ENDL
TEXAS

Date: 18 August 2005
To: T10 Technical Committee & SNIA OSD TWG
From: Ralph O. Weber
Subject: No Capability can have a Vendor Specific integrity check value algorithm

In OSD-2 r00, the Capability format includes a four-bit INTEGRITY CHECK VALUE ALGORITHM field.

Table 6 — Capability format

Bit Byte	7	6	5	4	3	2	1	0
0	Reserved				CAPABILITY FORMAT (1h)			
1	KEY VERSION				INTEGRITY CHECK VALUE ALGORITHM			
2	Reserved				SECURITY METHOD			
3	Reserved							
	⋮							

However, the supported integrity check value algorithm attributes in the Root Policy/Security attributes page define Vendor Specific integrity check value algorithm values that do not fit in four bits.

Table 114 — Supported integrity check value algorithm codes

Value	Algorithm	Reference
00h	No algorithm supported	
01h	HMAC-SHA1	FIPS 180-1 (1995) and FIPS 198 (2002)
02h - DFh	Reserved	
E0h - FFh	Vendor specific	

To correct the problem, table 114 needs to be changed.

All references are to osd2r00.pdf.

Detailed OSD-2 Changes

Table 114 — Supported integrity check value algorithm codes

Value	Algorithm	Reference
00h	No algorithm supported	
01h	HMAC-SHA1	FIPS 180-1 (1995) and FIPS 198 (2002)
02h - ~~DFh~~ 09h	Reserved	
0Ah - 0Fh	Vendor specific	
10h - FFh	Reserved	
~~E0h - FFh~~	~~Vendor specific~~	