

IEEE Security in Storage Workgroup (P1619.x) Status to T10

Matt Ball, SISWG Chair

M.V. Ball Tech

November 6, 2007

P1619 “Disk encryption” and P1619.1 “Tape encryption”

- Both P1619 and P1619.1 have successfully completed recirculation ballots and are now waiting for approval by IEEE RevCom on Dec 4, 2007
- Publication typically takes 2-6 months, but can be expedited for about \$9k (any interest?)
- Call for interest in follow-on projects, including amendments.
- We are planning to submit XTS to NIST for consideration as a FIPS 140-2 approved mode of operation.

P1619.2 “Wide block encryption”

- Held a face-to-face meeting in San Diego with the Security in Storage workshop (SISW) in September
- Rogaway was able to convince the University of California to provide a royalty-free license for EME*
- No updates on the draft

P1619.3 “Key Management”

- Significant work in the subcommittees, including Architecture, Objects and Operations, and Namespace (see e-mail reflector and website).
- New e-mail list:
<http://grouper.ieee.org/groups/1619/email-3/>
- No updates to the draft