SCSI Stream Commands - 3: Working Group Minutes – Draft (T10/07-006r0)
Date: December 11, 2006
Time: 10:00-12:00 pm MST
Location: Phone Conference

Attendance

```
SSC-3 Working Group Attendance Report - December 11, 2006
Name                                            Organization
 ------------------------------------------------------------------
Mr. Curtis Ballard                              Hewlett Packard Co.
Mr. Michael Banther                             Hewlett Packard Co.
Mr. Christopher Williams                        Hewlett Packard Co.
Mr. Kevin Butt                                  IBM Corp.
Mr. David Peterson                              McDATA
Mr. Paul Entzel                                 Quantum Corp.
Mr. Roger Cummings                              Symantec
Mr. Ralph Weber                                 ENDL
Mr. Paul Suhler                                 Quantum Corp.
Mr. Matt Ball                                   Quantum Corp.
Mr. Anderus Liveruv                             Tandberg
Mr. Gideon Avida                                Decru
Mr. David Black                                 EMC
Mr. Larry Hofer                                 McData
```

Results of Meeting

1. Opening remarks and introductions [Peterson]

2. Approval of agenda [Peterson]

3. Approval of meeting minutes [Peterson]

4. Old business
4.1 SSC-3 Using Public-Key Cryptography for Key Wrapping (06-389r3) [Gideon Avida]

David Black reviewed the major sticking points between him and Gideon:

1. Applications do not have access to SCSI Name Identifiers because they are related to the port. The initiator side of the SA in 06-449. Gideon has done 80% of the work. Ralph pointed out that we are trying to reach farther into the application client than we have ever done before so we need to tread carefully.

2. There may be some IP issues related to Eliptic Curve. both agree that there are differences of interpretation.
    From the introduction to ISO/IEC 18033-2:2006(E)

    Note forwarded by Gideon:

The ISO and IEC take no position concerning the evidence, validity and scope of this patent right.

The holder of this patent right has assured the ISO and IEC that he is willing to negotiate licences under reasonable and non-discriminatory terms and conditions with applicants throughout the world.

In this respect, the statement of the holder of this patent right is registered with the ISO and IEC.

Information may be obtained from:

ISO/IEC JTC 1/SC 27 Standing Document 8 (SD8) "Patent Information"

Standing Document 8 (SD8) is publicly available at:

http://www.ni.din.de/sc27

Attention is drawn to the possibility that some of the elements of this International Standard may be the subject of patent rights other than those identified above. ISO and IEC shall not be held responsible for identifying any or all such patent rights.

SD8 can be find in the document section here:

http://www.ni.din.de/sixcms/media.php/1377/SC27N4348_SD8_Patent_Informat

ion_Feb2005.pdf?backend_call=true

As David said on the call: talk to your attorneys...

Gideon reviewed the changes in his proposal.

Ralph and Michael discussed areas in the proposal that appeared to be needed in a model clause, but as the proposal is currently written this information and requirements will disappear. The group reviewed items that needed to be put into SSC-3. Paul Entzel asked what the new model clause title should be so we can know what should and should not be included.

There was some discussion about how Public Key - Private Key wrapping that may or may not have authentication and that authentication will not be all the way to the key manager.

Paul Entzel asked about the last two sentences of 4.1.2. Kevin Butt asked if Authentication wouldn't be covered by 06-449 and 06-369. The last two sentences are discussing how to install the device servers public key (i.e. the signing key). Gideon will attempt to clarify and provide a standard method of doing this. Gideon will attempt to rewrite these into a model clause.

Discussion about clause 4.3 states that there needs to be some controlled and protected from modification. The discussion seemed to be that the key modifications should be limited to specific entities. Roger Cummings wanted to see how to support this across a distributed application. The issue currently is about sender authentication. We either need to fully specify it or remove it.

There was a discussion about if it should include which threats this method will protect against. Ralph agreed that something like the table in 4.4.2 would be worth while.

There was concern in 5.2.2 about placing requirements on out of band items. Ralph, why do we have to have anything that states how this is used? Gideon deleted the note.

Matt Ball asked gideon to add additional "Parameter Set" values to Table W. Gideon stated that he prefered to not add anything else but let Matt do so in a different proposal.

Kevin had a question about 8.5.4.7 and 8.5.4.8 and what "arbitrary identification data" is intended to be. This led to a discussion that resulted in suggestion to use the Logical Unit Name (see SAM-4) for the device server in 8.5.4.7 and to append "that uniquely identifies the wrapping entity" in 8.5.4.8. Time ran out before we could discuss much on 8.5.4.8.

5. New Business

6. Next Meeting Requirements.

7. Review of new action items

7.1 [Gideon Avida] Rewrite clause 4 items into a model clause.

8. Adjournment