Draft Minutes
IEEE P1619.3 task group meeting
10 March 2008 - 1 PM to 6 PM EDT
Durham NC

The IEEE P1619.3 task group held a meeting at Durham NC on 10 March 2008. Attendance was 14 people from 13 companies and is tabulated at the end of this document. Not all organizations present were current members.

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

1 Opening remarks

1.1 Introductions

Matt Ball opened the meeting Monday, 10 March 2008 at 1:15 PM EDT. He thanked Network Applications for the meeting faciilities, Hitachi Data Systems for the teleconference facilities, Cisco Systems for the projector, and Sun for the conference telephone. He led a round of introductions.

2 Meeting Policy

2.1 Attendance and Membership

The meeting quorum is 14 member organizations and individuals. Only 10 were present either in the room or on the teleconference facility. The meeting will continue without making motions unless a quorum is later acheived.

2.2 Patents

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

There was discussion of the possibility of a company acquiring intellectual property (e.g., through a corporate acquisition) on which a prior RAND license had been granted, and then attempting to revoke the RAND license. Member legal staff is reviewing this question.

3 Approval of Agenda

The chair presented the following agenda.

1:00 - 1:30 Front Matter
- Introductions
- Thank Sponsors:
- IEEE patent slide set
- Approval of Agenda
- Approval of Previous Minutes

1:30 - 2:00 Liaison reports (KEYPROV, EKMI)
2:00 - 3:00 Tim Bray presents using XML in protocols, as given to IETF

3:00 - 4:00 Architecture Proposal/Vote to include into standard – Matt Ball for Walt Hubis
4:00 - 5:00 Objects and Operations Status - Landon Noll/Subhash
5:00 - 6:00 Review of P1619.3/D2 - Bob Lockhart

Those present agreed to conduct the meeting in accord with this agenda, modified that no actions would be taken that require a vote.

4 Review of Minutes

Prior minutes were not reviewed because there was no quorum for approval.

5 Scheduled Business

5.1 Practical guidelines for choosing XML — Tim Bray (Sun)

Tim identified considerations leading to productive answers to three main questions on the topic:

a) Should one use XML?
b) If using XML, should one invent a new XML language?
c) If inventing a new language, what considerations lead to a successful invention?

Some summary observations on choosing XML (or an alternative):

a) Use binary only if you are
    a) operating at a very low protocol level; and
    b) can tolerate the need for environment-specific implementations.
b) Don't use ASN.1 unless implementing something that needs to be compatible with one of the very few existing ASN.1 application (e.g., SNMP).
c) Don't dismiss a plain text solution until you are sure it is not adequate (e.g., if internationalization or extensibility are high-priority).
d) There is a Java-related language called JSON. It has a number of strong points, and a couple of relevant issues. Many of us were unfamiliar with it, so:
    a) Google Maps uses it.
    b) It parses quickly.
    c) It is optimized for simple data structures rather than documents.
    d) It browses easily.
    e) It evades certain security behaviors offered by XML.
    f) It is considered best used with ephemeral data, not persistent.
e) XML is very good at
    a) tools;
    b) extensibility;
    c) internationalization; and
    d) document representation.
f) Bad sides of XML
    a) ugly;
    b) verbose;
    c) does not map well to data structures; and
    d) programmer-hostile API.
g) Use XML if your application places a lot of priority on
    a) documents;
    b) internationalization;

c) extensibility; and/or
d) data re-usability.

Discussion of the choice of encodings raised the following points

a) Extensibility and data re-usability should be important goasl for the P1619.3 design, since it is entirely unclear all the places where 1619.3 data may get used.
b) Lack of a compact parser may or may not be an issue depending on where the parsing needs to be done. The requirement that keys shall not be distributed as clear text may automatically obviate this issue, since the minimal relevant environment is already is capable enough to do decryption.
c) Parsing speed of XML is not seen as an issue in practice unless some add-on features are exercised.

But XML does not define protocols, it defines languages. You need an XML language. Do you invent one specific to your application?

a) Invented XML languages have a low average success rate.
b) Invented XML languages need invented debuggers.
c) There are a few existing languages that have satisfied several disparate applications.
d) Grownups should discourage people from inventing new XML languages.

Discussion questions:

a) What would be the best existing languages for a request/response protocol? Atom and XMPP.
b) How does SOAP fit in? It is frowned on, mostly because of things it is used with, not inherent weaknesses. But it is not extensible.

If you are intent on inventing an XML language, read RFC 3470 first. If you are still intent...

a) It is important to PRECISELY define the semantics of every data tag...
b) but don't ignore that the eventual goal is getting the right bits on the wire.
c) Need to agree to design to the minimal requirements first.
d) Specification priorities should be:
    1) Human readability of the specification
    2) Examples and a validator
    3) Schema
e) Are there tools that generate validators from schemas? Yes, sort of, but they don't capture all the good things that a validator should check.
f) There are tools for generating XML language specifications. RelaxNG is a good one.
g) Consider how extensions are to be treated. Three approaches were described:
    a) prohibit them.
    b) must-understand any extensions encountered.
    c) must-ignore extensions that are not understood. This is the most flexible. RFC 4287 (ATOM) is an example.
h) There may be several byte representations of exactly the same XML syntax, and their signatures won't match. So far there is no really good resolution to this issue.

Language goals recommended by one member:

1) Extensibilty...
2) including extension to incorporate legacy implementations
3) embedding into cryptographic unit hardware is not a likely implementation;

The chair will invite Tim to the kickoff meeting of the Messaging and Transport Adhoc Group. Tim offered to participate/advise if his schedule permitted.

5.2 Architecture Proposal/Vote to include into standard — Walt Hubis

In the absense of Walt Hubis, Matt Ball presented.

Discussion was based on a marked up version of the ARCH document provided by Walt Hubis via email (Hubis to P1619.3, 7 March 2008).

The goal of the review today is to resolve any issues that those present feel should be resolved before inclusion in the draft standard.

It was questioned whether a glossary definition of a “Cryptographic Unit Identifier” is needed. It was agreed to defer this issue until the OO proposal.

It was agreed to use the definition of “Policy” from the OO proposal

It was agreed to use the definition of “Encryption Key” (or “Cryptographic Key“) from 1619.1.

It was agreed that for the purposes of this proposal, KMSS operations are presumed to be the same as KMCS. We may find the need for differences later. The goal is to make KMSS a minimal superset of KMCS.

It was agreed to move the Namespace subclause of the ARCH proposal to become clause 5 of the draft standard.

It was agreed to add short introductory paragraphs for the Key Management Object Model and Key Management Operations Model. These will be linked to more detailed subclauses provided by the OO subgroup.

It was understood disaster recovery actions may recover a key from the purged state. The state diagram only shows/will show only the “automatic” transitions.

It was agreed that a formal vote is not necessary to include generally agreeable content into the draft.

ACTION Matt Ball to provide the editor with a markup of ARCH to show the changes agreed at the P1619.3 meeting 10 March 2008.

ACTION Editor to publish a revision of the P1619.3 draft including the ARCH document with changes agreed at the P1619.3 meeting 10 March 2008.

6 Objects and Operations Status — Landon Noll/Subhash Sankuratripati

The current content and intended path toward completion were reviewed for the Objects and Operations proposal.

It was recommended to add a field to indicate the type of key wrapping. It is intended to include both standard-specified and vendor-specific wrapping types.

It was recommended to include values of the Key_encoding field to indicate both standard-specified and vendor-specific encodings.

It was recommended to consider specifying data types by URIs with certain reserved prefixes, rather than a list of reserved data type names. Reserved prefixes should include some reserved for standard use, some for vendor-specific use, and some for special purposes such as “not a name”.

7 Review of P1619.3/D2 — Bob Lockhart

Bob will email his list of issues and possible resolutions to the reflector, and expect any feedback by the same channel.

8 Meeting Schedule

Meeting facilities and time as for this meeting will be requested during the T10 plenary week hosted by NVidia in Santa Clara CA, 5-9 May 2008.

Intention to meet during the T10 plenary week hosted by Emulex in Anchorage AK, 14-18 July 2008 will be determined at the May meeting.

Meeting facilities and time as for this meeting will be requested during the T10 plenary week hosted by LSI in Colorado Springs CO, 8-12 September 2008.

9 Review of New Action Items

080310-1 Matt Ball to provide the editor with a markup of ARCH to show the changes agreed at the P1619.3 meeting 10 March 2008.

080310-2 Editor to publish a revision of the P1619.3 draft including the ARCH document with changes agreed at the P1619.3 meeting 10 March 2008.

10 Adjournment

The meeting was adjourned at 5:20 PM EDT on 10 March 2008.

11 Attendance

Representative	Organization
Landon Noll	Cisco
Subhash Sankuratripati	Decru/NetApp
Kevin Marks	Dell
Larry Hofer	Emulex
Bob Nixon	Emulex
Eric Hibbard	HDS
Chris Williams	HP
Glen Jaquette	IBM
Matt Ball	MV Ball Tech
Bob Lockhart	nCipher
Bill Colvin	Optica
James Fitzgerald	SafeNet
Tim Bray	Sun
Luther Martin	Voltage Security