

P1619.3 ARCH Minutes 2007-11-15

Contributed by Matt Ball
Thursday, 15 November 2007
Last Updated Thursday, 15 November 2007

The Regular meeting of the P1619.3 Architecture subcommittee (ARCH) was held on Nov 11, 2007 at noon Pacific Time. Mike Witkowski was in the chair and Matt Ball took minutes.

CipherMax sponsored the WebEx meeting sharing for this meeting.

Attendance:

Mike Witkowski, CipherMax

Jon Holdman, Sun Microsystems

Matt Ball, MV Ball Tech

Luther Martin, Voltage Security

Jim Randall, RSA Security

Glen Jaquette, IBM

Bob Lockhart, NeoScale

David Sheehy, PMC Sierra

Walt Hubis, LSI Logic

Agenda:

- Review Previous Actions
- “Draft” KM Conceptual Models
- “Draft” Key Lifecycle Models
- Items in Progress
- Next Steps

We discussed the slide show here: [P1619 ARCH Meeting 2007-11-15\(2\)](#)
Previous Action Items

- Mike W. to refine KM conceptual models; integrate into Model Proposal with definitions
- In progress, models “complete”;, working definitions

- Bob L., Jon H., and Larry H. to collaborate on single key lifecycle model
- Common model agreed to in concept. Still working some of the finer points. We will discuss a little bit today.

DiscussionWalt: Why do we have the KM API? Bob: This will help with implementations, but is not necessary for compliance

Slide 5:

- Changed 'KM Message & Transport Protocol' to 'KM Ops' (for brevity and to match slide 6)

Slide 6 (Conceptual Key Management Model):

- Add a 'in scope' box with the legend
- Move the KM User box to the middle and draw dotted lines to adjacent boxes
- Matt: Do we need slide 5 given that we have slide 6? Answer: Yes, but Bob will draw a version (see action items)

Slide 8 ("Draft" Key Lifecycle Models):

- Jon: Go with the right-side and change 'Deactivated' to 'Deactivated/Expired'
- What standards should we align with? These were proposed. We should create a diagram that maps our key states into these standards (in an informative annex):

- NIST SP 800-57A

- ISO 11770

- ANS X9.24

- Proposed to use the right-sided diagram, remove transitions 2,3, move transition 6 to go to 'disabled compromised'
- We decided to make all states mandatory and change the 'purged' state to a terminal node
- The client only understands two states: "write/read" and "read-only". Create a diagram to map the server's 9 or states into the clients two state.

Action Items:

- Bob Lockhart: Modify the slide 5 to show the data plane going from right-to-left and the control plane going up-and-down (due sometime next week)

- Luther Martin: Map the proposed states into ANS X9.24 (Due by next meeting in 2 weeks)
- Mike Witkowski, Landon Noll or Bob Lockhart, Ravi, Matt - Create document outline proposal.
- Mike, Landon, Ravi - Create Policy model/figure (to replace P1619.3/D1 Figure 1). Needs clarification from the OO group. 2 weeks
- Jon Holdman to finish Key Lifecycle model

The meeting was adjourned at 1:58 pm Pacific Time