P1619.2 Wide-Block Encryption

Contributed by Administrator
Thursday, 19 July 2007
Last Updated Saturday, 29 November 2008

(Project 1619.2 November 2, 2006) Standard for Wide-Block Encryption for Shared Storage Media

Scope:This standard specifies an architecture for encryption of data in random access storage devices, oriented towards applications which benefit from wide encryption-block sizes of 512 bytes and above.

P1619.2 Task Group Chair: James P. Hughes, Sun Microsystems

P1619.2 Editor: Fabio Maino, Cisco Systems

- Comparison of proposed modes
- Mode comparison page
- Patent Correspondence

StatusAs of Nov 2008, the P1619.2 task group has decided on standardizing only EME2 and XCB, and has included these modes within the latest draft, with test vectors. The second working group ballot and first sponsor ballot will start before the end of 2008.

Draft Schedule:Sept 2008 - 1st Working Group Letter Ballot completed

Dec 15, 2008 - 2nd Working Group letter ballot completes

Jan 22, 2009 - Sponsor Ballot completes

Feb 6, 2009 - Submit to IEEE RevCom

March 17-19, 2009 - IEEE RevCom and Standards Boards Reviews standard

Sept 2009 - (If approved) IEEE publishes 1619.2

Reference ImplementationsThere are reference implementations available for EME2, and soon for XCB, available on SourceForge within the Crypto1619 project .

Brian Gladman also has an EME2 reference implementation available here .