To: INCITS T10 Committee

From: Paul Entzel, Quantum

Date: 29 August 2006

Document: T10/06-391r0

Subject: SSC-3 Remove IV fields from the Data Encryption Algorithm descriptor

1 Revision History

Revision 0:
Posted to the T10 web site on 29 August 2006.

2 Reference

T10/SSC-3 revision 3a

3 General

The IV_MU, IV_WPU, IV_EBU, and IV_RN field in the Data Encryption Algorithm descriptor were originally added to provide some guidance to the application client with regards to the uniqueness of the IV being generated by the device server. This was intended to be used to decide how often the key or nonce should be changed by the application client to protect against IV collisions. However, from the questions I've received these fields instead appear to cause even more confusion than the resolve. To solve this problem, this proposal recommends that we remove these fields now and convert the space to "reserved" until such time as we come up with a better method.

Proposed additions or changes to the SSC-3 standard are shown in blue text; proposed deletions are shown in ~~red crossed out text~~, changed test are shown in red.

4 Changes to SSC-3

In table 98 of SSC-3 revision 3a, remove the bit fields labeled IV_MU, IV_WPU, IV_EBU, and IV_RN and convert the space to a single 4 bit reserved field.

Remove the following paragraphs from subclause 8.5.2.4 that describe these fields:

~~The initialization vector medium unique (IV_MU) bit shall be set to one if the initialization vector used by the encryption algorithm is unique for each medium. The IV_MU bit shall be set to zero if the initialization vector used by the encryption algorithm is not unique for each medium.~~

~~The initialization vector write pass unique (IV_WPU) bit shall be set to one if the initialization vector used by the encryption algorithm is unique for each write operation that over writes the same portion of the medium. The IV_WPU bit shall be set to zero if the initialization vector used by the encryption algorithm is not unique for each write operation that over writes the same portion of the medium.~~

~~The initialization vector encrypted block unique (IV_EBU) bit shall be set to one if the initialization vector used by the encryption algorithm is unique for each encrypted block on the medium. The IV_EBU bit shall be set to zero if the initialization vector used by the encryption algorithm is not unique for each encrypted block on the medium.~~

~~The initialization vector random number (IV_RN) bit shall be set to one if the initialization vector used by the encryption algorithm is either in part or wholly a random number. The IV_RN bit shall be set to zero if the initialization vector used by the encryption algorithm is not in part or wholly a random number.~~