Decisions from KMIP face-to-face

* Resolution to accept SoUs and start Special Majority vote on submitting V1.1 spec and profiles as Candidate Standards
* Plan face-to-face meetings on 6-month basis, with next f2F immediately preceding RSA Conference US 2013
* Weekly meetings going forward (except for selected dates such as US Thanksgiving holiday etc)
* Target 4 weeks to have high-level scoping for V1.2
* In determining what functionality to include in V1.2, at least 3 member organizations should commit in principle to implement/interop that functionality
* Defer end-user and admin/admin use cases
* Defer cloud key policy use cases
* Defer cloud and server-to-server key migration use cases
* Defer re-charter until v1.1 oasis vote is complete

Action Items from KMIP face-to-face

* Denis/John: create proposal for 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 tbd]
* Denis/BobG: write new Usage Guide section on how to do Metadata-only object [date tbd] (HSM use cases)
* Tim/Denis: complete proposal for encrypt etc, based on existing proposal; also write use cases [date tbd] (Storage/HSM/Cloud use cases)
* Bob/Gordon]: write new profiles and/or Usage Guide sections for 3 registration models [4 weeks] (Storage/cloud/HSM use cases)
* Bob/Gordon: investigate and return to committee on proving key-based erasure (date tbd) (storage, cloud)
* 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]
* 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: 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]: 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)
* Saikat/Denis: investigate and report back to TC on key versioning options (date tbd)