

SISWG Working Group Meeting Minutes 2011-06-01

Contributed by Walt Hubis
Tuesday, 05 July 2011
Last Updated Tuesday, 05 July 2011

1. IEEE Patent Slide Set and Call for Patents
2. A quorum was achieved.
3. Approval of the agenda
 - 3.1.1. Call for editor for "P1619.0a"
 - 3.1.2. Security implications of one-key XTS for an informative annex to P1619.0a
 - 3.1.3. Revision to 1619-2007 to include single-key mode
 - 3.1.4. Implications of SP 800-38E that limits the maximum size of each encrypted data unit
 - 3.1.5. Interest in a future face-to-face meeting
- 3.2. Approval Deferred
4. Approval of previous minutes
 - 4.1. Approval Deferred
5. Review of Previous Action Items
 - 5.1. Matt Ball to remove P1619.3 PAR and Project.
 - 5.1.1. Closed.
 - 5.2. Matt Ball to prepare informal notification that there will be a call for nomination and election of officers (and to please consider volunteering).
 - 5.2.1. Closed.
 - 5.3. Eric Hibbard to work with IEEE to resolve formal voting procedure requirements.
 - 5.3.1. Closed.
 - 5.4. Matt Ball to send out call for volunteers for P1619rev editor.
 - 5.4.1. Closed.
 - 5.5. Bob Lockhart to distribute draft 8 for comments.
 - 5.5.1. Closed.
 - 5.6. Matt Ball and Walt Hubis to update action plan based on capability to deliver draft 8.
 - 5.6.1. Closed.
 - 5.7. Matt Ball to migrate SISWG.NET to Grouper.IEEE.org.
 - 5.7.1. In progress.
 - 5.8. Matt Ball: 1619REV issues: Incorporate errata and NIST comments.
 - 5.8.1. Closed
6. New Business
 - 6.1. P1619rev
 - 6.1.1. Call for editors
 - 6.1.1.1. Subhash volunteers to edit this document.
 - 6.1.2. Discuss scope
 - 6.1.2.1. Unclear of interest in the need for XTS Single Key Mode.
 - 6.1.2.2. Changes Needed
 - 6.1.2.2.1. Editorial changes based on NIST and user feedback.
 - 6.1.2.2.2. Add one key XTS Mode.
 - 6.1.2.2.3. Provide one key XTS test vectors.
 - 6.1.2.2.4. Remove XML based key backup format.
 - 6.1.2.2.5. Clean up security rational, including rational for including one key XTS.
 - 6.1.3. Solicit any other recommendations for changes
 - 6.1.3.1. Request for additional changes after first draft.
 - 6.1.4. Face to face meeting
 - 6.1.4.1. No interest at this time.
 7. Next Meeting
 - 7.1. Wednesday, August 10, 2011, 10:00AM Pacific Time.
 8. Action Items
 - 8.1. Walt to check with TCG to determine interest.
 - 8.2. Eric to check CS1 interest.
 - 8.3. Luther to check with companies on FIPs certification for XTS mode.
 - 8.4. Matt to deliver last draft of 1619.
 - 8.5. Post documents to IEEE.Grouper website.
 - 8.6. Matt to give access information to officers and editors.
 9. Adjourn