# IEEE 1619 Security in Storage Working Group (SISWG)

Plenary Meeting Notes

April 15, 2009

# Agenda

1. Introductions and thank sponsors: LSI Logic
2. IEEE Patent Slide Set and Call for Patents
3. Approval of the agenda
4. Approval of previous minutes
5. Review of Previous Action Items
6. Liaison Reports:
    1. OASIS KMIP
    2. OASIS EKMI
    3. IETF KEYPROV
7. General Announcements and Status
    1. P1619.2 status (Ball/Hughes)
    2. P1619.3 status (Hubis)
    3. New Operating Procedures Template
    4. Key Management Summit 2010 in Reno, NV
    5. XTS Rationale to NIST
    6. IASC Officer Elections: Chair, Vice-chair, Secretary, and Treasurer
    7. Copyright release letter
8. New Business
    1. Motion to approve Walt Hubis as OASIS KMIP liaison to SISWG (Ball).
    2. "Move that P1619.3 include a subset of the KMIP binary encoding as a part of the binary protocol" (Updated March 18) (Hubis)
    3. Thales Object and Policy additions, changes and deletion proposal (Motion only -- full presentation at previous P1619.3 task group meeting) (Lockhart)
    4. Sun Overview of P1619.3 Proposals (Ball)
9. Late Agenda items (addressed as time permitted):
    1. Move that the SISWG maintain an OID (Object Identifier) registry from the OID arc 1.3.111.2.1619, starting with the text from the attached document entitled SISWG_OID_registry.txt ? (Ball)
    2. Move that the P1619.3 task group re-evaluate all P1619.3 subcommittees (Ball)
10. Next Meeting / Adjourn

# Instructions for the WG Chair

**The IEEE-SA strongly recommends that at each WG meeting the chair or a designee:**

- **Show slides #1 through #4 of this presentation**
- **Advise the WG attendees that:**
  - The IEEE's patent policy is consistent with the ANSI patent policy and is described in Clause 6 of the *IEEE-SA Standards Board Bylaws*;
  - Early identification of patent claims which may be essential for the use of standards under development is strongly encouraged;
  - There may be Essential Patent Claims of which the IEEE is not aware. Additionally, neither the IEEE, the WG, nor the WG chair can ensure the accuracy or completeness of any assurance or whether any such assurance is, in fact, of a Patent Claim that is essential for the use of the standard under development.
- **Instruct the WG Secretary to record in the minutes of the relevant WG meeting:**
  - That the foregoing information was provided and that slides 1 through 4 (and this slide 0, if applicable) were shown;
  - That the chair or designee provided an opportunity for participants to identify patent claim(s)/patent application claim(s) and/or the holder of patent claim(s)/patent application claim(s) of which the participant is personally aware and that may be essential for the use of that standard
  - Any responses that were given, specifically the patent claim(s)/patent application claim(s) and/or the holder of the patent claim(s)/patent application claim(s) that were identified (if any) and by whom.
- The WG Chair shall ensure that a request is made to any identified holders of potential essential patent claim(s) to complete and submit a Letter of Assurance.
- It is recommended that the WG chair review the guidance in *IEEE-SA Standards Board Operations Manual* 6.3.5 and in FAQs 12 and 12a on inclusion of potential Essential Patent Claims by incorporation or by reference.

Note: **WG** includes Working Groups, Task Groups, and other standards-developing committees with a PAR approved by the IEEE-SA Standards Board.



**(Optional to be shown)**

# Participants, Patents, and Duty to Inform

**All participants in this meeting have certain obligations under the IEEE-SA Patent Policy. Participants:**

- **"Shall inform the IEEE (or cause the IEEE to be informed)" of the identity of each "holder of any potential Essential Patent Claims of which they are personally aware" if the claims are owned or controlled by the participant or the entity the participant is from, employed by, or otherwise represents**
  - **"Personal awareness" means that the participant "is personally aware that the holder may have a potential Essential Patent Claim," even if the participant is not personally aware of the specific patents or patent claims**
- **"Should inform the IEEE (or cause the IEEE to be informed)" of the identity of "any other holders of such potential Essential Patent Claims" (that is, third parties that are not affiliated with the participant, with the participant's employer, or with anyone else that the participant is from or otherwise represents)**
- **The above does not apply if the patent claim is already the subject of an Accepted Letter of Assurance that applies to the proposed standard(s) under consideration by this group**

  Quoted text excerpted from IEEE-SA Standards Board Bylaws subclause 6.2

- **Early identification of holders of potential Essential Patent Claims is strongly encouraged**
- **No duty to perform a patent search**

# Patent Related Links

All participants should be familiar with their obligations under the IEEE-SA Policies & Procedures for standards development.

Patent Policy is stated in these sources:

IEEE-SA Standards Boards Bylaws

*http://standards.ieee.org/guides/bylaws/sect6-7.html#6*

IEEE-SA Standards Board Operations Manual

*http://standards.ieee.org/guides/opman/sect6.html#6.3*

Material about the patent policy is available at

*http://standards.ieee.org/board/pat/pat-material.html*

**If you have questions, contact the IEEE-SA Standards Board Patent Committee Administrator at patcom@ieee.org or visit http://standards.ieee.org/board/pat/index.html**

**This slide set is available at http://standards.ieee.org/board/pat/pat-slideset.ppt**

# Call for Potentially Essential Patents

- If anyone in this meeting is personally aware of the holder of any patent claims that are potentially essential to implementation of the proposed standard(s) under consideration by this group and that are not already the subject of an Accepted Letter of Assurance:
  - Either speak up now or
  - Provide the chair of this group with the identity of the holder(s) of any and all such claims as soon as possible or
  - Cause an LOA to be submitted

# Other Guidelines for IEEE WG Meetings

- **All IEEE-SA standards meetings shall be conducted in compliance with all applicable laws, including antitrust and competition laws.**
  - **Don't discuss the interpretation, validity, or essentiality of patents/patent claims.**
  - **Don't discuss specific license rates, terms, or conditions.**
    - Relative costs, including licensing costs of essential patent claims, of different technical approaches may be discussed in standards development meetings.
      - Technical considerations remain primary focus
  - **Don't discuss or engage in the fixing of product prices, allocation of customers, or division of sales markets.**
  - **Don't discuss the status or substance of ongoing or threatened litigation.**
  - **Don't be silent if inappropriate topics are discussed … do formally object.**

---

**See *IEEE-SA Standards Board Operations Manual*, clause 5.3.10 and "Promoting Competition and Innovation: What You Need to Know about the IEEE Standards Association's Antitrust and Competition Policy" for more details.**

# 1619.2 Status Report

***April 15th, 2009***

Fabio Maino
<fmaino@cisco.com>

# 1619.2 Status Report

- Latest draft published: D9
  - D10 not published yet, but Matt took a good pass to many of the open comments
  - D9 passed letter ballot on Jan. 09, but there are a few comments that needs to be addressed
- Comments Resolution:
  - 50 Editorial comments:
    - Some editing work required, but is clear how to proceed
  - 17 Technical comments:
    - 2 are critical: “Test Vectors” and “IBM-1”
- Target Sponsor ballot start by June 2009

# XCB Test Vectors (McGrew/Finney)

- 8 cases generated
  - Key sizes 16/32 bytes, PT 16/20/24/32/48/512/520 bytes, ADT 16 bytes
  - 5 verified successfully
  - 3 didn't pass independent verification
- A few more cases needed:
  - zero ADT
  - 2064 PT
  - Odd sizes PT: 17, 2065 bytes

# EME-2 Test Vectors (Finney/Gladman)

- There is a set of test vectors generated by Hal Finney and independently verified by Brian Gladman
  - Key sizes 64/48 bytes, PT 16/17/20/32/512/520/2064/2065 bytes, ADT 0/16 bytes
- Test vectors have not been published yet
  - Brian volunteered to check draft text when included
- Hal suggested to change K_ECB to K_WHITE in the draft
  - Shai agreed (AI to editor)

# Comment “IBM-1”

- “The XCB specification includes an impossible mix of bit-wise and byte-wise language…”
- Matt took a first stab at this comment (not sure it’s completed)
  - David Needs to verify outcome

# Liaison Reports

- OASIS KMIP (key management interoperability protocol)
  - First meeting is on April 24th in San Fran.
  - KMIP plans to vote on a liaison on April 24th
- OASIS EKMI
  - Arshad Noor has resigned as chair, and has been replaced by Anil Saldhana and Tim Bruce
- IETF KEYPROV
  - Steady progress on keyprov drafts

# IEEE SISWG P1619.3 Sub-Committee Status Summary

Walt Hubis

4/15/2009

# KMIP

- Should P1619.3 include the mandatory KMIP binary encoding in its entirety for our binary protocol?
- Plenary Item
- Proposal Needed (Hubis).

# KMIP – Future Direction

- Create an XML WSDL that is a mechanical translation of a subset of the KMIP binary protocol.
  - A Method to do mechanical translations.
- Add on P1619.3-specific extensions.

# KMIP/P1619.3 Mapping

- Mapping effort to identify features in P1619.3 that are not in KMIP are in process. (Waiting for first KMIP meeting). KMIP needs to first meet and approve the consortium's work
- Identify P1619.3-specific extensions that were left out of KMIP.
- Architecture Review (In Process)
- Formal Liaison (In Process)

# KMIP

- Add P1619.3 Namespace
  - KMIP does not define any namespaces.
  - The only requirement is that they are unique in the local server context
- Convergence is not an issue.

# KMIP

- Define concrete default port bindings for P1619.3/KMIP services
- Register ports with IANA
  - Required for Interoperability
- P1619.3 Requirements
  - Need to avoid conflicts

# KMIP

- Define an optional enrollment protocol.
  - Simplifies client management.
  - Need a proposal (TBD)
- Define a optional discovery protocol
  - Simplify management.
  - A proposal is needed (TBD)

# KMIP

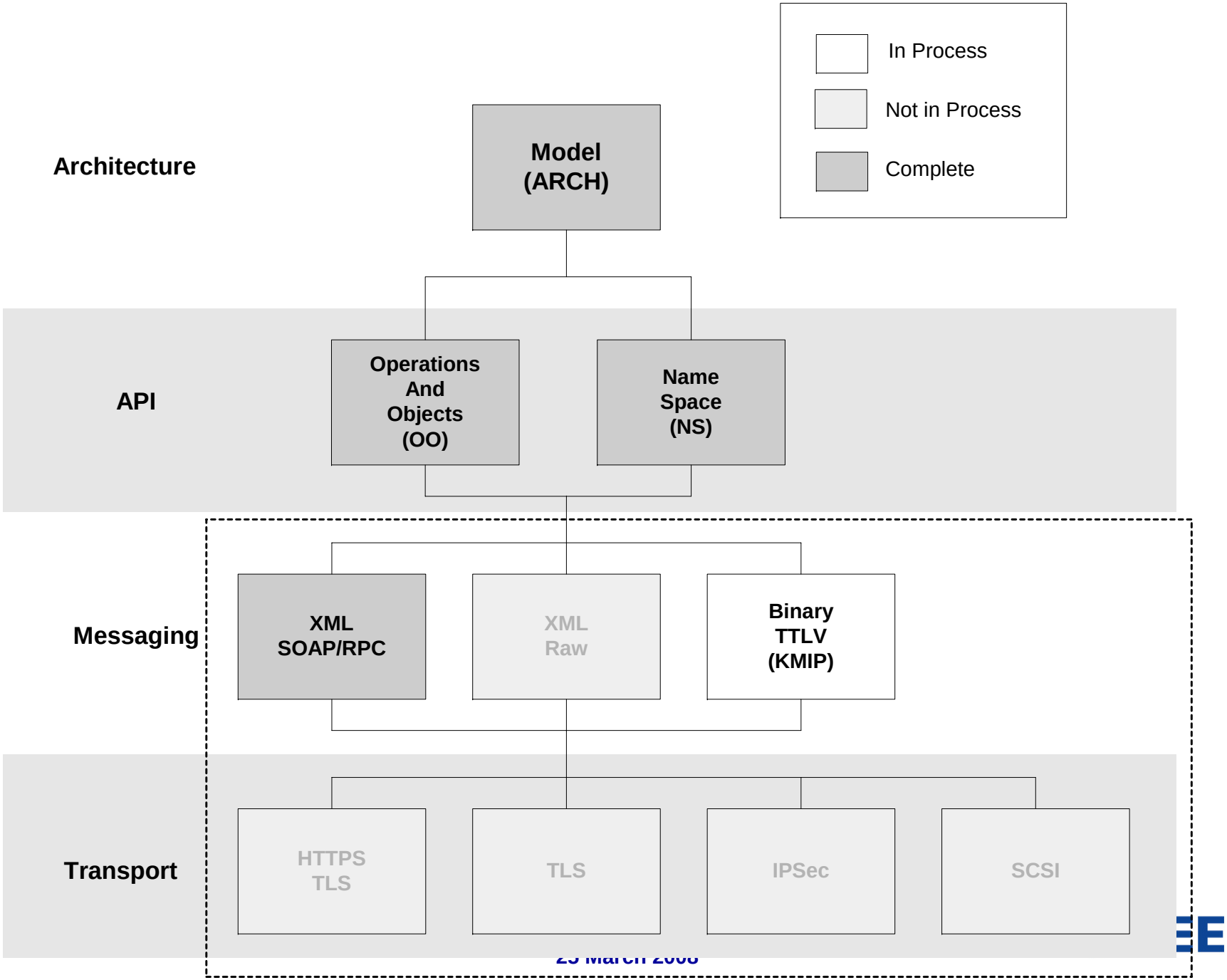
- Define Server-to-Server communication.
  - Deferred until a later version of the protocol.

# P1619.3 Overview

- Draft 6 now in Comment Review
  - Comment Deadline: End of April 2009
- In Process
  - Messaging
    - Binary: KMIP Evaluation
    - XML: KMIP Comparison

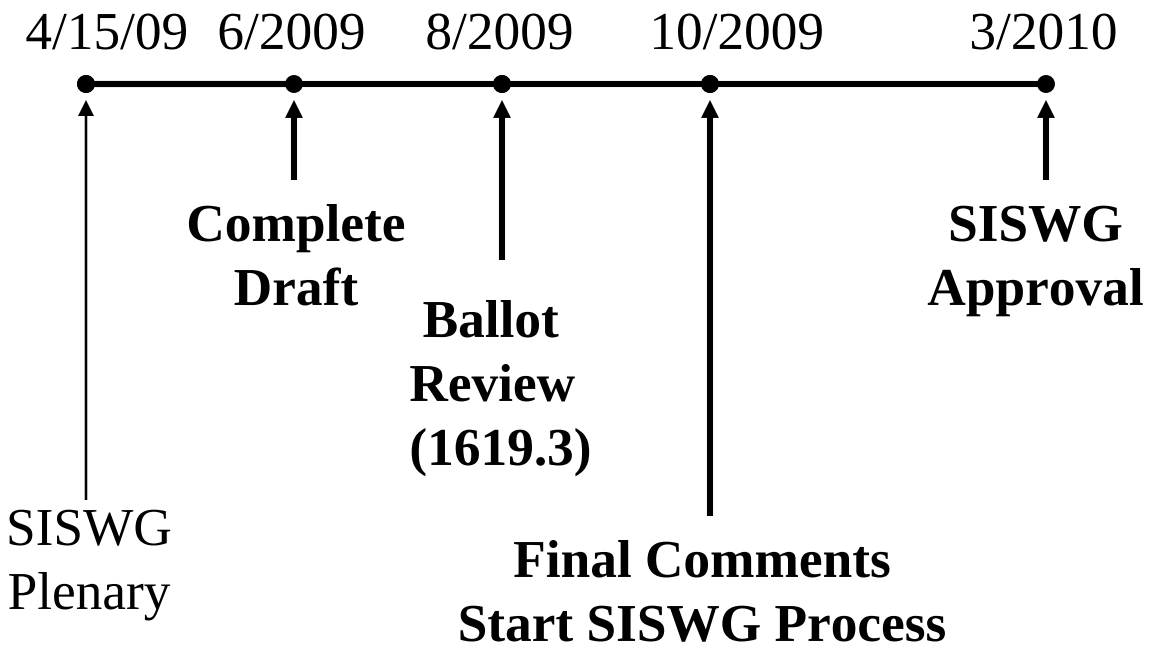
# Important Dates

- End of April, 2009
  - Deadline for Draft 6 Comments
- April 15, 2009
  - SISWG Plenary
    - Conference Call
  - Proposals Needed by March 16, 2009


In Process
Not in Process
Complete
Architecture
Model
(ARCH)
API
Operations
And
Objects
(OO)
Name
Space
(NS)
Messaging
XML
SOAP/RPC
XML
Raw
Binary
TTLV
(KMIP)
Transport
HTTPS
TLS
TLS
IPSec
SCSI

| Committee | Start Date | Current | Comments |
|---|---|---|---|
| ARCH | 10/2007 | Complete 3/2008 | |
| NS | 6/2007 | Complete 1/2008 | |
| OO | 9/2007 | Complete 11/2008 | |
| MSG (SOAP-XML) | 9/2007 | Complete 1/14/2009 | |
| MSG (Binary) | 9/2007 | TBD | Proposal to use KMIP |

# Timeline


4/15/09
6/2009
8/2009
10/2009
3/2010
Complete Draft
Ballot Review (1619.3)
SISWG Approval
SISWG Plenary
Final Comments Start SISWG Process

# IEEE P1619 Security in Storage WG (SISWG) Operating Procedures

## 15 April 2009

Eric Hibbard, CISSP, CISA

Vice Chair, IEEE SISWG

# What's Going On…

- IEEE-SA Baseline Operating Procedures for IEEE Standards Working Groups constitute the fundamental requirements for proper standards practice in the IEEE.
- IEEE Audit Committee (AudCom) is asking that working groups upgrade their operating procedures to comply with the newly published Baseline Operating Procedures.
- These baseline P&Ps become effective on 31 March 2009.
- AudCom will begin random audit of WG P&Ps in June of 2010, so we need to publish new conforming Operating Procedures before June 2010.

# Where Are The Issues?

- There are several clauses that must be added to the SISWG P&P; several of these just drop in.
- The SISWG is currently identified as an “individual method” WG, but our P&P look more like entity-based; if we want to remain “individual” based we need to:
  - Purge almost all of the language regarding entities; we need to track affiliations, but that is it
  - Align all membership at the individual level. This means that voting and attendance are completely associated with individuals. There are no restrictions on the number of voting members affiliated with a particular organization
- Switching to an entity-based method could result in annual membership fees for the represented entities

# Where Are The Issues?

- The concept of subgroups are introduced, but:
  - The default clause indicates the members of the subgroup are all appointed; only working group members appointed to the subgroup shall vote on questions within such subgroups.
  - Any resolution of a subgroup shall be subject to confirmation by the working group.
  - There is very little additional guidance associated with how subgroups are organized, how they conduct work, etc.

# IEEE Key Management Summit 2010

- (Information still preliminary)
- Next IEEE Key Management Summit is tentatively scheduled for April 13-14, 2010 in Lake Tahoe, NV
- Co-located with IEEE MSST again
- Looking for Session Chairs
- Need to avoid overlap with SNW

# XTS Rationale to NIST

- NIST has requested additional comments on XTS proposal
- Received comments from Seagate
- Latest Draft 3 published April 14th
- See https://siswg.net/index.php?option=com_docman&task=doc_download&gid=169&Itemid=41

# IASC Officer Elections

(From Jack Cole): An election will be held for IASC to select a new chair and potentially other officers. Nominations will be accepted throughout this month (April 2009). I am not a candidate, although I will still have a role in IASC, and I am able to act as nomination officer. Please send nominations and questions to me. Candidates must be members of the IEEE (any grade) and Standards Association (IEEE SA) members. Self-nominations are welcomed, and nominations of others must be followed by acceptance by the nominee. Nominations for chair, vice-chair, secretary, and treasurer are sought. If only a chair is nominated and elected, that chair may temporarily appoint the other officers until further nominations and another election can be held.

# Copyright Release Letter

- Matt Ball is working on creating a template letter for copyright releases, based on the template from the IEEE 2009 Style guide.

# New Business

1. Motion to approve Walt Hubis as OASIS KMIP liaison to SISWG (Ball) – Deferred until after first OASIS KMIP meeting.
2. "Move that P1619.3 include a subset of the KMIP binary encoding as a part of the binary protocol" (Updated March 18) (Hubis) – (Larry: What subset?) – Deferred until after complete P1619.3/KMIP evaluation
3. Bob Lockhart will send out a link to the recorded KMIP presentation.
4. Thales Object and Policy additions, changes and deletion proposal (Motion only -- full presentation at previous P1619.3 task group meeting) (Lockhart) – Deferred until next plenary

# Sun Proposals to P1619.3

- These proposals are based on the open source Sun Agent Toolkit
- Proposals based on Sun's agent toolkit:
  - An enrollment proposal, updated for P1619.3
  - A CA and Certificate service, updated for P1619.3
  - A Discovery proposal,
  - An XML key-backup format
- Each proposal will have a WSDL, in Document/Literal style for standards compliance (WS-I)
- See http://opensolaris.org/os/project/kmsagenttoolkit/

# Late Agenda Items

- Cyril moves that the SISWG maintain an OID (Object Identifier) registry from the OID arc 1.3.111.2.1619, starting with the text from the attached document entitled SISWG_OID_registry.txt. Matt seconds (Ball). Motion passes by acclimation.
- Walt moves that the P1619.3 task group dissolve all P1619.3 subcommittees. Matt Ball seconds. Motion passes by acclimations
- Landon Noll moves to create a subgroup to propose a PAR for an amendment to P1619. Matt Ball seconds the motion. Motion passes by acclimation. Please send Landon your intent to participate in this subgroup to draft PAR language for the next plenary.
  - Hal mentions that we'll need to review Phil Rogaway's proof on security of one-key.

# Next Meeting

- First Wednesday of each month via teleconference?  May 6th doesn't work because it's during T10 week
- May 13th is next plenary.  10:00am PDT