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

## 20 February 2020

Meeting Commenced at 9:08 AM PST

**Welcome and Roll Call** (Tony C)

* Quorum achieved

**Approve F2F Day One Agenda**

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

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

**Approve Previous Meeting Minutes (13 February 2020)**

***Motion to approve minutes from the 13 February 2020 KMIP TC Meeting***

* Tim H moves, Tim C seconds, No objections, abstentions, or comments. minutes for 13 February 2020 are approved

**Interop Review (Tony C)**

[RSA2020 Interop Review\_v3.pdf](https://www.oasis-open.org/apps/org/workgroup/kmip/document.php?document_id=66740)

* Tony C provided a summary of the Interop event which occurred at the end of 2019.
* There were 7 clients and 7 servers with 7 organizations participating (Fornetix and IBM have subsequently pulled out of the Interop and will not be at the booth at RSAC)
* 51K test runs. This was a much larger test scope at this event given both KMIP 2.0 and 2.1 were covered.
* Used a new results collection process this time which made testing details visible during live testing and also eased the post collation of results.
* Result review was quick. Many issues end up being data entry problems
* Results were used to tune KMIP 2.1
* Abbreviated Interop process is working well for our TC. Still have hopes that this will be adopted by OASIS.

**Interop Operation**

* Tony C raised the topic of the Interop operation, which was added in KMIP 2.1 to allow markers to be put in logs to indicate Interop testing, and the fact that this operation was not used by most participants in this recent Interop event. He asked the TC is this operation should be deprecated if it is not going to be used.
* Tim H (Cryptsoft) noted that it does have value especially is testing is more automated, but it would require that all participating in the interop event support the operation if it was to be of value.
* Mark J (P6R) noted that they were will into add it to their SDK
* John L (Q-Labs) noted they were also willing to support the operation.
* Fortanix which was another client interop participant was not present to comment.
* TC decided to leave the Interop operation in KMIP and make the use of this operation mandatory for the next Interop event.

***Motion to make use of the Interop operation mandatory in the next TC Interop event***

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

**Automation Problem Domain (Key Management Automation) (Tim C)**

[140-Automation Problem Domain.pdf](https://www.oasis-open.org/apps/org/workgroup/kmip/document.php?document_id=66752)

* Tim C took the TC through his presentation setting the context for need for key management automation.
* Cloud use cases are the primary motivators for automation. Automation at scale in a cost-effective manner is a requirement for the Cloud.
* KMIP while it is a rich protocol has gaps including automation interfaces, Client provision is still a deficiency.
* We will likely lose KMIP market share to the CSPs unless we address these gaps around automation. Need to consider a KMIP 3.0 which will cover the basics.
* TC members discusses their experiences with CSPs and what they are/are not doing about key management. The fact that each CSP has done something different has resulted in a mess since there is no cross-industry consistency and any customer or vendor that needs to work across multiple clouds is stuck supporting multiple approach. This is not unlike the situation with Storage/Tape Drives that resulted in the creation of KMIP more than a decade ago.

**Break**

**Automation Architecture (Tim H)**

[Automation Architecture.pdf](https://www.oasis-open.org/apps/org/workgroup/kmip/document.php?document_id=66719)

* Tim H went through his presentation. He took a step back reviewing historical proposals to determine why KMIP has not tackled automation before now.
* Tim H laid out a set of problem areas in KMIP and where there are gaps that prevent it being used for automation at scale, which is required by the CSPs
* Tim H then preceded to present potential changes to KMIP to address each problem space. This included the following:
  + New class of objects (System Objects) – Existing KMIP managed objects are for users of a system. The system itself needs objects. This will allow for automation and enable checking of secure configuration of a system prior to use.
  + Make sure we don’t mix these with the existing managed objects. But can certainly ‘borrow’ from the existing formats and leverage operations on both object classes.
* TC members raised questions and discussed Tim H’s proposal.
  + Sue G: Won’t system level objects potentially be at a higher level than user objects – so isn’t there a hierarchical/access control model needed? Tim H agreed this is needed and there is a presentation planned for Day 2 of the F2F to cover this topic.
  + Judy F: Regarding the desire to check the correct configuration of systems – How would this intersect with the existing attestation concept in KMIP? Tony C agreed that this needed to be looked at he felt that the system object concept could make attestation deeper since we would not be able to differentiate between carbon (human user) and silicon (platform).
  + John L recommended that we take a step back and provide examples of how the new system managed object would be used. While automation is a reasonable goad, he want to get a better idea of who, what and why we are automating.
  + Tony C observed that existing KMIP is pretty flat and we don’t have all the places where one could add in the hooks for automation in the protocol today. We have consistency in the KMIP model but need more levels of granularity to support automation hooks.

**User Handling (Clients and Credentials as Users) (Tim H)**

[Clients and Credentials as Users.pdf](https://www.oasis-open.org/apps/org/workgroup/kmip/document.php?document_id=66720)

* Tim review the existing Client and Credential capabilities in KMIP.
* It is possible to build a KMIP implementation without ever using a credential.
* Credentials are stackable. They can be used in combination and all ‘criteria’ of each need to be satisfied in order to be successful. Or in other words we only support AND and not OR.
* Use of credentials is the primary place where ‘users’ become visible in KMIP.
* In KMIP 2.0 we introduced Login/Logout with a ticket. All credential types can be used with Login.
* In KMIP 2.1 we added reprovisioning. This was essentially a way to replace out credentials (e.g. client certificates). **NOTE**: Test cases for reprovisioning are still needed.
* If we wanted to keep the certificates used for TLS separate for other credentials there hasn’t been a separate class for doing this.
* Tim H walked the TC through several create and distribute User & Credential examples.
* Bruce R asked if an object class should have been specified in the example to state user vs system class. Tim H agreed this was an omission and will be added.
* John L noted that in the current Destroy operation it may not destroy attributes related to the object being destroyed. What should be the behavior for users/credentials? In response TC discussed the need to keep state for users. We could model this after the NIST key state lifecycle.
* Discussion then turned to Credential and which of two approaches should be taken.
* Credential as a System Object: Credential is currently focused on what a client needs in order to do its job. Server would need more information in order to do its job.
* Credential stays as is as a passing mechanism.
* Jim S though a combination of both solutions would be needed since sometimes you need to be able to explicitly include an object vs a link to an object.
* Steve H noted that we need more access controls for users than keys. Others in the TC noted that we have sidestepped most privilege discussions in the past but felt that we should revisit this topic after we make some of these proposed changes visible in KMIP.
* John L wanted to make sure we cover things like handling broken links, error conditions, and rollback policy.
* TC consensus that this level of changes to KMIP would be a KMIP 3.0

**Alternate Encoding Format (Anthony B)**

[Alternate Encoding Format.pdf](https://www.oasis-open.org/apps/org/workgroup/kmip/document.php?document_id=66721)

* Anthony B took the TC though his presentation.
* Some users have high throughput requirements, others have slow bandwidth. TTLV encoding has a lot of padding, Booleans, etc. which makes it less than optimal for these type of users/environments
* Anthony proposed using the Concise Binary Object Representation (CBOR) to address these user requirements. CBOR is an industry standard (IETF RFC 7049) and is JSON like. It is used for transmission encoding and trades transmission efficiency over human readability. It is efficient to store and to process.
* CBOR would not replace TTLV encoding in KMIP. Instead this would be an optional additional encoding method. It is possible to convert from TTLV to CBOR
* Would need to investigate any IPR and licensing concerns with using CBOR in KMIP
* Will need to change the spec where the client tells the maximum size of the message which is based on TTLV (same held for JSON and XML)
* Mark J agreed it makes sense to look at how we can make KMIP smaller, but he had reservations about chopping 42 special bytes. He would like to see the Spec deltas and test cases first before making a final decision He also recommended leaving the message size open for now.

***Motion to investigate CBOR further with Spec Delta, Test Cases and Example Representations for TTLV and HTTP-S and ensure there are no IPR/Licensing concerns.***

* Jim S moves, John L seconds, No objections, abstentions, or comments. Motion approved.

**Lunch**

**NVMe KPIO (Judy F)**

[NVMeKPIO-KMIPF2FFeb2020.pdf](https://www.oasis-open.org/apps/org/workgroup/kmip/document.php?document_id=66707)

* Judy F presented the NVMe Key Per IO concept which is going through standardization in NVMe and TCG.
* NVMe KPIO drives will have encryption capabilities but unlikely the current SEDs, they will be able to take encryption keys from the outside world and applications/products that leverage the NVMe drive will be able to specify which key to used to encryption what I/O stream.
* Given that the drives are different from current SEDs the existing SED profile will not apply. So, a new KMIP profile will need to be developed for NVMe KPIO drivers. Its unclear if the NVMe/TCG standardization effort will be at a point to allow the new profile to be created for the next release of KMIP but we will monitor the timing as work on KMIP NG progresses.
* Participants the TCG effort have expressed interested in creating a liaison with the KMIP TC to discuss encryption and key management approaches. We can revisit this topic at a future KMIP meeting if a TCG liaison is desired.

**PKCS#11 Test Cases (Tim H)**

[PKCS11 XML for KMIP test cases.pdf](https://www.oasis-open.org/apps/org/workgroup/kmip/document.php?document_id=66722)

* PKCS #11 3.1 will be adding an XML-based test case notation. This aligns PKCS #11 with what KMIP test notation and in turn facilitates having a test case in PKCS#11 be reusable in a KMIP test case.
* No changes to protocol were made just change the test case representation to be more human friendly.
* There is no impact to the KMIP Specification or Usage Guide.
* The KMIP PKCS#11 Profile and Test Cases documents will be updated to describe this test notation and strategy.

***Motion that KMIP adopt XML representation of PKCS#11 for the KMIP PKCS#11 Profile and associated test cases***

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

**Split Key (Anthony B)**

[SplitKey.pdf](https://www.oasis-open.org/apps/org/workgroup/kmip/document.php?document_id=66723)

* Anthony presented three problems related to supporting and managing Split Keys with KMIP along with proposed changes to KMIP to address these problems.

1. Problem: There are multiple polynomials (GFs) over which the splitting algorithms are calculated.

Solution: Add a new **Split Key Polynomial** attribute. The attribute will have two defaults for the two commonly used polynomials

1. Problem: Missing Links for referencing the different split portions of keys

Solution: Add two New Link Types to handle references to the split portions of the keys

* **Split Key Base**
* **Joined Split Key Parts**

1. Problem: Missing attributes to describe split keys

Solution: Add the missing attributes:

* **Split Key Parts**
* **Key Part Identifier**
* **Split Key Threshold**
* **Split Key Method**
* Brief discussion on the name of the ‘Key Part Identifier’ Decision was made to no rename this attribute, just leave it as ‘Key Part Identifier’.

***Motion to add new Split Key Polynomial attribute, add the two missing links and add the four omitted attributes to KMIP NG***

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

**Client Mutual Authentication (Tim H)**

[Client Mutual Authentication.pdf](https://www.oasis-open.org/apps/org/workgroup/kmip/document.php?document_id=66724)

* Tim H provided the KMIP history on Client Mutual Authentication and proposed changes for KMIP NG.
* For 1.x client authentication was required except for a few operations (Query, Discover Versions)
* For 2.x client authentication was required for all operations
  + We also have KMIP authentication above and beyond the mutual authentication
  + In the market there are KMIP servers that exhibit all kinds of configuration options around KMIP over mutually authenticated TLS and KMIP authentication. In some servers there is no link between the client authentication and KMIP authentication. Which means many non-conforming servers exist in the market.
* Do we need to rethink authentication? Should we continue to keep TLS client authentication mandatory?
  + It’s a barrier for configuring KMIP
  + Cloud Service Providers don’t require it.
* Proposal: Relax the requirement for TLS client authentication on all KMIP operations (connections). If a client does not use TLS client authentication, then it MUST populate the Credentials in the KMIP header. KMIP Servers would need to make the choice of authentication configurable.
* Silence in the room while folks contemplated the proposal.

***Motion to move forward with this proposal and create KMIP Spec and Profiles deltas and assess the impact on test cases***

* Jim S moves, Greg S seconds, No objections, abstentions, or comments. Motion approved.

**Miscellaneous – Batch (Anthony B)**

[Batching.pdf](https://www.oasis-open.org/apps/org/workgroup/kmip/document.php?document_id=66725)

* Anthony discussed issues with Batch related attributes and proposed three be removed in KMIP NG.
  + Batch Count – Propose Removing
  + Batch Order Option – Propose Removing
  + Unique Batch Item ID – Propose Removing since it is used in Batch Order Option

***Motion to proceed with removing the Batch Count, Batch Order Option and Unique Batch Item ID in KMIP NG***

* Mark J moves, Klye W seconds. No objections, abstentions, or comments. Motion approved.

**Obliterate (Anthony B)**

[Obliterate.pdf](https://www.oasis-open.org/apps/org/workgroup/kmip/document.php?document_id=66726)

* Anthony present his proposal for an Obliterate operation for cases where Destroy is not enough.
* Destroy only guarantees that the object is destroyed. Many servers still retain attributes (e.g. meta data) for a destroyed object such as unique identifier.
* Anthony noted that there are cases when you need to destroy the object and all of its attributes.
* Discussed if different security controls are needed to be applied to Obliterate vs Destroy. Decided no.
* John L noted that Q-Lab has a vendor extension to Destroy called ‘Purge’
  + Tim H suggested that the new operation should be called ‘Purge’ vs ‘Obliterate’
  + There was a long discussion on the appropriate name for the new options. The TC Chairs will set up a Straw Poll to determine the name of the ‘Obliterate’ Operation
* Discussion on whether UUID would be deleted as part of this operation.
  + Decided to move forward with this new operation but to not remove UUID
  + UUID deletion/reuse will be revisited at a future date.

***Motion to move forward with spec deltas for the new ‘Obliterate’ operation. This operation will NOT remove the UUID***

* Mark J moves, Kyle W seconds. No objections, abstentions, or comments. Motion approved.

**Identifiers or References (Tim H)**

[Identifiers or References.pdf](https://www.oasis-open.org/apps/org/workgroup/kmip/document.php?document_id=66727)

* Tim H noted that Unique Identifier and several other attributes are defined as TextString
* Links referring to managed objects are also TextString
* By the Context you know whether the text string is a UID etc.
* However, we don’t have a way to type vendor attributes via context.
* Tim went through several solutions on how to address the problems with using identifiers and references
  + Solution 1 – Add a new Item Type – Reference – Applied to both User and System objects.
  + Solution 2 – Add a new Item Type – Identifier – Applied to Unique ID, Linked Object, & Vendor Attributes
  + Solution 3: Both solution -- Add two Item Types Identifier (for UID) and Reference (for objects)
    - UID would return as an type of Identifier but still encoded as Text String
* There is a related presentation (Referential Integrity) planned for Day Two of the Face-to-Face that folks wanted to hear before deciding to move forward on this proposal

**Locate Predicates (Anthony B)**

[Locate Predicates.pdf](https://www.oasis-open.org/apps/org/workgroup/kmip/document.php?document_id=66728)

* Anthony presented some limitations with the Locate operation.
  + Locate supports equality searches except for data ranges which is presently a hack to make it work.
  + Located does not support negation type searches.
* Anthony proposed adding explicit operators (Greater Than, Less Than) to Locate. This will allow specific data ranges to be met.
* Tim H suggested an alternative ‘Between’ Operation. The between would need to be inclusive of the end point values specified.
* In addition to the Spec, the Usage Guide and Test Cases will also need to be updated for this new ‘Between’ Operation

***Motion to move forward with Spec deltas for an ‘Inclusive Between’ Operation***

* Chuck W moves, Greg S seconds, No objections, abstentions, or comments. Motion approved.

**Close Day One (Tony C)**

**Call for Additional Attendees**

* None

**Next Meeting**

* Thursday, 21 February 2020

**Motion to adjourn**

* Tim H moves, Jim S seconds. No objections, abstentions, or comments. Meeting adjourned

Meeting Adjourned at 3:35 PM PST