

P1619.3 OO Minutes 2007-11-14

Contributed by Matt Ball
Wednesday, 14 November 2007
Last Updated Wednesday, 14 November 2007

The regular meeting of the P1619.3 OO subject met on Wednesday, Nov 11, 2007, at 12:30 Pacific Time. Ravi and Landon were facilitators, and Matt Ball took minutes.

Attendees:

Mike Witkowski, CipherMax

Chris Williams, HP

Walt Hubis, LSI Logic

Landon Noll, NeoScale

Luther Martin, Voltage Security

Matt Ball, MV Ball Tech

Jon Holdman, Sun Microsystems

Ravi Kavuri, NetApp

Michael Marcil, Vormetric

Glen Jaquette, IBM

David Sheehy, PMC Sierra

We discussed the document [OO] NeoScale_NetApp_Update_v2 2007-11-05, given to the P1619.3 face-to-face meeting

Key management servers must support the following objects:

- Keys
- Clients
- Symlink
- Retention Policy
- Cryptographic policy? TBD (needs clarification)

- Group
- KMS object
- (Others not discussed -- please make suggestions)

Clients must support these objects:

- Keys
- Retention Policy -OR- ability to periodically check server whether key is valid
- Any others?

Optional objects:

- Policy - Conformance to a particular standard (e.g., FIPS 140-{2,3}, Common Criteria, hardware security)
- others?

Landon - A server must enforce a policy marked as mandatory (to be P1619.3 compliant).

Open questions:

Do we make 'Cryptographic Policy' mandatory? (From discussion, we decided to split this up so that the lists are separate from the algorithms -- this item needs clarification)

What do we do in the case of 'referrals'? That is, when the client presents a symlink to the key manager for a key that the key manager doesn't have, and doesn't have access to. In this case, the key manager could 'resolve' the symlink for the client and give the client the option to get the key itself.

How does a client enroll? What information does the client give to the server?

Do we need to have a 'notify time'? This allows the key manager to set the disable and expiration time after the client requests a key beyond the notify time.

Jon: Key states group talking about having two periods: encryption period and crypto period. The encryption period is the time that encryption is allowed. The crypto period is the time decryption is allowed. The encryption period must be contained within the crypto period.

Jon, Larry, and Bob L are working on a proposal for key states and will have a proposal out soon.

Landon and Ravi will start to put the OO proposal into a template for the standard.

What questions do we need to answer to put this into a template?

- We need to state whether support of certain objects and operations is mandatory or optional for the server and client. (possibly display this as a table with links to sections that provide definition)
- Who defines client credentials? ARCH will define the model -- OO will define the details.
- Other questions listed above

Action Item: Landon and Ravi to produce list of questions for next meeting that need clarification for the proposal

Action Item: Landon and Ravi to Propose first cut of proposal in 4 weeks.

If anyone can help, please contact Landon and Ravi.

The meeting was adjourned at 2:30 Pacific Time.