Draft Minutes
IEEE P1619.3 task group meeting
5 May 2008 - 1 PM to 6 PM EDT
Santa Clara CA

The IEEE P1619.3 task group held a meeting at Santa Clara CA on 5 May 2008. Total attendance was 25 people from 22 organizations and is tabulated at the end of this document. 21 of these organizations are members of IEEE P1619.3.

Minutes were taken by Bob Nixon (bob.nixon@emulex.com). Please report any corrections by email to P1619-3@LISTSERV.IEEE.ORG.

1 Opening remarks

1.1 Introductions

Matt Ball opened the meeting Monday, 5 May 2008 at 1:05 PM EDT. He thanked our host organization, NVidia, and Hitachi Data Systems for the teleconference facilities, HItachi GST for the projector, and Sun for the conference telephone. He led a round of introductions.

2 Meeting Policy

2.1 Patents

Matt Ball reviewed the IEEE guidelines for use of proprietary information in standards.

No new patent issues were raised in response to the review.

2.2 Attendance and Membership

The meeting quorum is 14 member organizations and individuals. More than 14 member organizations answered the quorum check, either in person or on the teleconference service.

2.3 Approval of Agenda

The agenda for this meeting had been posted to the membership and the SISWG web site via email (Ball to P1619.3 reflector, 2 May 2008, “Draft agenda and details for this Monday's Face-to-face meeting”):

1:00 Introductions
1:15 Liaison Reports
  KEYPROV
  EKMI
1:45 Objects and Operations Proposal (Subhash Sankuratripati)
2:45 WS-Management (Jon Hass)
3:30 OASIS XACML (Michael Marcil)
4:30 Key Management Summit 2008 (Matt Ball)
5:00 Review of latest draft P1619.3 (Bob Lockhart)

6:00 Adjournment

Eric Hibbard (HDS) moved and Landon Noll (Cisco) seconded to approve the agenda as posted. The motion was approved unanimously.

2.4 Review of Minutes

At the meeting 10 March 2008, a quorum was not present so the minutes of the meeting held 14 January 2008 could not be approved. This meeting therefore reviewed the meeting minutes for both 14 January 2008 and 10 March 2008.

No corrections were offered for the meeting minutes of either 14 January 2008 or 10 March 2008. They are therefore approved as written.

2.5 Review of Action Items

The open action items for this meeting had been posted to the membership and the SISWG web site via email (Ball to P1619.3 reflector, 3 May 2008, “Updated Action Item list”).

The chair presented the status of open action items in accord with his records. He requested the membership to review it for further corrections and updates.

ACTION All members to review the published action list and report corrections to the chair. Due date for this action is 12 May 2008.

2.6 Liaison Reports

2.6.1 EKMI/OASIS **Arshad Noor**

OASIS is currently in active writing. A 1.00 draft was intended by beginning of May, but the editor found it was harder than expected to prepare formal text. Revised goal is a public review mid-June and forward to OASIS in September.

2.6.2 IETF KeyProv **Mingliang Pei**

Ming introduced the goals and current work of the IETF KeyProv group, which is closely relevant to the work of this group. The goals revolve around means to distribute symmetric shared key authentication tokens.

Three specifications are in preparation: DSKPP (Distributed Symmetric Key Provider Protocol), PSCK (Portable Symmetric Key Container format - XML declarations), SKPC (Symmetric Key Package Content Type - ASN.1 declarations).

Ming then gave short overviews of each.

The discussion of DSKPP noted a possible vulnerability to downgrade attack.

The discussion of SKPC identified that P1619.3 may have interest in adopting one or more of CMS, SKPC, and PSKC. CMS is currently well-established, while SKPC and PSKC are both in development.

ACTION Matt Ball to post the IETF/KeyProv presentation to the SISWG web site.

3 Scheduled Business

3.1 Objects and Operations Status — Subhash Sankuratripati

The proposal had been posted to the membership and the SISWG web site via email (Sankuratripati to P1619.3 reflector, 4 May 2008, “Objects and Operands Proposal”).

Subhash presented in detail the proposed text for the Objects and Operations clause.

It was suggested that the data in a Key Blob attribute should be represented in Base64_encode (with a length) for all key types. If it is perceived that the application community for certain key types finds a different encoding more convenient, conversion between the convenient endoding and Base64_encode may be provided at the API. Not all members supported this suggestion.

There was not unanimous consent to the need for a key-wrapping signature.

It was understood that the set of *required* key-wrapping algorithms is as small as meets the need and probably will remain at its current size, but the list of *recommended* algorithms should be expected to expand to reflect future technologies.

It was recommended to require SHA-512 as the hash algorithm for the key-wrapping signature.

Much of the review was deferred for lack of time.

3.2 WS-Management — Jon Hass

The presentation had been posted to the membership and the SISWG web site by email (Hass to SISWG, 2 May 2008, “WS-Management Transport Proposal for 1619.3 “).

The presentation described the WS-Management (Web Services Management) work done by DMTF, and suggested how it might be used in the context of the P1619.3 architectural model.

Its values to P1619.3 were described as leveraging an appropriate protocol and object modeling methodology (i.e., CIM) for which specifications, implementations, development tools, and test tools are widely available.

The main negative was described as a perception of it being a heavy infrastructure. Its weight may be offset by its rich feature set and its existing wide availability in platforms targetted for P1619.3.

Its advantages versus some of the other protocols that are in consideration (e.g., SOAP) were described as including WS-Management’s reduced operation set, efficiently matching the needs of P1619.3.

It was noted that SNIA, through the SMI-S 1.4 work-in-progress, still enthusiastically classifies anything based on WS-Management as Experimental.

Some concern was expressed that the operation set of WS_Management is too sparse for the operations presumed (or known to be) necessary for P1619.3.

ACTION Jon Hass to provide detailed examples for mapping P1619.3 onto WS-Management. Due 21 May 2008.

3.3 OASIS XACML — Michael Marcil

The proposal had been posted to the membership and the SISWG web site via email (Ball to P1619.3 reflector, 3 May 2008, “Preliminary presentation for Vormetric's presentation on OASIS XACML for policies and access control“).

Michael introduced Extended Access Control Markup Language (XACML), which is “an Oasis standard to express enterprise security policies with a common XML based policy language.”

The presenter posed XACML as a means of distributing acess control policy including key usage policy, not necessarily the only means, and not for the underlying key distribution function. Richly functional applications may already be using XACML for security policy statements, and it would be advantageous for them to use XACML for key managment policy as well. This suggests that a KM Server should (shall?) be able to manage policy objects expressed in XACML, not that the KM Server needs to understand and operate in compliance with a XACML policy.

3.4 Key Management Summit

This agenda item was not considered due to lack of time.

4 Review of P1619.3/D3 Bob Lockhart

The proposal had been posted to the membership and the SISWG web site via email (Lockhart to P1619.3 reflector, 4 May 2008, “Comments for Draft 2 & Draft 3“).

This agenda item was not considered due to lack of time.

5 Meeting Schedule

The group considered monthly meetings to be useful at this time. This allows wider consideration of the output of the subgroups, which have already been meeting as often as weekly.

Meeting at a hotel is not essential, company facilities are seen as acceptable.

As an intermediate effort, a whole-group teleconference could be held in months alternating with the bimonthly meetings.

ACTION Chair to schedule a full group teleconference on 21 May 2008 to determine procedure for expediting technical closure.

6 Review of New Action Items

ACTION All members to review the published action list and report corrections to the chair. Due date for this action is 14 May 2008.

ACTION Matt Ball to post the IETF/KeyProv presentation to the SISWG web site.

ACTION Jon Hass to provide detailed examples for mapping P1619.3 onto WS-Management. Due 21 May 2008.

ACTION Chair to schedule a full group teleconference on 21 May 2008 to determine procedure for expediting technical closure.

7 Adjournment

It was moved by Landon Noll and seconded by Bob Nixon to adjourn. The motion was approved unanimously.

The meeting was adjourned at 6:22 PM EDT on 5 May 2008.

8 Attendance

Organization	Representative
Scott Kipp	Brocade
Landon Noll	Cisco
Subhash Sankuratripati	Decru/NetApp
Jon Hass	Dell
Kevin Marks	Dell
Larry Hofer	Emulex
Bob Nixon	Emulex
Eric Hibbard	HDS
Glen Jaquette	IBM
John Geldman	Lexar Media
Walt Hubis	LSI Logic
Mark Benedikt	Microsoft
Matt Ball	MV Ball Tech
Bob Lockhart	nCipher
Bill Colvin	Optica
James Fitzgerald	SafeNet
Eric Hopkins	Seagate
Arshad Noor	StrongAuth
Jon Holdman	Sun Microsystems
Mingliang Pei	Verisign
Luther Martin	Voltage Security
Manish Ahluwalia	Vormetric
Michael Marcil	Vormetric
Thomas Hardjono	Wave Systems
Garry McCracken	WinMagic