December 12, 2013 Meeting Minutes

Start 21:00UTC

Role Call

Taken by Subhash Sankuratripati (Subhash) Quorum Achieved

Proposed Agenda

1. Approve Previous Minutes
2. Saikat Saha (Saikat) review rechartered List of companies Recontribition Letter status
3. Tony Cox (Tony C.) review of interop meeting
4. RNG Proposals from Tim Hudson (Tim H.)
5. Chuck White (Chuck W.) and Joeseph Brandt (Joe B.) Presentation on NIST lifecycle
6. Tim H. review Cryptographic Streaming proposal
7. John Leiseboer (John L.) review Streaming Object proposal
8. Scheduling Next Meeting

Motion to accept agenda

- Tim H. Moves to accept agenda - approved
- Joe B. seconds the motion
- No objections - No Discussion
- Motion Passes

1. Approve Previous Meeting Minutes

November 14, 2013 Minutes

- Tim H. Moves to approve minutes from November 14, 2013 meeting
- Chuck W. Seconds the motion
- No objections - No Discussion
- Motion Passes

December 05, 2013 Minutes

- Tim Moves to approve minutes from December 5, 2013 meeting
- Chuck White Seconds the motion
- No objections - No Discussion
- Motion Passes
2. Review of Recontribition letters

- Status review by Saikat
- Judith Furlong (Judy) EMC letter in process
- Michael Jenkins (Mike J.) will review Kelley's contributions for NSA for letter
- Additional action pending outcome of email with OASIS administration on requirements or suggestions

3. Review of Interop Sub-Committee meeting

- Agreed process for interop
- Full exchange of credentials has not occurred yet
- Credentials should be out this week based on commitments

4. Tim H. walkthrough of RNG proposal comments

- Link RNG Base Proposal
- Link RNG Query Proposal
- Link RNG Attribute Proposal
- Link RNG Specify Proposal
- Comments received from John L. and Peter Robinson
- Bob Lockhart (Bob L.) needs to review after return from time away
- Proposals to be kept separate for easier discussion and implementation

5. KMIP and SP800-130 Meta-Data security requirements

- Presented by Chuck W. & Joseph B. covered
- Link KMIP and SP800-130 Requirements
- Using KMIP to provide a method for protecting attributes appropriately including access control on the server side
- Subhash looking for interop across servers using a common wrapping key?
  - Chuck W. Yes
  - Subhash - Can you provide a proposal that meets the requirements? Wrapping proposal being done by Tim H. and may be reusable.
- Bob L. Attributes each with their own attributes such that you end up with every attribute as a structure?
- Hal L. Attributes each can have their own metadata
- Tim H. Wrap all attributes to start, then all for individually wrapped attributes
- John L. End users could work within exiting KMIP specification by encrypting metadata and storing it as Secret Data or an Opaque Object with the UUID of protected metadata stored as attribute of a key (just one example).

6. Update on Cryptographic operations streaming proposal
Presented by Tim H.

- Link: Cryptographic Streaming Proposal

### 7. Update on Cryptographic operations streaming proposal

Presented by John L.

- Link: Cryptographic Operations Streaming Presentation

- Need to skinny down proposals for Random to one of three options
- Subhash would a straw poll be appropriate?
- John L. could we split out Random?
- Tim H. We have done this before and then the vote was to not separate it out

**Motion to create a straw poll**

- John L. moves to create a straw poll on streaming proposals
- Peter R. Seconds the motion
- No objections or discussion
- Motion Passes

**Straw Poll Subhash will create**

- Tim H. to bring forward a proposal based on presentation
- John L. to bring forward a proposal based on presentation
- Both to bring forward a proposal
- Neither to bring forward a proposal

### 8. Scheduling Next Meeting

- Tim H. moves to have next TC meeting on January 9, 2014 and cancel December 19th, 26th and January 2nd meetings.
- Kiran T. Seconds the motion
- No objections - No Discussion
- Motion Passes

**Motion to Adjourn**

- Tim H. moves to Close Meeting
- Chuck W. seconds the motion
- No objections - No Discussion
- Motion Passes
- Meeting adjourned 22:01UTC