To: INCITS Technical Committee T10
From: Dale LaFollette
Date: Friday, October 10, 2008 4:08 PM
Document: T10/08-410r0 – SSC-3: Resolution to LB Comment EMC-001

1 Revisions

1. 08-410r0 Initial revision

2 Introduction

During SSC-3 letter ballot EMC submitted Letter Ballot comment 001 that reads:

> From the spec it looks like if the SDK_C bit is set then the device supports supplemental decryption keys but the only way to determine how many is by setting the SDK's until you get a MAXIMUM NUMBER OF SUPPLEMENTAL DECRYPTION KEYS EXCEEDED error (Set Data Encryption Page for SECURITY PROTOCOL OUT - 8.5.3.2.1, p.192). It would be nice if SECURITY PROTOCOL IN could provide that info before the error occurs, perhaps in the Data Encryption Algorithm descriptor.

This proposal intends to resolve that comment.

In the course of preparing this resolution I discovered that additional information was needed for the operation of Decrypting and Supplemental Decryption Keys usage.

Key:

~~Deleted Text~~

Added Text

Editors Notes

3 Proposal

4.2.21.13 Unauthenticated key-associated data (U-KAD) and authenticated key-associated data (A-KAD)

Some encryption algorithms allow or require the use of additional data which is associated with the key and the plaintext, but which is not encrypted. It may be authenticated by being included in the message authentication code (MAC) calculations for the encrypted plaintext if such a MAC exists, or unauthenticated by not being included in these calculations.

The device server reports its capability with respect to key-associated data in the Data Encryption Algorithm descriptor(s) (see 8.5.2.4). If the device server reports that it requires key-associated data from the application client and a Set Data Encryption page is processed that does not include a key-associated data descriptor, the device server shall terminate the command with CHECK CONDITION, with the sense key set to ILLEGAL REQUEST, and the additional sense code set to INCOMPLETE KEY-ASSOCIATED DATA SET.

NOTE 12 A key-identifier or key reference may be stored in the U-KAD or A-KAD.

The U-KAD field is provided for applications that do not require the key-associated data to be protected by an MAC.

8.5.2.4 Data Encryption Capabilities page

The Data Encryption Capabilities page Data Encryption Capabilities page requests that information regarding the set of data encryption algorithms reported by this device server be sent to the application client. If external data encryption control is supported, then the set of data encryption algorithms reported by the device server may not include all of the algorithms in the set of data encryption algorithms supported by the physical device.

Table 121 — Data Encryption Capabilities page

Bit / Byte	7	6	5	4	3	2	1	0
0	(MSB)							
1	PAGE CODE (0010h)							(LSB)
2	(MSB)							
3	PAGE LENGTH (n-3)							(LSB)
4	Reserved				EXTDECC		CFG_P	
5	Reserved							
19								
	Data Encryption Algorithm descriptor list							
20	Data Encryption Algorithm descriptor (first)							
	Data Encryption Algorithm descriptor (last)							
n								

See SPC-4 for a description of the PAGE CODE field PAGE LENGTH field. The page code field shall be set to the value specified in Data Encryption Capabilities page.

The external data encryption control capable (EXTDECC) field specifies the external data encryption control capability of the physical device. The EXTDECC field values are specified in EXTDEC.

Table 122 — EXTDECC field values

Code	Description
00b	The external data encryption control capability is not supported.
01b	The physical device is not external data encryption control capable.
10b	The physical device is external data encryption control capable.
11b	Reserved

The configuration prevented (CFG_P) field specifies the data encryption parameters configuration capabilities for the algorithms reported in the Data Encryption Algorithm descriptors. The CFG_P field values are specified in CFG_.

Table 123 — CFG_P field values

Code	Description
00b	The data encryption configuration capabilities are not reported.
01b	The physical device configured to allow this device server to establish or change data encryption parameters.
10b	The physical device is configured to not allow this device server to establish or change data encryption parameters.
11b	Reserved

Each Data Encryption Algorithm descriptor Data Encryption Algorithm descriptor contains information about a data encryption algorithm supported by the device server. If more than one descriptor is included, they shall be sorted in ascending order of the value in the ALGORITHM INDEX field.

Table 124 — Data Encryption Algorithm descriptor

Bit / Byte	7	6	5	4	3	2	1	0
0	ALGORITHM INDEX							
1	Reserved							
2	(MSB)							
3	DESCRIPTOR LENGTH (20)							(LSB)
4	AVFMV	SDK_C	MAC_C	DED_C	DECRYPT_C		ENCRYPT_C	
5	AVFCLP		NONCE_C		DKAD_C ~~Reserved~~	VCELB_C	UKADF	UAKADF
6	(MSB)							
7	MAXIMUM UNAUTHENTICATED KEY-ASSOCIATED DATA BYTES							(LSB)
8	(MSB)							
9	MAXIMUM AUTHENTICATED KEY-ASSOCIATED DATA BYTES							(LSB)
10	(MSB)							
11	KEY SIZE							(LSB)
12	Reserved					RDMC_C		EAREM
~~13~~	~~Reserved~~							
~~19~~								
13	Reserved							
14	(MSB)							
15	UNDEFINED SUPPLEMENTAL KEYS							(LSB)
16	Reserved							
19								
20	(MSB)							
23	SECURITY ALGORITHM CODE							(LSB)

The ALGORITHM INDEX field is a device server assigned value associated with the algorithm that is being described. The value in the ALGORITHM INDEX field is used by the SECURITY PROTOCOL OUT command Set Data Encryption page to select this algorithm.

The algorithm valid for mounted volume (AVFMV) bit shall be set to one if there is a volume currently mounted and the encryption algorithm being described is valid for that volume. The AVFMV bit shall be set to zero if there is no volume mounted or the algorithm is not valid for the currently mounted volume.

The supplemental decryption key capable (SDK_C) bit shall be set to one if the device server is capable of supporting one or more supplemental decryption keys. If the SDK_C bit is set to one, then the UNDEFINED SUPPLEMENTAL KEYS field shall contain a non-zero value. The supplemental decryption keys shall be used for decryption only. The SDK_C bit shall be set to zero if the device server is not capable of supporting supplemental decryption keys. If the SDK_C bit is set to zero, then the UNDEFINED SUPPLEMENTAL KEYS field shall contain a zero value.

The distinguish encrypted data capable (DED_C) bit shall be set to one if the device server is capable of distinguishing encrypted data from unencrypted data when reading it from the medium. The DED_C bit shall be set to zero if the device server is not capable of distinguishing encrypted data from unencrypted data when reading it from the medium. If the ability to distinguish encrypted data from unencrypted data is format specific and a volume is mounted, the DED_C bit shall be set based on the current format of the medium. If no volume is mounted, the DED_C bit shall be set to one if the device server is capable of distinguishing encrypted data from unencrypted data in any format that the device server supports.

The message authentication code capable (MAC_C) bit shall be set to one if the algorithm includes a message authentication code added to encrypted blocks. The MAC_C bit shall be set to zero if the algorithm does not include a message authentication code added to encrypted blocks. If the inclusion of a message authentication code is format specific and a volume is mounted, the MAC_C bit shall be set based on the current format of the medium. If no volume is mounted, the MAC_C bit shall be set to one if the device server adds a message authentication code to data encrypted with this algorithm in any format that the device server supports.

The DECRYPT_C field DECRYPT_ specifies the decryption capabilities of the physical device.

Table 125 — DECRYPT_C field values

Code	Name	Description
00b	no capability	The physical device has no has data decryption capability using this algorithm. This value shall be returned if the specified algorithm is disabled.
01b	software capable	The physical device has the ability to decrypt data using this algorithm in software.
10b	hardware capable	The physical device has the ability to decrypt data using this algorithm in hardware.
11b	capable with external control	The physical device has the capability to decrypt data using this algorithm, but control of the data encryption parameters by this device server is prevented.

The ENCRYPT_C field ENCRYPT_ specifies the encryption capabilities of the physical device.

Table 126 — ENCRYPT_C field values

Code	Name	Description
00b	no capability	The physical device has no has data encryption capability using this algorithm. This value shall be returned if the specified algorithm is disabled.
01b	software capable	The physical device has the ability to encrypt data using this algorithm in software.
10b	hardware capable	The physical device has the ability to encrypt data using this algorithm in hardware.
11b	capable with external control	The physical device has the capability to encrypt data using this algorithm, but control of the data encryption parameters by this device server is prevented.

The algorithm valid for current logical position (AVFCLP) field specifies if the encryption algorithm being specified is valid for writing to the mounted volume at the current logical position. AVFCL specifies the values for the AVFCLP field.

Table 127 — AVFCLP field values

Code	Description
00b	Current logical position is not applicable to the encryption algorithm validity or no volume is loaded.
01b	The ecryption algorithm being specified is not valid for writing to the mounted volume at the current logical position.
10b	The ecryption algorithm being specified is valid for writing to the mounted volume at the current logical position.
11b	Reserved

Table 128 specifies the values for the NONCE_C field.

Table 128 — NONCE_C field values

Code	Description
0	This algorithm does not require a nonce value.
1	The device server generates the nonce value.
2	The device server requires all or part of the nonce value to be provided by the application client.
3	The device server supports all or part of the nonce value provided by the application client. If the Set Data Encryption page that enables encryption does not include a nonce value descriptor, the device server generates the nonce value.

If the Decryption KAD (DKAD_C) bit is set to one, then this algorithm requires a key-associated data descriptor, U-KAD or A-KAD, to be provided by the application client for decryption operations. If the Decryption KAD (DKAD_C) bit is set to zero, then this algorithm does not require a key-associated data descriptor, U-KAD or A-KAD, to be provided by the application client for decryption operations.

If the volume contains encrypted logical block capable (VCELB_C) bit is set to one, then the device server is capable of determining that a volume contains logical blocks encrypted using this algorithm when the volume is mounted. If the VCELB_C is set to zero, then the device server is not capable of determining that a volume contains logical blocks encrypted using this algorithm when the volume is mounted. If the capability of determining that a volume contains logical blocks encrypted using this algorithm is format specific and a volume is mounted, then the VCELB_C bit is set based on the current format of the medium. If no volume is mounted, the VCELB_C bit is set to one if for at least one algorithm that the device server supports the device server is capable of determining that a volume contains logical blocks encrypted using that algorithm.

The U-KAD Fixed (UKADF) bit shall be set to one if the device server requires the length of U-KAD in the parameter data for a SECURITY PROTOCOL OUT command to equal the value in the MAXIMUM UNAUTHENTICATED KEY-ASSOCIATED BYTES field. If the UKADF bit is set to one, then the MAXIMUM UNAUTHENTICATED KEY-ASSOCIATED BYTES field shall contain a non-zero value. If the UKADF bit is set to zero and the value in the MAXIMUM UNAUTHENTICATED KEY-ASSOCIATED BYTES field is non-zero, then the length of the U-KAD, if present in the parameter data for a SECURITY PROTOCOL OUT command, shall be a value between one and the value in the MAXIMUM UNAUTHENTICATED KEY-ASSOCIATED BYTES field.

The A-KAD Fixed (AKADF) bit shall be set to one if the device server requires the length of A-KAD in the parameter data for a SECURITY PROTOCOL OUT command to equal the value in the MAXIMUM AUTHENTICATED KEY-ASSOCIATED BYTES field. If the AKADF bit is set to one, then the MAXIMUM AUTHENTICATED KEY-ASSOCIATED BYTES field shall contain a non-zero value. If the AKADF bit is set to zero and the value in the MAXIMUM AUTHENTICATED KEY-ASSOCIATED BYTES field is non-zero, then the length of the A-KAD, if present in the parameter data for a SECURITY PROTOCOL OUT command, shall be a value between one and the value in the MAXIMUM AUTHENTICATED KEY-ASSOCIATED BYTES field.

The MAXIMUM UNAUTHENTICATED KEY-ASSOCIATED DATA BYTES field indicates the maximum size of the unauthenticated key-associated data (see 4.2.21.13) that the device server can support for this algorithm.

The MAXIMUM AUTHENTICATED KEY-ASSOCIATED DATA BYTES field indicates the maximum size of the authenticated key-associated data (see 4.2.21.13) that the device server can support for this algorithm.

The KEY SIZE field indicates the size in bytes of the encryption key required by the algorithm.

The raw decryption mode control capabilities (RDMC_C) field indicates the capabilities the encryption algorithm provides to the application client to control read operations that access encrypted blocks while the decryption mode is set to RAW. RDMC_C defines the values for the RDMC_C field.

Table 129 — RDMC_C field values

Code	Description
0h	No capabilities are specified.
1h	The encryption algorithm does not allow read operations in RAW decryption mode.
2h-3h	Reserved
4h	The encryption algorithm disables read operations in RAW mode by default and allows the application client to control RAW reads via the RDMC field in the Set Data Encryption page **Error! Reference source not found.**.
5h	The encryption algorithm enables read operations in RAW mode by default and allows the application client to control RAW reads via the RDMC field in the Set Data Encryption page **Error! Reference source not found.**.
6h	The encryption algorithm disables read operations in RAW mode by default and does not allow the application client to control RAW reads via the RDMC field in the Set Data Encryption page **Error! Reference source not found.**.
7h	The encryption algorithm enables read operations in RAW mode by default and does not allow the application client to control RAW reads via the RDMC field in the Set Data Encryption page **Error! Reference source not found.**.

The encryption algorithm records encryption mode (EAREM) bit shall be set to one if the encryption mode is recorded with each encrypted block. The EAREM bit shall be set to zero if the encryption mode is not recorded with each encrypted block.

The UNDEFINED SUPPLEMENTAL KEYS field contains the current number of undefined supplemental keys that the device server has available for use with this algorithm. If there are currently no supplemental keys loaded then this value would be the maximum number of supplemental keys that this device server supports with this algorithm.

The SECURITY ALGORITHM CODE field contains an security algorithm code (see SPC-4).