

SSC-3 Working Group Agenda ()

Date: April 10, 2007

Time: 8:00 am-10:00 am

Location: Phone conference

Agenda

1. Opening remarks and introductions

2. Approval of agenda

3. Approval of meeting minutes

4. Review of old action items [Butt]

5. Old business

5.1 General items

5.1.1 Vendor Feedback (05-351r1) [Group]

5.1.2 Configurable EW (05-423r3) [Butt]

5.1.3 TapeAlert Delineation (06-138r3) [Butt]

5.2 Security-related items

5.2.1 Using NIST AES Key-Wrap for Key Establishment (06-225r5) [Ball]

5.2.2 Keyless Copy of Encrypted Data (06-462r4) [Butt]

5.2.3 Encryption Error Behavior when unsupported medium is loaded (07-005r1) [Butt]

5.2.4 Additional controls for keyless copy (07-016r1) [Entzel]

6. New Business

6.1 General items

6.1.1 Cleaning Model (05-285r0) [Butt]

6.1.2 Requested Recovery log page (07-046r1) [Banther]

6.2 Security-related items

7. Liaison reports

7.1 P1619 Status Report [Ball]

8. Project status**8.1 Next meeting requirements (Seattle, WA)****8.2 Target date for letter ballot - Nov 2007****9. Review of new action items****10. Adjournment****Attendance**

SSC-3 Working Group Attendance Report - April 2007

Name	S	Organization
Mr. David Peterson	P	Brocade
Mr. Gideon Avida	P	Decru
Mr. Curtis Ballard	V	Hewlett Packard Co.
Mr. Michael Banther	A	Hewlett Packard Co.
Mr. Christopher Williams	V	Hewlett Packard Co.
Mr. Kevin Butt	A	IBM Corp.
Mr. Paul Entzel	P	Quantum Corp.
Dr. Paul Suhler	A	Quantum Corp.

8 People Present

Status Key: P - Principal
 A,A# - Alternate
 AV - Advisory Member
 E - Emeritus
 L - Liaison
 V - Visitor

Results of Meeting

1. Opening remarks and introductions [Peterson]

2. Approval of agenda (07-040r0) [Peterson]

Dave Petereson asked if anybody had anything to cover. Paul Entzel had revised his proposal. Nobody else had anything that was ready to discuss.

3. Approval of meeting minutes [Peterson]

Not covered

4. Review of old action items [Butt]

Not covered

5. Old business

5.1 General items

5.1.1 Vendor Feedback (05-351r1) [Group]

5.1.2 Configurable EW (05-423r3) [Butt]

5.1.3 TapeAlert Delineation (06-138r3) [Butt]

5.2 Security-related items

5.2.1 Using NIST AES Key-Wrap for Key Establishment (06-225r5) [Ball]

5.2.2 Keyless Copy of Encrypted Data (06-462r4) [Butt]

5.2.3 Additional controls for keyless copy (07-016r2) [Entzel]

Paul covered the modifications.

Gideon asked for an additional note that states “Warning to the user that even the layman will understand that even if he sets the no copy bit the media is not bullet-proof.”

Discussion surrounded the fact that nobody knows how to do this without saying you cannot trust that any encrypted media has not been copied by raw copy methods.

[Paul Entzel] The point was brought up that if we state this is not cryptographically secure then we must do the same for all areas in the standard where things are not cryptographically secure.

The point was also brought up that a user will need to reference P1619.1 also to ensure that a tape drive is secure - assuming the tape drive claims compliance to P1619.1.

One of the changes to acronyms was missed in this revision and Paul stated he would change it.

Gideon wants to qualify statements about disabling reads by adding “in device servers compliant with this standard”. Discussion was that everything we state implies “in device servers compliant with this standard”.

Paul Entzel moved that Additional controls for keyless copy (07-016r2) be included in SSC-3. Chris Williams seconded. The motion passed on a 4:0:1 vote.

5.2.4 IKEv2 for CAP (06-449r2) [Black]

6. New Business

6.1 General items

6.1.1 Cleaning Model (05-285r0) [Butt]

6.1.2 Requested Recovery log page (07-046r1) [Banther]

6.2 Security-related items

7. Liason reports

7.1 P1619.1 Status report [Ball]

8. Project Status

8.1 Next Meeting Requirements (Memphis, TN)

8.2 Target date for letter ballot.

9. Review of new action items

9.1 Dave Peterson to add Additional controls for keyless copy (07-016r2) into SSC-3

10. Adjournment

Dave Peterson made a motion for adjournment at 8:53 am PDT. Seconded by Chris Williams.