

[Email This Letter](#)

09 May 2007

Curtis Anderson
Mendocino Software, Inc.
47001 Benicia Street
Fremont, CA 94538-7331
curtisanderson1@comcast.net

Re: P1619 - Standard for Cryptographic Protection of Data on Block-Oriented Storage Devices

Dear Curtis:

I am pleased to inform you that on 07 May 2007 the IEEE-SA Standards Board approved the above referenced project until 31 December 2008. A copy of the file can be found on our website at <http://standards.ieee.org/board/nes/projects/1619.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 August 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: jack.cole@ieee.org, matt.ball@quantum.com BCC: s.hampton@ieee.org, t.t.lee@ieee.org

PAR Request Date: 07 March 2007**PAR Approval Date:** 07 May 2007**PAR Signature Page on File:** Yes**Type of PAR:** Modification to Approved PAR**Status:** Modification to a Previously Approved PAR P1619, 15 August 2002**Root Project:** New Project**1.1 Project No.:** **1619****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 Cryptographic Protection of Data on Block-Oriented 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 Storage Systems \(C/SS\)](#)**Sponsor Chair**
[Anderson, Curtis](#)
Email: curtisanderson1@comcast.net**Name of Standards Liaison Representative (if applicable)****3.3 Joint Sponsor**
[IEEE Computer Society Information Assurance \(C/IA\)](#)
[Cole, Jack](#)
Phone: 410 278 9276
Email: jack.cole@ieee.org**4.1 Type of Ballot:** Individual**4.2 Expected Date of Submission for Initial Sponsor Ballot:** April 2007**4.3 Projected Completion Date for Submittal to RevCom:** September 2007**5.1 Approximate number of people expected to work on this project:** 30**5.2 Scope:** This standard specifies elements of an architecture for cryptographic protection of data on block-oriented storage devices, describing the methods, algorithms, and modes of data protection to be used.**Old Scope:** This standard specifies the architecture for protection-use-data in sector-level storage devices, describing the methods, algorithm(s), and modes of data protection to be used.**5.3 Is the completion of this document contingent upon the completion of another document?** No

5.4 Purpose: This standard defines specific elements of an architecture for cryptographically protecting data stored in constant length blocks. Specification of such a mechanism provides an additional and improved tool for implementation of secure and interoperable protection of data residing in storage.

Old Purpose: This standard provides a standard architecture for media security and enabling components. Present non-standard, insecure encrypted storage methodologies are augmented, and users will be able to create higher-assurance, standard, interoperable solutions.

5.5 Need for the Project: The confidentiality and integrity of information stored on block-oriented storage devices is becoming a significant issue. This standard will address the security qualities of encrypted storage systems. Block-oriented storage devices (e.g. disk drives) have special security requirements in that the length of a field must not be changed by the encryption algorithm. There is a market need, given the widespread use of removable and portable block storage devices (including magnetic disks and other media), to develop an independent standard for the cryptographic protection of 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 device is stolen or lost. Further, this standard may allow multiple vendors that use the encryption algorithms in the same way 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 disk drives, disk storage systems, 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: 2007-02-17

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? No

If yes, please explain:

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:

The title and scope were made more specific in order to better reflect the content of the standard. The original par was too broad.

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: