections, abstentions, or comments. Motion approved.

**Query Defaults for Object Groups (Bruce R)**

[Query Defaults for Object Groups Proposal](https://www.oasis-open.org/committees/document.php?document_id=64788&wg_abbrev=kmip)

* Bruce R presented the proposal to the TC.
* Allow object groups to be a parameter in query so you can make a query against a specific group.

***Motion to proceed with the Query Defaults for Object Groups proposal for KMIP 2.1***

* Mark J moves, Tim H seconds. No objections, abstentions, or comments. Motion approved.

**Constraints**

**Set Defaults (Bruce R)**

[Set Defaults Proposal](https://www.oasis-open.org/committees/document.php?document_id=64787&wg_abbrev=kmip)

Note that the Title slide of the presentation is incorrect

* Bruce presented the proposal to the TC
* Proposes a new ***Set Default*** operation which provides an in-protocol way to set defaults.
* Mark J thinks this proposal requires updates to error codes for unknown object. Bruce R and Tim H concurred.

***Motion to proceed with the Set Defaults proposal for KMIP 2.1***

* Anthony B moves, Mark J seconds. No objections, abstentions, or comments. Motion approved.

**Default Constraints (Tim H)**

[Default Constraints Proposal](https://www.oasis-open.org/committees/document.php?document_id=64786&wg_abbrev=kmip)

* Tim H presented the proposal to the group.
* Problem: We can provide defaults for attributes, but we can’t provide constraints, like ‘must be AES 192 keys and not AES 128 keys’.
* Solution: Allow Constraints to apply to attributes. This is a building block that could be used to construct a policy.
* TC discussed the proposal
  + Sue didn’t like approach of putting constraints into Set Defaults. Tim H was happy to split the proposals and have a separate proposal with a ***Set Constraints*** option instead.
  + Discussion on how defaults and constraints are applied in a system and when a user would know there could be a conflict between defaults and constraints. For now, go with a simple list and it is an OR (one of constraints) must apply.
  + This proposal will also be useful with implementing a crypto agility plan where you can constrain use of certain algorithms and be able to change those algorithms constraints over time.
  + There will be additional reason codes that will need to be specified as part of this proposal.

***Motion to proceed with a Set Constraints proposal (separate from but modeled after Default Constraints) for KMIP 2.1***

* Sue G moves, Anthony B seconds. No objections, abstentions, or comments. Motion approved.

**Revisit Key Management Domain Discussion – Tim H**

* Revisiting the first presentation of the afternoon, Tim H presented a cut at defining the definition for key management domain.
* This started a very a very lively editing session to come to a definition on which the TC could agree.
* We ended the session with Tony C taking the action to refine the definition a bit more and bring it back to the TC at a future point.

**Call for Additional Attendees**

* None

**Next Meeting**

* Thursday, 28 February 2019

**Motion to adjourn**

Mark J moves, Tim H seconds. No objections, abstentions, or comments. Meeting adjourned

Meeting Adjourned at 4:00 PM PST