To: INCITS T10 Committee
From: Paul Entzel, Quantum
Date: 25 April 2007
Document: T10/07-204r0
Subject: SSC-3: Fix conflict between 06-412r3 and 07-016r2

1 Revision History

Revision 0:
Initial revision posted to the T10 web site on 25 April 2007.

2 Reference

T10/SSC-3 revision 3c
T10/06-412r3, SSC-3 Encryption KAD Lengths and Nonces
T10/07-016r2, SSC-3 Additional controls for keyless copy

3 General

On 3 January 2007 the SSC-3 working group approved proposal 06-412r2 as revised for inclusion in SSC-3. In a teleconference on 10 April 2007 the SSC-3 working group approved proposal 07-016r2 for inclusion in SSC-3. Both of these proposals assigned new meaning to the previously reserved bits 0 and 1 in byte 5 of the Data Encryption Algorithm descriptor (table 99 in SSC-3 revision 3c). The new meaning assigned to these bits is not the same in the 2 proposals, not even close.

Here is how the byte looks after 06-412r3 modifies it:

Bit Byte	7	6	5	4	3	2	1	0
5	Reserved		NONCE_C		Reserved		UKADF	AKADF

Here is how the byte looks after 07-016r2 modifies it:

Bit Byte	7	6	5	4	3	2	1	0
5	Reserved		NONCE_C		RDMC_C			EAREM

Since 06-412r3 was approved first, it should take precedence forcing a move of the fields defined in 07-016r2. However, this is complicated because 07-016r2 requires a 3 bit field and there are no reserved fields with 3 consecutive bits left in byte 5 after 06-412r3 grabs bits 0 and 1. The simpler approach is to move the two bits defined in 06-412r3 to bits 6 and 7 and put the 2 fields in 07-016r2 into bits 0 through 3, but this may cause problems for anyone already implementing 06-412r3. So, this proposal has 2 alternatives from which to choose.

4 Changes to SSC-3

4.1 Alternative 1

Modify byte 5 of table 99 in SSC-3 revision 3c as follows:

Bit Byte	7	6	5	4	3	2	1	0
5	UKADF	AKADF	NONCE_C		RDMC_C			EAREM

4.2 Alternative 2

Define byte 5 of table 99 in SSC-3 revision 3c as show below (from 06-412r3):

Bit Byte	7	6	5	4	3	2	1	0
5	Reserved		NONCE_C		Reserved		UKADF	AKADF

Modify byte 12 of table 99 in SSC-3 revision 3c as shown below (to accommodate 07-016r2). Byte 12 is currently reserved:

Bit Byte	7	6	5	4	3	2	1	0
12	Reserved				RDMC_C			EAREM