## Meeting Minutes KMIP Face-to-Face (F2F) Day One 12 April 2018

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***

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

**Approve Previous Meeting Minutes (5 April 2018)**

***Motion to approve minutes from the 5 April 2018 KMIP TC Meeting***

* Tim H moves, Gerry S seconds, No objections, abstentions, or comments. minutes approved

**Secretary Nominations** (Tony C)

Tony C called for nominations for the open KMIP TC Secretary position.

No nominations were made so the secretary position remains unfilled

**F2F Proposals Rules of Engagement** (Tony C)

For each proposal presented over the two days the TC has to make a decision about each proposal with three options:

* More time/info is needed to proceed with the proposal for KMIP 2.0
* Approve proposal for inclusion in KMIP 2.0
* Reject proposal for inclusion in KMIP 2.0

For proposals approved it will be the responsibility of the proposer to develop the content for changes/additions to the Spec, Usage Guide, Profiles and/or Test Case documents.

Tim H started a new table on the wiki to list the 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/2.0>

**One Time Passwords (OTP)** (Tim H)

[OTP Proposal - Apr18 F2F](https://www.oasis-open.org/apps/org/workgroup/kmip/document.php?document_id=62856)

Tim acknowledged Anthony for his assistance with the slides

No consistent way to handle the OTP passwords in KMIP – different vendor approaches for concatenating the OTP with a password.

Propose adding a new OneTimePassword credential type

***Motion to add the new OneTimePassword credential type to KMIP 2.0***

* Gerry S moves, Mark J seconds, No objections, abstentions, or comments. proposal approved for inclusion in KMIP 2.0

**AKLC Review (Interop)** (Prashant)

Issue that arose in the interop of the AKLC profile test

Key format type of certificate digest coming back from servers were very different PKCS8, X.509. Returning a public key in a certificate format. - Not a PKCS1 formatted RSA key so you had to derive it.

Moved to Key Format proposal since it may resolve this interop issue.

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

[Key Format Proposal - Apr18 F2F](https://www.oasis-open.org/apps/org/workgroup/kmip/document.php?document_id=62857)

Problems:

* No way to specify Key Format Type in Constructors
* No well-defined default Key Format for Constructors
* Inconsistent digests are produced
* Get without a Key Format Type produces inconsistent results

Solution is to define a new Key Format Type attribute. This can be specified on Create, Create Key Pair, or Derive Key. If the client doesn’t provide one then the server will generate one for you. The server will have to support all key format translations. Eases the issue for the client having to figure it out themselves or dealing with translation.

Prashant agreed that this proposal would have solved the issue he presented from the Interop

This proposal will require Profile changes as well as Specification changes

John L asked about certificates and PGP keys – Certificates are deterministic. Bruce noted that he will cover these in the proposal.

***Motion to move forward with this proposal for KMIP 2.0***

* Bruce R moves, Mark J seconds, No objections, abstentions, or comments. proposal approved for inclusion in KMIP 2.0

Had a brief discussion around PGP keys, whether anyone is using them. The TC options were

* Do nothing (leaving PGP keys in the 2.0 Spec)
* Deprecate (them in 2.0)
* Remove (them in 2.0)
* Do PGP keys correctly in 2.0 or a future release

TC opted for removal. A ‘migration’ approach for PGP should be covered in the Usage Guide

PGP keys can be carried in an opaque object and use vendor extension to say it’s a PGP key. John L to provide Usage Guide text.

***Motion to remove PGP Keys as a Key Type in KMIP 2.0***

* John L moves, Mark J seconds, No objections, abstentions, or comments. PGP keys will be removed from KMIP 2.0.

**Break**

**Cryptographic Usage Mask** (Nitin)

1. First issue: Cryptographic Usage Mask presently applies to all objects which doesn’t always make sense. So we need information in the Specification to state which objects a specific cryptographic usage mask value applied to.
2. Second issue: The purpose of some of the usage mask descriptions are not clear and need better descriptions. Some of the text in the Usage Guide can be moved into the Specification to provide clarity. Other descriptions will need to be added.
3. Third issue: Unused cryptographic usage masks should be removed

TC discussed a number of the cryptographic usage masks and their meanings

* Derive Key: Two types of secret data – one where you want to derive key material from and some (like a password) that you don’t. Derive key usage mask applies to all secret data objects
* Encrypt (pubic) & Decrypt (private): This is the general case, but there is an opposite case used to show proof of possession where the private is used to encrypt and public is used to decrypt.
* Export usage mask doesn’t control export of a key from a HSM – that is done via the sensitive and exportable (PKCS#11) attributes.

***Motion to remove Export cryptographic usage from KMIP 2.0***

* Mark J moves, Bruce R seconds, No objections, abstentions, or comments. Export usage will be removed from KMIP 2.0 Specification but the bit will be left as reserved

Observation made that we are mixing too many concepts with cryptographic usage mask and that we should split the discussion out into

* Things that servers need to adhere to
* Things that clients need to adhere to
* Properties/attributes of the outcomes – NonRepudiation/ContentCommit is a property of the signature –sits within the certificate

Nitin raised two new usage mask options – unexportable and undeletable. TC discussed these and agreed that they are attributes not cryptographic concepts. KMIP already has the unexportable attribute now. Undeletable could be added as an attribute but the use case for this was unclear – folks felt it was too implementation specific.

TC also discussed the TR31 Usages:

* Generate/Validate Cryptogram
* Translate Encrypt/Decrypt/Wrap

KMIP doesn’t have operations that use these currently but folks didn’t want to remove these without checking with folks that know the payments requirements better than those attending the TC meeting.

Based on this discussion, Tony C and Chuck W will take a stab at the clarification/clean up of the cryptographic usage mask content in KMIP 2.0 Specification

**Hash Passwords** (Anthony Berglas)

[Hashed Passwords Proposal - Apr18 F2F](https://www.oasis-open.org/apps/org/workgroup/kmip/document.php?document_id=62858)

Problem: Passwords are sent in clear, but some upstream systems don’t allow/provide plain text passwords

Solution: Send a hashed password and include a nonce to prevent reply. Server provides different hash to prove possession of the initial password. Store the double hashes at the server. These would be sent in the Credential Type and the Name will be ‘Hash’.

Some issues with the presentation slides were noted and should be reflected in the final Specification changes:

* Need to genericize this to use any viable hash algorithm. SHA256 can be set as the current default.
* ‘Timestamp’ in proposal will change to ‘credential nonce’ to prevent confusion with other timestamps
* Bytestream typo is corrected to ByteString

***Motion to accept this proposal with the changes noted above for inclusion in KMIP 2.0***

* Mark J moves, Gerry S. seconds, No objections, abstentions, or comments. Proposal with noted changes will be included in KMIP 2.0.

**Login Operations** (Tim H)

[Login Operations Proposal - Apr18 F2F](https://www.oasis-open.org/apps/org/workgroup/kmip/document.php?document_id=62859)

Problem: Need to put username/password in each request. Not the normal practice when using external directories and it makes the messages look verbose.

Solution: Introduce a Login Operation that returns a login Ticket. The ticket can be used during a KMIP session. Login can request a Ticket for a fixed time or for a usage limit. A Logout Operation invalidates the ticket. This would be an optional operation either if fixed time/usage is not used or if you want to invalidate the token sooner than its expiration. The ticket value is up to server to define for what makes sense for its environment.

How does this apply to batch? – Right now you can request this ticket anywhere in the batch.

***Motion to accept proposal for inclusion in KMIP 2.0***

* Jim S moves, Chuck W seconds, No objections, abstentions, or comments. Proposal will be included in KMIP 2.0

**Lunch Break**

**Delegation** (Tim H)

[Delegation Proposal - Apr18 F2F](https://www.oasis-open.org/apps/org/workgroup/kmip/document.php?document_id=62860)

Problem: Clients want to delegate authority to perform an action on their behalf. Current way has been to share credentials which is not appropriate. KMIP has no concept of delegation, but adding to address common client use cases.

Solution: Delegated Login Ticket (already has Lease Time and Usage) need to further limit its use in the delegation case. Need to know what Objects it applies to and what Operations are allowed or denied.

Can invalidate Login with a Logout operation (proposal discussed earlier). Can be combined with Login and can support Two Factor Authentication.

John L noted that the Quintessence Labs server has this delegation feature. If added to KMIP it needs to be an optional features since it allows client to dictate policy the server can follows.

CryptSoft noted that they currently support delegation via KMIP extensions

Clients need to be able to delegate independent of which server they work with.

Chuck thinks some use cases/Usage Guide text and test cases to show examples of what can be done with this are needed.

Chuck also ask for extension to be consider in proposal (Tim H and Chuck to discuss further)

Chuck also made observations that attributes was missing– like which set of attributes a delegate can affect.

Steve W wanted more time to think about this proposal.

***Motion to progress this work for inclusion in KMIP 2.0***

* Bruce R moves, Mark J seconds, No objections, abstentions, or comments. Work on proposal will progress for KMIP 2.0

**Client Provisioning** (Anthony B)

[Client Provisioning Proposal - Apr18 F2F](https://www.oasis-open.org/apps/org/workgroup/kmip/document.php?document_id=62861)

Problems:

* Simple client provisioning uses username/password.
* Need to clarify existing approaches and need to define what goes into provisioning request.
* The Client Registration Method enumeration missing test case

Proposed mandating support for client provisioning in KMIP 2.0 and modifying Client Registration Method to support PKCS#12.

Authentication for the provisioning request is over a server side TLS connection. The password used to protect the PKCS#12 is shared with client and that is a level of authentication of server since password to unlock PKCS#12 has to be pre-shared with client.

* Server Pre-Generated
* Server On Demand
* Client Generated (CSR)
* Extend query on PKCS#12 to get certificate in fewer operations
* Client Registered

How to handle renewal? Should we cover this in this proposal or keep separate? The TC desire was to keep renewal separate.

There is no mechanism to re-provision either client or server TLS certificates in KMIP today – Definitely agree it’s needed. Complete this initial provisioning proposal first then work on the re-provisioning. John ask that if we mandate provisioning we should also to the same for re-provisioning

***Motion to progress proposal for inclusion in KMIP 2.0***

* Jim S moves, Judy F seconds, No objections, abstentions, or comments. Work on proposal will progress for KMIP 2.0

**Break**

**Protection Storage Security** (Bruce)

[Protection Storage Proposal - Apr18 F2F](https://www.oasis-open.org/apps/org/workgroup/kmip/document.php?document_id=62862)

Problem: How is a key be protected at the server? Can the client get information and ask for certain protections?

Solution: Add Protection Storage Mask for objects.

Protection Storage Mask example discussed with the following additions to the proposal recommended:

* Need to add a location type flag (white list a list of countries and/or regions) so you can restrict where keys can be stored to deal with HIPPA, GDPR, another restrictions. Use ISO country codes.
* Client gets to specify minimum protection requirements
* Add microservices and clusters to the storage mask list

It was noted that that query changes are also required for this proposal

***Motion to progress proposal for inclusion in KMIP 2.0* with the addition of Location, Microservices, Clustering**

* Mark J moves, Gerry S. seconds, No objections, abstentions, or comments. Proposal with noted changes to be included in KMIP 2.0

**Multiple ID Placeholder** (Tim H)

[Multiple ID Proposal - Apr18 F2F](https://www.oasis-open.org/apps/org/workgroup/kmip/document.php?document_id=62863)

Problem: Too many id options and related functions use different options

Solution: Leave ID Placeholder as is. Allow an explicit indication of origin of Unique Identifier so it can be used in multiple places (type Enumeration). Allow actions to be performed or not performed on a list of know ids. Unique Identifier – Type Integer (matches test case usage).

Sue asked about how to handle multiple locates in a batch? – This proposal only looks at one (most recent) Locate to keep it simple. You would have to structure your batches differently to keep locate to one. Also presumes synchronous only – More description (Usage Guide text) to cover this scenario.

***Motion to include proposal in KMIP 2.0***

* Chuck W moves, Gerry S. seconds, No objections, abstentions, or comments. Proposal to be included in KMIP 2.0

**Interop 2018 Review** (Tony C)

[RSA2018 Interop Review - Apr2018 F2F](https://www.oasis-open.org/apps/org/workgroup/kmip/document.php?document_id=62864)

8 clients, 10 servers

33K successful test runs

Connectivity Test period eliminated some of the delays we’ve seen in past interops.

* Mark suggested we expand connectivity test to check that the Server’s time is properly set.
* Not just connectivity – expand to run a successful query and possible discovery. This query will also check the server time issue that Mark raised

TC reviewed the results of the testing

TC discussed the common slides for the vendor presentation

John L asked about which template to use for the vendor presentations. TC agreed that vendor use their own slide templates (not OASIS).

Open discussion on Interop Experiences

* John L actually liked the shorter test cycle
* Tim H though shorter time to resolve issues was great
* Like dropping the manual configuration tests was good – keep this to a minimum
* New vendors this year were better on communicating
* Thad felt it was really rushed from a new vendor perspective
* No significant changes to KMIP 2.0 (Mark) came out of the Interop
* Keep the number of tests around the same level – limit to newer version only
  + So if we limit this way how do on-board new vendors? – Plug fests are one way of doing this
* Add more frequent plug fest during the year (incremental testing) can be used to test out new
* SNIA dropped the interop testing
  + How to get a more public venue to show which clients work with what servers?
  + Gap in consistent industry adoption
  + Server vendors put in place for testing
* Can we either drop or flag test cases that cause the tests to fail (Thales DSM runs in FIPS mode) – GCM test cases – Will move these so they don’t fail. Another KMIP 1.4 errata candidate.

Tim H noted that more OASIS board members will be visiting the booth (at least two will be at event) could be up to four, since there is more visibility about Interop testing at the board level.

**AI Review/Day 1 Wrap-up** (Tony)

Participation in 2019 conference will be discussed/voted on Friday (tomorrow) (showcase or interop)

PKCS#11 TC elected not to commit to an interop next year since some vendor can’t make the go/no-go in the timeframe. PKCS#11 co-chairs will talk to ICMC (international crypto module conference) to see if they could host the P11 interop next year (May in DC area)

Also talk about booth sharing and pod sharing

Review wiki list of actions

**Call for Late Arrivals** (Tony C)

* One Member (Thad)

***Motion to Adjourn***

* Jim S moves, Chuck W seconds. No objections, abstentions, or comments. Meeting adjourned

Meeting Adjourned at 4:13 PM PDT