P1619

Submitter Email: walt@hubis.com
Type of Project: Revision to IEEE Standard 1619-2007
PAR Request Date: 30-Jun-2017
PAR Approval Date: 28-Sep-2017
PAR Expiration Date: 31-Dec-2021
Status: PAR for a Revision to an existing IEEE Standard
Root Project: 1619-2007

1.1 Project Number: P1619
1.2 Type of Document: Standard
1.3 Life Cycle: Full Use

2.1 Title: Standard for Cryptographic Protection of Data on Block-Oriented Storage Devices
Changes in Title: IEEE Standard for Cryptographic Protection of Data on Block-Oriented Storage Devices

Contact Information for Working Group Chair
Name: Walter Hubis
Email Address: walt@hubis.com
Phone: 303.641.8528
Contact Information for Working Group Vice-Chair
Name: Eric Hibbard
Email Address: eric.hibbard@gmail.com
Phone: 408-314-0515

3.2 Sponsoring Society and Committee: IEEE Computer Society/Cybersecurity and Privacy Standards Committee (C/CPSC)
Contact Information for Sponsor Chair
Name: Eric Hibbard
Email Address: eric.hibbard@gmail.com
Phone: 408-314-0515
Contact Information for Standards Representative
Name: Eric Hibbard
Email Address: eric.hibbard@gmail.com
Phone: 408-314-0515

4.1 Type of Ballot: Individual
4.2 Expected Date of submission of draft to the IEEE-SA for Initial Sponsor Ballot: 01/2018
4.3 Projected Completion Date for Submittal to RevCom
Note: Usual minimum time between initial sponsor ballot and submission to Revcom is 6 months.: 10/2018

5.1 Approximate number of people expected to be actively involved in the development of this project: 10
Changes in scope: This standard specifies elements of an architecture for cryptographic protection of data in operation on block-oriented storage devices, describing the methods of Advanced Encryption algorithms. It is intended for use with block-oriented storage devices.

5.2 Scope: This standard specifies the XTS cryptographic mode of operation for the Advanced Encryption Standard (AES) block cipher for block-oriented storage devices.
Changes in scope: This standard specifies elements of an architecture for cryptographic protection of data in operation on block-oriented storage devices, describing the methods of Advanced Encryption algorithms. It is intended for use with block-oriented storage devices.

5.3 Is the completion of this standard dependent upon the completion of another standard: No

5.4 Purpose: The purpose of this standard is to define the XTS cryptographic mode while maintaining backward compatibility with existing implementations that are compliant with IEEE Std 1619-2007.
Changes in purpose: This standard is intended for use with block-oriented storage devices. It provides a secure and interoperable protection of data residing in storage.
5.5 Need for the Project: (1) IEEE Std 1619-2007 is nearing the end of the validity period.
(2) NIST has published XTS-AES in Jan-2010 as an approved mode in NIST SP 800-38E. As a result, changes will be required to maintain consistency, including but not limited to removal of XML based key archive functionality.

5.6 Stakeholders for the Standard: The stakeholders include vendors of data storage devices such disk drives, disk storage systems, and encryption appliances.

Intellectual Property
6.1.a. Is the Sponsor aware of any copyright permissions needed for this project?: No
6.1.b. Is the Sponsor aware of possible registration activity related to this project?: Yes
If yes please explain: The SISWG maintains an OID registry for cryptographic algorithms. See http://grouper.ieee.org/groups/1619/SISWG_OID_registry.txt

7.1 Are there other standards or projects with a similar scope?: No
7.2 Joint Development
   Is it the intent to develop this document jointly with another organization?: No

8.1 Additional Explanatory Notes: The revisions to the scope and purpose of 1619-2007 are intended to limit any changes to just the XTS mode of operation.

5.2 XTS refers to "XEX-based tweaked-codebook mode with ciphertext stealing". XTS is not typically expanded in this way in any publication.