P1619.1

Submitter Email: walt@hubis.com
Type of Project: Revision to IEEE Standard 1619.1-2007
PAR Request Date: 20-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: 1619.1-2007

1.1 Project Number: P1619.1
1.2 Type of Document: Standard
1.3 Life Cycle: Full Use

2.1 Title: Standard for Authenticated Encryption with Length Expansion for 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: 06/2018
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
5.2 Scope: This standard specifies requirements for cryptographic units that provide encryption and authentication for data contained within storage media.
Changes in scope: This standard specifies requirements for cryptographic units that provide encryption and authentication for data contained within storage media. Full interchange requires additional format specifications (such as compression algorithms and physical data format) that are beyond the scope of this standard.

5.3 Is the completion of this standard dependent upon the completion of another standard: No
5.4 Purpose: This standard is suitable for encryption of data stored on tape because tape easily accommodates length expanding ciphertext. In addition, this standard applies to other storage devices if these support storing extra metadata with each encrypted record. The algorithms of this standard are designed to ensure the confidentiality and integrity of stored data within systems requiring a high level of assurance.

5.5 Need for the Project: (1) IEEE Std 1619.1-2007 is nearing the end of the validity period.
5.6 Stakeholders for the Standard: The stakeholders include vendors of data storage devices such as tape drives, disk drives, 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: 5.2: The members of CPSC felt that the second sentence of the original description was out of place and distracted from the clarity and accuracy of the scope statement.