# OASIS KMIP F2F Day 2 – April 13, 2018 – Meeting Minutes

**Roll Call** (Tony C)

Quorum achieved

**Day Two Agenda Review** (Tony C)

***Motion to approve F2F Day Two Agenda***

* Chuck W moves, Tim C. seconds, No objections, abstentions, or comments. Agenda approved

**Post Quantum Cryptography (PQC)** (Andrew B, Judy F)

[LatticeKeyProposal\_13-Apr-2018.pdf](https://www.oasis-open.org/apps/org/workgroup/kmip/document.php?document_id=62867)

Andrew B introduced the topic and the SAFECrypto project.

Tim H stated that the ability to support PQC algorithms in not presently available in OpenSSL

Anthony B asked about the size of lattice keys. Judy/Andrew noted that they are not that much bigger that existing keys, they are just different in form.

Judy walked through the changes required in KMIP to support Lattice Keys

Tim H raised a number of concerns with the proposal. He felt that the concept of a transparent key plus generic didn’t fit with the current KMIP transparent key concept. He also expected a greater list of components. He felt that each of the key components should be tracked separately (rather than genetically) and that standardized method of representing them should be used.

Andrew B noted that there is a lot of variety in the algorithm components and not much generic repetition.

Tim H noted that he has not seen a generic way of expressing the key components.

Chuck stated if we go this way, there is no point if we don't have an effective standard to utilize

Tony C asked -- Do we need a framework/structure for describing the key components? The KMIP TC has elected to simply cater for as many keys/algorithms as possible (not pick just the "winners")

Tim H asked to see some worked examples. We should look at a better level of detail for transparent keys.

Bruce noted that PKCS#11 doesn't have a path for this either. Tim H agreed we should look at it and see how we could do it.

Anthony asked about the NIST timeframe? Which is three years. General discussion about NIST competitions ensued.

***Motion to progress work on Lattice Key representation including worked examples***

* Gerry S moves, Tim C seconds, No objections, abstentions, or comments.

**Break**

**Set Attribute** (Anthony B)

[Set Attribute Proposal - KMIP F2F Day 2](https://www.oasis-open.org/apps/org/workgroup/kmip/document.php?document_id=62872)

**Set Attribute** – If attribute does not have a value it works like an add attribute, if the attributes has a value it works like a modify attribute. This reduces the number of operations to one versus having to a Get Attribute followed by either the Add Attribute or Modify Attribute.

**Increment Attribute** – Lots of folks uses attributes for counting, but current situation is not concurrency safe where you have distributed servers and/or multiple clients. Proposing a ‘Tweak’ attribute instead of modify where you can increment decrement and negate a counting type attribute. TC was fine with idea but didn’t like the name ‘tweak’. Alternative names were discussed with folks agreeing on ‘Adjust’ as the name.

***Motion to include a Set Attribute in KMIP 2.0***

* Chuck W moves, John L seconds, No objections, abstentions, or comments.

***Motion to include an Adjust (Tweak) Attribute in KMIP 2.0***

* Chuck W moves, Tim H seconds, No objections, abstentions, or comments.

**Asynchronous Command Enhancer** (Gerry S)

Problem: Need ability to force an asynchronous command. Right now it is at the discretion of the server to go asynchronous for certain transactions. Within a batch any of the operations could cause an asynchronous transaction which pauses the rest of the operations in the batch.

Solution: Add Full Asynchronous command which allows the client to request that the full request (batch included) is done asynchronously.

John L asked could we just remove the original Asynchronous concept and change the behavior to work this way. No longer a suggestion of the client it would be an honored demand.

Problems

* Servers are not required to implement.
* Changing the current definition could have unintended consequences

But this KMIP 2.0 and we can do a break/fix changes if we want.

Need Usage Guide text to describe this change. Consideration be given to batch order and ID Placeholder and make sure these get covered in Usage Guide. Also include Usage Guide text to cover the migration from existing to 2.0.

Tony C noted that the TC really needs to get out there on education as to what is coming/changing/going away in 2.0 – Webinars, RSA Booth, etc. etc.

***Motion to add a Full Asynchronous capability into KMIP 2.0***

* Tim H moves, Chuck W seconds, No objections, abstentions, or comments.

***Motion to remove the existing Asynchronous capability (Async Indicator Type Boolean Type False) into KMIP 2.0***

* Chuck W moves, John L seconds, Tim H abstains

**AWS Signature** (Anthony B)

[AWS Signature Proposal - KMIP F2F Day 2](https://www.oasis-open.org/apps/org/workgroup/kmip/document.php?document_id=62873)

Problem: Derive AWS Signature for Cloud Services. Three parties involved AWS, person who owns the secret access key, someone who needs access to the services the key gives access. Folks want to delegate access to AWS services without giving access to the secret key.

Add an AWSSignatureVersion4 as a derivation method in KMIP. Also need to make Derivation Data repeatable and allow type to be Text String (to avoid Internationalization issues).

Any concerns with making derivation data repeatable?

Indra asked if there would be text to describe why we added this in Usage Guide?

Tony C suggested this is a good candidate for a profile.

***Motion to add the AWSSignatureVersion4 derivation method to KMIP 2.0 and to create a Profile for this use case.***

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

**Flow Control** (Chuck W)

Need to address Server to Client Operations where the client is not available to receive a command. Client not available to receive a Put or Notify. Client only periodically connects to the server and send me all that you have available for me.

Propose a ChangeFlow that allows the clients to tell the server you want to ‘flip the role’ or communication direction. Put/Notify request into response like the server initiated it. Maintain TLS session but who is the initiator and the receiver. When done the server can switch back control or order.

Bruce asked if both client/server need to track what state they are currently in? Yes

Only good for one connection, independent connections would proceed as normal.

Discussion ensued to get everyone on same page.

There is an impact on Query to make sure that parties support this function before going down path of trying to use it.

Proposal fixes the story on how we make these server to client functions.

Handle as a tag with enumerations – FlowControl

John L noted that guidance to include in the Usage Guide is needed to state that server just gives back control if it has nothing to return. Folks agreed with this behavior but how to achieve this is TBD.

If connection fails – order goes back to normal direction

Bruce thinks a usage limited is need – number of operations to receive -- time limit.

***Motion to add Flow Control concept into KMIP 2.0 Specification including Query impact and associated Usage Guide details as discussed***

* Tim H moves, John L seconds, No objections, abstentions, or comments.

**Lunch**

*Note: Needed to make some adjustments to agenda to accommodate for folks being away at meetings and to allow John L out at 2 PM*

**Destroy Enhancements** (Bruce)

[Destro Revoke/Recover Proposal - KMIP F2F Day 2](https://www.oasis-open.org/apps/org/workgroup/kmip/document.php?document_id=62874)

First Problem: It takes multiple trips to destroy active key when the key is in an active or archived state. It would be nice to fire and forget so client doesn’t have to wait around.

Solution: A new revocation reason ‘Destroy’

Second Problem: Destroy Date cannot be set. This is inconsistent with other dates which can be set by client.

Solution: Allow set attribute on Destroy Date and the server acts on that destruction at the date specified. If date is in the past destroy it now.

Discussion on the proposals commenced with a number of topics covered by no concensus reached.

* Looking at the NIST Key State Model you are forcing through a compromise using revocation reason
* This problem use case originates in making clean-up from Interop test rounds easier.
* We need to protect clients from doing something stupid.
* What about a batch request with all the required operations needed to destroy the key as currently required included. Use Continue on Error to ignore any errors back.
* Do we put this stack sequence into test scripts?
* Destroy Date approach has state transition violation issue

TC recommended that we suspend this discussion and revisit at a future meeting.

**Rekey** (Anthony)

[Rekey Proposal - KMIP F2F Day 2](https://www.oasis-open.org/apps/org/workgroup/kmip/document.php?document_id=62875)

Problem: Initiated by clients not by the server so there is no way for the serer to control the rekey.

Solution: Add new Rotation attributes: Rotate Offset, Rotate Usage Limits and Rotate Protect Stop Date. Server can use these with ReKey/ Rekey Key Pair. Send request with a key id. If this key has been rekeyed then you get the latest key back

This proposal also generated discussion with no concensus reached so the TC recommended that we suspend this discussion and revisit at a future meeting.

**Review Vendor Booth Presentations** (Multiple Presenters)

QLabs – John L

* No comments/concerns from TC on messaging of slide deck

CryptSoft – Greg S

* No comments/concerns from TC on messaging of slide deck

Fornetix – Chuck W

* No comments/concerns from TC on messaging of slide deck

Thales – Alan B

* No comments/concerns from TC on messaging of slide deck

For any company that didn’t have their slides ready they need to be posted then to the reflector for reviewed by the TC. Deadline is Monday morning (April 16, 2018) PDT

Final vendor decks for those reviewed also need to be posted by Monday morning

**Defaults for Mandatory Crypto** (Bruce R)

Problem: Why do clients have to provide things like key length?

Solution: Make Cryptographic Algorithm, Cryptographic Length, and Cryptographic Usage Mask optional and have the server provide these values if they are not specified by the client.

This does require the server to have defaults.

Client should be able to query what the defaults the server has set.

***Motion to accept this proposal (including query changes) for inclusion in KMIP 2.0***

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

**Break**

**Re Encrypt** (Tim)

[ReEncrypt Proposal - KMIP F2F Day 2](https://www.oasis-open.org/apps/org/workgroup/kmip/document.php?document_id=62876)

Problem: Don’t let plaintext data leave the server.

Solution: Need a way for client to ask for a function to be done, acknowledge that function was done but don’t sent the output/results back to me.

Model this after ID Placeholder. Ephemeral suspension of returning results of an operation. Get data from last encryption option.

Will solve re encrypt and potential other concerns. Take decrypt’s output and feed it into encrypt. This allows it to be done on server only via a batch process.

It’s a general solution since it allows other function outputs to flow into the next like encrypt followed by a sign.

Usage Guide content is needed to show how to use these building blocks to implement the re encrypt and the encrypt/sign use case. Another Usage Guide section is needed to describe how you can link batch items together to provide a pattern for solving future use cases.

***Motion to add the capabilities into KMIP 2.0***

* Chuck W moves, Tim C seconds, No objections, abstentions, or comments. proposal approved for inclusion in KMIP 2.0

**KMIP vNext** (Tony C, Judy F)

Discussed the KMIP 2.0 schedule. Normally 4-6 month lag between TC completed and the final OASIS standard.

Target is to have KMIP 2.0 final publication in 2018 so that would require the TC to complete its work in the August/September 2018 timeframe.

Do we need a plug-fest to validate the KMIP 2.0 changes? Don’t think we can organize an interop in that short of timeframe.

Finalize the KMIP 2.0 schedule by the end of May 2018

Need co-editor(s) for Profiles document to assist Tim H (Bob L was Tim H’s co-editor)

Next version (post 2.0) will be referred to as vNext for now. We can decide if 2.1 or 3.0 end of May once we decide what makes the final cut for 2.0.

**Interop 2019** (Tony C)

Should the TC hold an Interop Event at the 2019 US RSA Conference? What type of event (Interop vs Showcase)?

* Interop yes / Showcase no – Cryptsoft, Fornetix, Thales, NetApp, Dell
* IBM think either option is good
* MicroFocus believe TC should hold an event with a preference that it is Interop

***Motion that KMIP TC Request OASIS organize an Interop Demonstration Event at US RSA Conference 2019***

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

***Motion to say the above Interop Demo Event runs under a TC approved process based on the existing approved TC interop process.***

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

***Motion that OASIS TC Interop Demo Event dedicated KMIP is in booth of their own not shared with other OASIS committees***

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

Discussed election of an interop lead. While it was noted that the interop lead should ideally not be a co-chair folks still went ahead and nominated Tony C as interop lead and he graciously accepted the nomination.

Call for other nominations with no additional ones brought forward

***Motion to close nominations for Interop Lead***

* Bruce R moves, Tony C seconds, No objections, abstentions, or comments

***Motion to elect Tony Cox as the Interop Lead***

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

***Motion of the TC to formally thank Tony Cox for his Awesome job in running this year’s interop***

* Gerry S moves, Bruce R seconds, No objections, abstentions, or comments

***Motion that the KMIP TCs co-chairs again make a request to the brief the OASIS Board on Interop Process and Policy***

* Tim H moved, Chuck W seconds, No objections, abstentions, or comments

**AI Review** (Tony C, Judy F, Tim H)

Live editing of old 2.0 Lists on Wiki – Cleaned up table

List of proposals/AI from this F2F – Add links to presentations

Started a vNext List

**Revisit Secretary Nominations (Tony C)**

Still no nominations brought forward

**Next Meeting**

Next meeting of the TC will be held on May 3, 2018

**Next F2F Meeting (Tony C, Judy F)**

Start exploring an East Coast F2F to be held approximately 6 months for now -- no later than October 2018.

Possible venues: NIST/Fornetix/Dell

TC will revisit at end of May

**Pause for a moment of silence in memory of Bob Lockhart**

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

None

**Adjourn**

***Motion to Adjourn***

* Tim H moves, Sue G seconds. No objections, abstentions, or comments. Meeting adjourned

Meeting adjourned at 3:49 PM PDT