

To: INCITS T10 Committee  
From: Paul Entzel, Quantum  
Date: 5 October 2006  
Document: T10/06-453r0  
Subject: SSC-3 Add a random number page to the Tape Data Encryption protocol



## 1 Revision History

Revision 0:  
Posted to the T10 web site on 5 October 2006. Derived from 06-385r0 with comments from the September 2006 SSC-3 working group meeting.

## 2 Reference

T10/SSC-3 revision 3a

## 3 General

Many tape drives have available within them a pretty good entropy source making the generation of a good random number a fairly straight forward process. Since a random number source this good is not always available to the application clients through other means, it would be helpful to at least offer access to the random number generator through SCSI.

## 4 Changes to SSC-3

Add a new page to return a random number. Support for this page is optional.

In 8.5.2.1 (SECURITY PROTOCOL IN command specifying Tape Data Encryption security protocol overview), add to the security protocol specific field values table (table 93) the following entry:

Code	Description	Reference
0021h	Next Block Encryption Status page	8.5.2.8
0022h – 002Fh	Reserved	
0030h	Random Number page	8.5.2.9
0031h - FFFFh	Reserved	

Add the following subclause:

### 8.5.2.9 Random Number page

Table X specifies the format of the Random Number page.

**Table X – Random Number page**

Byte	Bit	7	6	5	4	3	2	1	0
0	(MSB)	PAGE CODE (0030h)							
1		(LSB)							
2	(MSB)	PAGE LENGTH (32)							
3		(LSB)							
4		RANDOM NUMBER							
35									

The RANDOM NUMBER field contains a random nonce (see SPC-4) generated by the device server using a source of entropy available within the device. Each request for the Random Number page shall return a different value in the RANDOM NUMBER field.