Agenda

- Project management (Time and major functionality)
- action items from f2f
- start with where we stand on 1.1 ballots
- discussion about f2f meetings in general
- update on the webinar

Tim moves that we approve agenda as posted, Bob L seconds.
Hearing no objections/abstentions; agenda is approved.

6th of September minutes - any corrections? - none were brought up
Tim moves that we approve minutes as posted, Bob L seconds.
Hearing no obections/abstentions, minutes are approved.

1.1

Both documents have over 75% approval - so most likely they would pass.
Based on new OASIS rules, we need an additional 60 day review. No requests for additional length were brought up.

Project management

More formal project management
Discuss schedules in a more formal way (not sure if gant charts are required)
Track progress on each of the task lists in a more formal way

Scoping for 1.2

- release ship criteria (release does not ship without this functionality)
- take a look at the action items from the f2f and identify most critical items for 1.2
- intersection of time and functionality is how we should manage the 1.2 program

f2f recap

- number of areas where we reached consensus without formal votes

Bob going thro' a list of what he things are consensus:

- recognition that f2f meetings are very important. Next one should be around the time of the RSA conference (Thursday and Friday before the conf)
- speaker phones not just in one place but ones throughout the room give better reception to members that are attending remotely
- consider NetApp facilities for the next f2f even though it is a little further away from the city
- Tim: two and a half days is better
- weekly meetings is the consensus
- current time seems to be working out better for everyone
- 1.2 - major functionality that needs to fully specced out by end of Q2. Four weeks from the end of the f2f is when the scoping should be done
- interop importance - don't move ahead unless we have reasonable declarative commitment that at least three member organizations should step forward and commit to doing interop
- use cases: 3 fairly large chunks that should be deferred out of 1.2;
--- end-user/administrative use cases
--- cloud (key migration from one CSP to another; new class of s2s)
--- policy propagation between providers (can be handled via attribute setting and sync by the client)
--- Mike: Should we leave them in the use cases document?
--- Bob L: re-order by priority; OR move unimplemented into an appendix?
--- Bob L: Mark them as implemented/not implemented; seems like the consensus
--- need another rev of the use cases doc; Mike, Denis and Bob L to work on an updated version
--- need to include remote attestation
- recharter discussion: best to defer initiating until we are close to completion on 1.1 vote
-- first step is to craft a new charter
-- need to look @ do we leave all the excluded items
-- are there any implications to important revision items? If members are aware; please notify right away.
-- start working with your legal
-- s2s relationships; cloud and alternative representations are clearly areas that cannot be finalized until re-charter is done

AI

Action Items from KMIP face-to-face

- Denis/John: create proposal for **<edit from Bruce: key>** value as optional and new "not here" attribute [3 weeks] (HSM and stream use cases)

- Tim/John/BobG: create proposal for Get Random operation based on Crypto Profile; also write use case write-up [date tbd} (Storage/HSM use cases)

- Kelley/BobG: write new Usage Guide section on how to do attestation for Get, using Register and Get Random [date **two weeks**]

- Denis/BobG: write new Usage Guide section on how to do Metadata-only object [date tbd] (HSM use cases); **Denis - first cut**

- Tim/Denis/**Another volunteer from Thales**: complete proposal for encrypt etc, based on existing proposal; also write use cases [date tbd] (Storage/HSM/Cloud use cases). **Might be a 1.2 release driver** (Tim - we might be able to demonstrate it by RSA 2013 interop) Bob L: Profiles to support JCE, PKCS.

- Bob/Gordon: write new profiles and/or Usage Guide sections for 3 registration models [4 weeks] (Storage/cloud/HSM use cases)

From here on, potentially nice to have for 1.2

- Bob/Gordon: investigate and return to committee on proving key-based erasure (date tbd) (storage, cloud) Might be a 1.2 or even a 1.3 item

- BobG/Subhash/BobL: create draft proposal/example of Profile doc and library revision, based on f2f discussion (date tbd)

- Judy/Indra/BobG: review Usage Guide to determine whether to

remove information, create new organization (assumptions / guidance on functionality / how to implementation attestation, etc) (date tbd)

- Tim/BobG: present updated proposals on alternative protocol representations (date tbd)

- Mike/BobG/Judy: present proposal for mapping PGP requirements into existing/new capabilities + Usage Guide section, including pgpuserid, ADK, object signature [date tbd] (PGP use cases)

- Mike/Tim: present proposal for new forward/back and parent/child link types [1 week] (PGP use cases)

  Mike/Tim: investigate and possibly present proposal to remove requirement for unique name (date tbd) (PGP use cases)

- Bruce/Tim: investigate and return to committee with information to resolve decision on mutability of values, either as general issue or as template-specific [information in 2 weeks from today]

- Gordon/BobG: determine whether to document the key escrow use case (date tbd) (storage)

- Denis/BobL): write proposal for crypto-domain parameters in key block [date tbd] (HSM use cases)

- Gordon/Bob/Kiran/**Saikat**: write proposal for attribute-based grouping mechanism for tenant support [2 weeks] (cloud)

- BobL): write proposal on supporting encrypt/decrypt in usage limits [2 weeks] [HSM]

- BobL/BobG/**Kiran**]: write proposal for client-specific usage limits and reporting back on what clients have used [date tbd]

- Tim/BobG: investigate and report back to TC on whether any other query enhancements are needed[date tbd]

- JohnL: investigate and report back to TC on whether enhancements to notify/put are needed (date tbd) (stream)

- Gordon): investigate and report back to TC on whether "protected data" attribute is needed (date tbd) (storage)

- Gordon/Bob): investigate and report back to TC on whether we should support a mechanism for identifying the master when copying keys [date tbd] (S2S, storage)

- John: investigate and report back to TC on group managed object in order to enable clients to identify other clients. (date tbd) (Stream)

- Denis: define additional list of ECC algorithms and other enumerations (including RNGs) (date tbd)

- Tim/BobG: identify possible things we should deprecate in V1.2 (date tbd)

- Gordon/Bob/Bruce/Judy: specify flow and test cases for asymmetric key wrapping of symmetric keys [date tbd)

- BobL?: investigate and report back to TC on alternatives to tlS communication for V1.2 (date tbd)

- BobG/Subhash: look into how to drive more parallel activity in V1.2 (date tbd) 2-3 issues and resolutions in our meetings

- Saikat/Denis: investigate and report back to TC on key versioning options (date tbd)

Tim moves that we adjourn, Mike A seconds.
Hearing no objections/abstentions, we are adjourned.