

## P1619.3 Minutes 2007-11-05

Contributed by Fabio Maino  
Tuesday, 06 November 2007  
Last Updated Tuesday, 06 November 2007

The regular IEEE P1619.3 Task Group meeting was held on Nov 5th 2007 in Las Vegas, NV. Matt Ball was in the chair, Fabio scribing.

Introductions Matt thanks T10 and Hitachi GST for hosting the meeting, and Hitachi Data Systems for Webex conference service and SUN microsystem for phone.

### Attendees:

Fabio Maino Cisco  
Ravi Kavuri Decru/NetApp  
Subhash Sankuratripati Decru/NetApp  
Robert Sussland Decru/NetApp  
Kevin Marks Dell  
Larry Hofer Emulex  
Bob Nixon Emulex  
Eric Hibbard HDS  
Doug Whiting Hifn  
Mark Schiller HP  
Chris Williams HP  
Glen Jaquette IBM  
John Geldman Lexar Media  
Walt Hubis LSI Logic  
Matt Ball M V Ball Tech  
Bob Lockhart NeoScale  
Landon Noll NeoScale  
Hannes Tschofenig Nokia Siemens Networks  
Joe Lepine PMC Sierra  
Craig Carlson QLogic  
Andrea Doherty RSA Security/EMC  
Jack Harwood RSA Security/EMC  
Jim Randall RSA Security/EMC  
Jim Coomes Seagate  
Marty Czekalski Seagate  
Jon Holdman Sun Microsystems  
Luther Martin Voltage Security  
Michael Marcil Vormetric  
Garry McCracken WinMagic

### Agenda:

1. Introductions, roll call
2. Thank you to our sponsors:
  1. Hitachi GST : Conference Room and Phone Line
  2. Hitachi Data Systems : Web hosting and teleconference
  3. Sun Microsystems : Conference phone
  4. LSI Logic : Projector
3. Approval of the agenda
4. IEEE patent slideset
5. Approval of previous minutes
6. Review of past action items
7. Liaison Reports
  1. IETF KEYPROV - Andrea Doherty
  2. OASIS EKMI - Matt Ball on behalf of Arshad Noor
8. Subgroup discussions and status
  1. Project Management (PM): Matt Ball
  2. Architecture (ARCH): Mike Witkowski
  3. Name Space (NS): Bob Lockhart

4. Operations and Objects (OO): Landon Noll
5. Messaging (MSG): Ravi/Subhash (Note: Transport to merge under MSG)
6. Use Cases (USE): Call for new facilitator
7. Should SISWG buy Webex Services
9. Review of new action items
10. Schedule next meeting
  1. Next T10: Jan 14, 2008 in Santa Ana, CA
  2. T11: Feb 4-8, 2008 in Austin, TX (or Dec 3-7 in Lake Mary, FL)
  3. Conference call in between?

Eric moves, and Fabio Seconds, approval of Agenda. No objections.

Matt shows IEEE slide sets.

Landon mentions that Neoscale has filed a disclosure letter that is now on the 1619 website. Approval of previous minutes

Minutes were posted. No changes/objection. Minutes are approved.      Review of previous Action Items

AI 1 &ndash; [Curt Kolovson] Mark Schiller will check on public availability of the API for library to KMA communications [Carryover]

AI 3 - Bob Griffin to provide a draft mapping of PKCS#11 on D1 draft by next meeting to illustrate how it could be used in this context. (carry-over)

AI 5, Fabio &ndash; Flesh-out what of the Threshold Secret Sharing proposal goes on section 5 and what on 6. Elaborate a couple of use cases that helps understand where/how this is going to be used. Also show the math behind it. (carry-over).

AI 8 - Fabio, check with IEEE where are we with the mailing list splitting task (Done)

AI 9 - Matt Ball, Investigation on IEEE acquiring an high level URI for use of KEY ID/Namespace as specified in KEYPROV (carryover, Email sent to the Liason, but not heard back)

AI 10, editor: remove 4.4.2 and send to the API group (carryover)

AI 11, editor: incorporate comments from this meeting (such as separate informative from normative, address terminology and glossary), send to reflector to collect further comments and prepare for incorporation. (carryover, This was related to the namespace proposal)

AI 12, Bob Griffin: sends a few proposals on how to 'promote/market' the work of the group through whitepapers and the like (carryover, Matt should check with Jim Hughes that has now a role in SNIA that might be useful for this)

AI 13, Bob Lochart: send a blank template of the namespace docs to be used as template for the other documents. Insert a 'this is not a draft standard' warning somewhere in the doc (Done)

#### Status Report

IETF KEYPROV - Andrea Doherty (Presentation posted to the reflector)

Active work is on DSKPP, and Key container specification. New internet draft submitted by hallm baker (algorithm-identifiers), comments are welcome.

Dskpp is at its 2nd draft, and it was a complete restructuring of the original doc. Incorporates feedback form IETF 69 and it's getting close to last cal. Possibly last call after Vancouver meeting

PSKC is at its 2nd draft since WG adoption.

OASIS EKMI - Matt Ball on behalf of Arshad Noor

EKMI is being actively marketed right now, and will likely be voted on in the 11/14 meeting. There's an open source implementation called StrongKey.org (Java).

Technical DiscussionProject Management (PM): Matt Ball

No meeting yet, probably one coming in January. \Architecture (ARCH): Mike Witkowski

A proposed Key Management Model has been drafted. Two options for the Control plane on the table (one with SW Library, the other with a monolithic KM Client). Hanse raises the question of what the KM API would really be. Group answer is that the K SW Lib will be a smaller piece of SW with a set of basic/simpler functionalities provided. The API might not be part of the std, but the KM SW Lib could be provided as a reference implementation (it might be similar to the functions provided by PKCS #11). The real focus of the std is the KM Msg and Transport Protocol.

Larry talks the group through the Key Lifecycle Model that is a superset of the ISO/NIST model.

John Holdman shows the slides that describes the NIST 1857 model for Key Lifecycle. The subgroup needs to work more details out, and come to the group with a proposal. Matt: we need to define where the std will stop in term of specifying Key lifecycle. At least we need to define how many states are needed to figure out the metadata that shall be associated with a key. John, Larry, and Bob will come back with a proposal.

Next Call Thu Nov. 15th. Operations and Objects (OO): Ravi Kavuri

Combined preso by Neoscale and NetApp. A number of objects have been described in term of metadata, states, and operations: key, client, Symlink, Policy are a few examples. The issue of "dormant client" was raised during this preso. Some of the clients may not have the capability to retain time across reboots, and the standard should consider if the API should support a way to provide a secure timestamp to a client.

The group discussed also the concept that if a client doesn't understand a piece of a policy, it shall not use that policy.

The issue was raised that with the many subgroups it's getting harder to keep track of what is going on unless one follows all the subgroups (that are kept at a very tight schedule).

Ravi proposes to move the subcommittee to once a month, and this would give a little more time to digest proposals. Eric suggests that we use the .3 meeting as a way to validate that the direction taken by each subgroup is the right one, and send them back to produce more elaborate text that will go into the draft.

Matt then asks if the slideset presented is a reasonable set of objects. Michael Marcel suggests that there is need for an end-point access control policy object.

Key manager object is another one that would need to be added.

Matt asks that group produces a table that shows all objects and compares them.

Is there a need for users and roles that administers the key manager. Also the question is raised why the KM user has been removed from the model? It might be out of the scope of the std, but should certainly part of the conceptual model.

A proxy object might also be needed (like tape to library proxy). The draft should state that the stupid disk/tape that does encryption only is a CU and is as such part of the current model. Name Space (NS): Bob Lockhart

Bob goes through the changes made to NS the draft. This document seems to get closer to a state that would allow incorporation.

Name Space group will schedule another meeting in two weeks. Mail will be sent out to entire .3 group.

Messaging (MSG): Ravi/Subhash (Note: Transport to merge under MSG) Use Cases (USE): Call for new facilitator

Matt will be the acting facilitator, but call is kept open and volunteers are welcome. Should SISWG buy Webex Services?

SO far Hitachi and LSI have provided webex, but it would be nice if we have a handful of companies that can cover. Netapp, Cisco, Vortec can possibly join, and will confirm at next meeting.

The issue seems to be more to have one of the members available to host the call rather than the cost of the webex service for a given company.

Eric points out that it's hard to predict how long the activities of the group will go on for, and we might expose ourself to the liability of having the service running for longer then the life of the group. Action Items

AI 1 &ndash; [Curt Kolovson] Mark Schiller will check on public availability of the API for library to KMA communications

AI 3 - Bob Griffin to provide a draft mapping of PKCS#11 on D1 draft by next meeting to illustrate how it could be used in this context.

AI 5, Fabio &dash; Flesh-out what of the Threshold Secret Sharing proposal goes on section 5 and what on 6. Elaborate a couple of use cases that helps understand where/how this is going to be used. Also show the math behind it.

AI 9 - Matt Ball, Investigation on IEEE acquiring an high level URI for use of KEY ID/Namespace as specified in KEYPROV (Email sent to the Liason, but not heard back)

AI 10, editor: remove 4.4.2 and send to the API group

AI 11, editor: incorporate comments from this meeting (such as separate informative from normative, address terminology and glossary), send to reflector to collect further comments and prepare for incorporation. (This was related to the namespace proposal)

AI 12, Bob Griffin: sends a few proposals on how to 'promote/market' the work of the group through whitepapers and the like (Matt should check with Jim Hughes that has now a role in SNIA that might be useful for this)

AI 14, Matt: Consolidate use cases in a single doc. AI 15, Fabio, Ravi, Mike W.: check with their own companies availability of Webex

#### Next Meeting

At next T10: Jan 14, 2008 in Santa Ana, CA from 12 to 5 PM

Meeting is adjourned at 5.25 PM.