Email This Letter

07 June 2007

Jack Cole
US Army Research Laboratory
504 Idlewild Road
Bel Air, MD 21014-4419
jack.cole@ieee.org

Re: P1619.1 - Standard for Authenticated Encryption with Length Expansion for Storage Devices

Dear Jack:

I am pleased to inform you that on 07 June 2007 the IEEE-SA Standards Board approved the above referenced project until 31 December 2009. A copy of the file can be found on our website at http://standards.ieee.org/board/nes/projects/1619-1.pdf.

Now that your project has been approved, please forward a roster of participants involved in the development of this project. This request is in accordance with the IEEE-SA Operations Manual, Clause 5.1.2i under Duties of the Sponsor which states:

"Submit annually to the IEEE Standards Department an electronic roster of individuals participating on standards projects"

For your convenience, an Excel spreadsheet for your use has been posted on our website at http://standards.ieee.org/guides/par/roster.xls. Please forward this list to me via e-mail at s.hampton@ieee.org no later than 05 September 2007.

Please visit our website, IEEE Standards Development Online (http://standards.ieee.org/resources/development/index.html), for tools, forms and training to assist you in the standards development process. Also, we strongly recommend that a copy of your draft be sent to this office for review prior to the final vote by the working group to allow for a quick review by editorial staff before sponsor balloting begins.

If you should have any further questions, please contact me at +1 732 562 6003 or by email at s.hampton@ieee.org.

Sincerely,

Sherry Hampton
Administrator, Governance
Standards Activities
Phone +1 732 562 6003
FAX +1 732 875 0695
Email: s.hampton@ieee.org

CC: curtisanderson1@comcast.net, matt.ball@quantum.com BCC: s.hampton@ieee.org, t.t.lee@ieee.org

PAR Request Date: 27 April 2007

PAR Approval Date: 07 June 2007

PAR Signature Page on File: Yes

Type of PAR: Modification to Approved PAR

Status: Modification to a Previously Approved PAR P1619.1, 15 September 2006

Root Project: New Project

1.1 Project No.: 1619.1

1.2 Type of Document: Standard

1.3 Life Cycle: Full-Use

1.4 Is this document in ballot now? No

2.1 Title
Standard for Authenticated Encryption with Length Expansion for Storage Devices

3.1 Working Group Name	Security in Storage Working Group
Working Group Chair	Ball, Matt Phone: (720) 406-5766 Email: matt.ball@quantum.com
Working Group Vice Chair	Hibbard, Eric A Phone: 408-970-7979 Email: eric.hibbard@hds.com
3.2 Sponsor	IEEE Computer Society Information Assurance (C/IA)
Sponsor Chair	Cole, Jack Phone: 410 278 9276 Email: jack.cole@ieee.org
Name of Standards Liaison Representative (if applicable)	
3.3 Joint Sponsor	IEEE Computer Society Storage Systems (C/SS) Anderson, Curtis Email: curtisanderson1@comcast.net

4.1 Type of Ballot: Individual

4.2 Expected Date of Submission for Initial Sponsor Ballot: May 2007

4.3 Projected Completion Date for Submittal to RevCom: October 2008

5.1 Approximate number of people expected to work on this project: 30

5.2 Scope: This standard specifies requirements for cryptographic units that provide encryption and authentication for data contained within storage media. Full interchange requires additional specifications (such as compression algorithms and physical data format) that are beyond the scope of this standard.	**Old Scope:** This standard specifies requirements for cryptographic modules that provide encryption and authentication for data contained within storage media. Furthermore, this standard facilitates interchange between two compliant solutions through the specification of standard encryption algorithms. However, full interchange requires additional format specifications (such as compression algorithms) that are beyond the scope of this standard.

5.3 Is the completion of this document contingent upon the completion of another document? Yes
This standard uses an algorithm specified in P1619. This PAR request is to make minor changes to the Scope and Purpose so that the PAR can exactly match the final draft. These changes are largely editorial and represents, if anything, a slight narrowing of the scope.

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.	**Old Purpose:** This standard is especially suitable for encryption of data stored on tape because tape easily accommodates length-expanding ciphertext. In addition, this standard applies to hard disk drives if these support storing extra metadata with each record. The algorithms of this standard are suitable for ensuring the confidentiality and integrity of stored data within systems requiring a high level of assurance. By following this standard, a vendor creates encryption devices that a consumer can differentiate from proprietary implementations with generally lower security and limited interoperability.

5.5 Need for the Project: The confidentiality and integrity of information stored on tape is becoming a significant issue. This standard will address the security qualities and interoperability of encrypted storage systems, such as tape. <br> There is a market need, given the widespread use of removable storage (such as digital magnetic tape), to develop an independent standard for the cryptographic protection of this information. The standard will describe how storage systems can protect this information. This will benefit the users of these devices by allowing them to ensure the confidentiality of information stored on this media, and the public in general by protecting their private information in the event that a tape is lost. Further, this standard will allow multiple vendors to be able to interoperate when this data is encrypted.

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

6.1.a. Has the IEEE-SA policy on intellectual property been presented to those responsible for preparing/submitting this PAR prior to the PAR submittal to the IEEE-SA Standards Board? Yes **Presented Date:** 2006-08-04
If no, please explain:

6.1.b. Is the Sponsor aware of any copyright permissions needed for this project? No
If yes, please explain:

6.1.c. Is the Sponsor aware of possible registration activity related to this project? Yes
If yes, please explain: This standard uses an OUI (contained within an NAA or EUI-64) as part of an optional key transform function. The existing registries should be sufficient for registering these values.

7.1 Are there other standards or projects with a similar scope? No
If yes, please explain:

Sponsor Organization:
Project/Standard Number:
Project/Standard Date: 0000-00-00
Project/Standard Title:

7.2 Is there potential for this standard (in part or in whole) to be adopted by another national, regional, or international organization? ? Do not know at this time
Technical Committee Name and Number:
Contact person:
Contact person Phone Number:
Contact person Email Address:

7.3 Will this project result in any health, safety, security, or environmental guidance that affects or applies to human health or safety? No

7.4 Additional Explanatory Notes:
This modification was necessary for a couple reasons: - We decided to change the term 'cryptographic module' to 'cryptographic unit' so that we avoid confusion with NIST FIPS 140-2. - We ultimately determined that interchange was not achieved, so it made sense to remove mention of this. - There was some word-smithing to increase the precision of the Scope and Purpose for how the standard ultimately developed. We also removed subjective language that some members found disagreeable.

8.1 Sponsor Information:

Is the Scope of this project within the approved scope/definition of the Sponsor's Charter? Yes

If no, please explain: