memorandum

Hewlett-Packard Company
3000 Hanover Street
Palo Alto, CA 94304-1185
USA
www.hp.com

T10/06-006r0

To	From	Subject	Date
INCITS T10 Committee	Chris Williams, HP	SSC Encryption Strawman	25 November 2005

Revision history

Revision 0 – Initial document.

Related documents

None

Background

The intent of this document is to define a method for controlling encryption in an SSC Device Server

This document is based on IEEE 1619.1, while allowing for other encryption algorithms.
This means that algorithm ID's and flexible data structures will be needed to pass varying lengths of keys, IV's, and other data needed, such as Additional Authenticated Data in IEEE 1619.

This is also based on using unencrypted keys, with extensions to be defined later for handling encrypted keys. All efforts will be made to allow these extensions to be defined in a backward compatible manner.

Keys will be Write-only, to minimize the chance of retrieving the key from the device server.

Being able to read the encrypted data for decryption outside the drive is required.

It is assumed that the application software will be in control of the encryption process, and aware of what needs to be done.

Basic Operational Modes:

Standard: No encryption/decryption functions. Unencrypted data does not change.
On a read, if there is encrypted data on the media, it is passed encrypted to the host.

Encrypt Data: Data is encrypted with the provided key and defined algorithm

Decrypt data: Data is decrypted with the provided key and defined algorithm

Decrypt Mixed Data: Encrypted data is decrypted with the provided key and defined algorithm. Unencrypted data is passed thru without decryption. Note that some formats or implementations may not allow this mode.

Once written, the key will reside in the device server until a) it is overwritten, b) a zero key command is received, c) power is removed, d) Media unload e) a Hard Reset is received.

Functions required:

Identify drive capabilities:
Encryption supported, algorithm ID's supported (table tbd.)
Key lengths and types supported
IV required?
Additional data required and/or allowed, and byte count (16 byte increments for IEEE 1619.1)

Send to Drive, Encryption:
Encryption on/off
Key (possibly wrapped with a CRC – there is no way to verify the key once it is written)
Additional Data (AAD, such as a Key ID in IEEE 1619.1), byte count
IV (optional)

Hewlett-Packard Company
3000 Hanover Street
Palo Alto, CA 94304-1185
USA
www.hp.com

T10/06-006r0

, 2005

Send to Drive, Decryption:
Decryption control: Off (default), On., auto (pass unencrypted data, decrypt encrypted data with key),
Key, as above.
IV (optional)

Housekeeping functions:
Zero Key function: Overwrites the key in the device server with zeroes, and turns off all encryption and decryption functions.
Crypto Module Selftest: Verify operation with known or provided data, AAD, IV, and key, Resulting data must be returned to allow external verification, in addition to internal test modes.

Read Data:
AAD (including Key ID if defined), IV, and Encryption type ID, must be available after a Read,. This applies to the record at the current logical position on media.

Error detection and reporting: Sense codes, possibly descriptor format sense data also
Invalid key (usually means key has not been set)
Key transmission error (crc fail, in future key decryption error)
Encryption failure – required data not set
Encryption/Decryption Failure, HW error
Decryption Error (record does not authenticate). Caused by incorrect key or HW failure
Decryption Error, decryption of unencrypted data attempted.
Decryption Error, reason unknown
Key Changed (UA to all initiators?)

Tape alert flags : TBD

Need controls on error reporting to allow auto decryption without errors being reported, and allow reading of encrypted data from the device.

Still needing definition:

Extended Copy behavior