January 23, 2006 06-051r2 The Requirement for More than One Decryption Key

To: T10 Technical Committee
From: Dwayne Edling (dwayne.edling@sun.com)
Date: 23 Jan 2006
Subject: T10/06-051r2 The Requirement for More than One Decryption Key

Revision History

Revision 0 (7 Jan 2006): Presentation to explain the need for more than one decryption key.
Revision 1 (19 Jan 2006): First proposal to implement more than one read Key.

Related Documents

05-446r1 - SSC-3: Add commands to control data encryption

Overview

Revision 1

This proposal incorporates changes that would be necessary to implement passing more than one decryption key in proposal 05-446r1.

- Added to Data encryption algorithm descriptor page:
  - MAXIMUM NUMBER OF ENCRYPTION KEYS
  - MAXIMUM NUMBER OF DECRYPTION KEYS
  - MAXIMUM NUMBER OF COMBINED KEYS (Used for both encryption and decryption)
  - MAXIMUM NUMBER OF KEYS FOR ALL MODES AND SCOPES
- Added to the Data encryption status page
  - NUMBER OF ENCRYPTION KEYS IN USE
  - NUMBER OF DECRYPTION KEYS IN USE
  - NUMBER OF COMBINED KEYS IN USE
  - NUMBER OF KEYS IN USE FOR ALL MODES AND SCOPES
- Added to the Set data encryption page.
  - KEY USE field; indicates whether this is a combined use key, encryption key or decryption key.
  - Keep Previous Decryption Key (KPDK) field; this field indicates whether the device server should keep the previously send decryption key.
  - Add scenarios how keys are sent and status that gets reported.
- I believe that I retained the functionality of the previous draft so that the model should not have to change.
- There were also some edits in the model sections to incorporate the concept of more than one key being used in the system.

Revision 2

Added edits from Paul Entzel.

- Changed wording in model section.

- Moved the following fields to the Data Encryption capabilities page
  - MAXIMUM NUMBER OF ENCRYPTION KEYS
  - MAXIMUM NUMBER OF DECRYPTION KEYS
  - MAXIMUM NUMBER OF COMBINED KEYS (Used for both encryption and decryption)
  - MAXIMUM NUMBER OF KEYS FOR ALL MODES AND SCOPES
- Changed wording in Set data encryption page to clarify various SCOPE and mode uses. Also changed various wording to add clarity. Removed last paragraph.

Suggested Changes

4.2.19.5 Managing keys within the device server

The security provided by data encryption is only as good as the security used when managing the keys. For this reasons, the data encryption key and mode are volatile in the device server and never reported to an initiator. The device server also may have limited resources for storage of keys.

If a device server processes a Set Data Encryption page with the ENCRYPTION MODE field set to DISABLE and DECRYPTION MODE field set to DISABLE or RAW, the device server shall release any resources that it had allocated to store a key value for the I_T nexus associated with the DATA SECURITY OUT command and shall clear any memory containing the key value. A unit attention condition with the additional sense of DATA ENCRYPTION MODE CHANGED BY ANOTHER INITIATOR shall be establish for any other I_T nexus that is affected by the loss of the key, (i.e., any I_T nexus that is using a scope of PUBLIC and sharing the key.)

Editor's note: DATA ENCRYPTION MODE CHANGED BY ANOTHER INITIATOR is a new ASC.

If a device server processes a Set Data Encryption page that includes an ~~key~~ ENCRYPT ~~write encryption~~ or COMBINED key~~, a COMBINED key can be used for either encryption or decryption,~~ or DECRYPT key with the keep previous decryption key (KPDK) bit set to zero, the device server shall release any resources that it had allocated to store ~~a~~ key values of the type specified in the KEY USE field of the Set Data Encryption page set by a previous DATA SECURITY OUT command from that I_T nexus and shall clear any memory containing the key values. A unit attention condition with the additional sense of DATA ENCRYPTION MODE CHANGED BY ANOTHER INITIATOR shall be establish for any other I_T nexus that is affected by the change of the keys (i.e., any I_T nexus that is using a scope of PUBLIC and sharing the key).

A device server shall save at most ~~the number of keys reported in the Data encryption algorithm descriptor page~~ one ENCRYPT key or one COMBINED key and the MAXIMUM NUMBER OF DECRYPTION KEYS reported in the Data Encryption Capabilities page ~~one key~~ with a scope of ALL I_T NEXUS. If a device server processes a Set Data Encryption page with the SCOPE field set to ALL I_T NEXUS, the device server shall release any resources that it had allocated to store ~~a key value write encryption or COMBINED key value or a read decryption key value with the keep previous decryption key (KPDK) set to zero~~ keys of the type specified in the KEY USE field of the Set Data Encryption page set by a previous DATA SECURITY OUT command with a scope value

of ALL I_T NEXUS and shall clear any memory containing the key values. A unit attention condition with the additional sense of DATA ENCRYPTION MODE CHANGED BY ANOTHER INITIATOR shall be establish for any other I_T nexus that is affected by the change of the keys, that is, any I_T nexus that is using a scope of public and sharing the key.

A device server shall save at most ~~the number of keys reported in the Data encryption algorithm descriptor page~~ one DECRYPT key or one COMBINED key and the MAXIMUM NUMBER OF DECRYPTION KEYS reported in the Data Encryption Capabilities page ~~one key~~ with a scope of RESERVATION GROUP. If a device server processes a Set Data Encryption page with the SCOPE field set to RESERVATION GROUP, the device server shall release any resources that it had allocated to store ~~a key value write encryption or COMBINED key value or a read decryption key value with the keep previous decryption key (KPDK) set to zero~~ keys of the type specified in the KEY USE field of the Set Data Encryption page set by a previous DATA SECURITY OUT command with a scope value of RESERVATION GROUP and shall clear any memory containing the key values. A unit attention condition with the additional sense of DATA ENCRYPTION MODE CHANGED BY ANOTHER INITIATOR shall be establish for any other I_T nexus that is affected by the change of the keys, that is, any I_T nexus that is using a scope of public and sharing the key.

If a vendor specific event occurs that changes or clears ~~a~~ data encryption keys, the device server shall establish a unit attention condition with the additional sense of DATA ENCRYPTION MODE CHANGED BY OUT-OF-BAND EVENT for any I_T nexus that is affected by the change of the key.

Editor's note: DATA ENCRYPTION MODE CHANGED BY OUT-OF-BAND EVENT is a new ASC.

7.X.4 Data encryption capabilities page

Table E1 shows the format of the Data encryption capabilities page.

Table E1 – Data Encryption capabilities page

Bit / Byte	7	6	5	4	3	2	1	0
0	PAGE CODE (10h)							
1	Reserved							
2	(MSB)	PAGE LENGTH (n-3)						
3								(LSB)
4	(MSB)	MAXIMUM NUMBER OF ENCRYPTION KEYS						
5								(LSB)
6	(MSB)	MAXIMUM NUMBER OF COMBINED KEYS						
7								(LSB)
8	(MSB)	MAXIMUM NUMBER OF DECRYPTION KEYS						
9								(LSB)
10	(MSB)	MAXIMUM NUMBER KEYS FOR ALL MODES AND SCOPES						
11								(LSB)
	Encryption algorithm descriptors							
12	(MSB)	Data encryption algorithm descriptor						
								(LSB)
	:							
	(MSB)	Data encryption algorithm descriptor						
S								(LSB)

See SPC-3 for a description of the PAGE LENGTH field.

The MAXIMUM NUMBER OF ENCRYPTION KEYS field indicates the maximum number of write encryption keys that the device server has resources to store at any one time.

The MAXIMUM NUMBER OF COMBINED KEYS field indicates the maximum number of keys which can be used for both write encryption and read decryption that the device server has resources to store at any one time.

The MAXIMUM NUMBER OF DECRYPTION KEYS field indicates the maximum number of read decryption keys that the device server has resources to store at any one time.

The MAXIMUM NUMBER OF KEYS FOR ALL MODES AND SCOPES field indicates the maximum number of keys for either write encryption or read decryption that the device

server can save at any one time. This field shall be the total of encryption keys, COMBINED keys and decryption keys that the device server has resources to store.

Each data encryption algorithm descriptor (see table E2) 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 E2 – Data encryption algorithm descriptor

Bit / Byte	7	6	5	4	3	2	1	0
0	ALGORITHM INDEX							
1	Reserved							
2	(MSB)	DESCRIPTOR LENGTH (n-3)						
3								(LSB)
4	Reserved	KBR_C	MAC_C	DED_C	DECRYPT_C		ENCRYPT_C	
5	Reserved		NONCE_C		IV_RN	IV_EOU	IV_WPU	IV_MU
6	(MSB)	MAXIMUM UNAUTHENTICATED KEY-ASSOCIATED DATA BYTES						
7								(LSB)
8	(MSB)	MAXIMUM AUTHENTICATED KEY-ASSOCIATED DATA BYTES						
9								(LSB)
~~10~~	~~(MSB)~~	~~MAXIMUM NUMBER OF ENCRYPTION KEYS~~						
~~11~~								~~(LSB)~~
~~12~~	~~(MSB)~~	~~MAXIMUM NUMBER OF COMBINED KEYS~~						
~~13~~								~~(LSB)~~
~~12~~	~~(MSB)~~	~~MAXIMUM NUMBER OF DECRYPTION KEYS~~						
~~13~~								~~(LSB)~~
~~14~~	~~(MSB)~~	~~MAXIMUM NUMBER KEYS FOR ALL MODES AND SCOPES~~						
~~15~~								~~(LSB)~~
10	Reserved							
17								
18	ALGORITHM NAME LENGTH (n-19)							
19								
20	ALGORITHM NAME							
N								

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 DATA SECURITY OUT command Set Data Encryption page to select this algorithm.

The ENCRYPT_C field (see table E3) indicates the encryption capabilities of the device.

Table E3 - ENCRYPT_C field values

Value	Description
0	The device server has no data encryption capability using this algorithm.
1	The device server has the ability to encrypt data using this algorithm in software.
2	The device server has the ability to encrypt data using this algorithm in hardware.
3	Reserved

The DECRYPT_C field (see table E4) indicates the decryption capabilities of the device.

Table E4 - DECRYPT_C field values

Value	Description
0	The device server has no data decryption capability using this algorithm.
1	The device server has the ability to decrypt data using this algorithm in software.
2	The device server has the ability to decrypt data using this algorithm in hardware.
3	Reserved

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 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 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 key by reference capable (KBR_C) bit shall be set to one of the device server supports a value in the key FORMAT FIELD of the Set Data Encryption page that indicates key by reference format. The KBR_C bit shall be set to zero of the device server does not support a value in the key FORMAT FIELD of the Set Data Encryption page that indicates key by reference format.

The initialization vector medium unique (IV_MU) field shall be set to one if the initialization vector used by the encryption algorithm is unique for each medium. The initialization vector medium unique (IV_MU) field 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) field 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 initialization vector medium unique (IV_MU) field 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 object unique (IV_EOU) field shall be set to one if the initialization vector used by the encryption algorithm is unique for each encrypted object on the medium. The IV_EOU field shall be set to zero if the initialization vector used by the encryption algorithm is not unique for each encrypted object on the medium.

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

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

~~The MAXIMUM NUMBER OF ENCRYPTION KEYS field indicates the maximum number of write encryption keys that the device server has resources to store at any one time.~~

~~The MAXIMUM NUMBER OF COMBINED KEYS field indicates the maximum number of keys which can be used for both write encryption and read decryption that the device server has resources to store at any one time.~~

~~The MAXIMUM NUMBER OF DECRYPTION KEYS field indicates the maximum number of read decryption keys that the device server has resources to store at any one time.~~

~~The MAXIMUM NUMBER OF KEYS FOR ALL MODES AND SCOPES field indicates the maximum number of keys for either write encryption or read decryption that the device server can save at any one time. This field shall be the total of encryption keys, COMBINED keys and decryption keys that the device server has resources to store.~~

Table E5 describes the values in the NONCE_C field.

Table E5 - NONCE_C field values

Value	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.

The ALGORITHM NAME LENGTH contains the length in bytes of the ALGORITHM NAME field.

The ALGORITHM NAME field contains a null terminated, null padded UTF-8 format string that describes the encryption algorithm. The string shall contain the standardization authority that has registered the algorithm if there is a standard that defines it.

7.X.5 Data encryption status page

Table S1 shows the format of the Data Encryption status page.

Table S1 – Data encryption status page

Bit / Byte	7	6	5	4	3	2	1	0
0	PAGE CODE (11h)							
1	Reserved							
2	(MSB)	PAGE LENGTH (n-3)						
3								(LSB)
4	DECRYPTION MODE				ENCRYPTION MODE			
5	SCOPE			Reserved		SOURCE		
6	KEY GENERATION							
7	ALGORITHM INDEX							
10	(MSB)	NUMBER OF ENCRYPTION KEYS SAVED ~~IN USE~~						
11								(LSB)
12	(MSB)	NUMBER OF COMBINED KEYS SAVED ~~IN USE~~						
13								(LSB)
14	(MSB)	NUMBER OF DECRYPTION KEYS SAVED ~~IN USE~~						
15								(LSB)
16	(MSB)	NUMBER OF KEYS SAVED ~~IN USE~~ FOR ALL MODES AND SCOPES						
17								(LSB)
18	(MSB)	KEY-ASSOCIATED DATA DESCRIPTORS						
N								(LSB)

Table S2 defined the values for the ENCRYPTION MODE field.

Table S2 – ENCRYPTION MODE field values

Value	Name	Description
0h	DISABLE	Data encryption is disabled.
1h	EXTERNAL	The device server has been configured to treat the data associated with WRITE(6) and WRITE(16) commands as if it has been encrypted by a system that is compatible with the algorithm specified by the ALGORITHM INDEX field.
2h	ENCRYPT	The device server has been configured to encrypt all data that it receives for a WRITE(6) or WRITE(16) using the algorithm specified in the ALGORITHM INDEX field.
3h – Fh		Reserved

Table S3 defined the values for the DECRYPTION MODE field.

Table S3 – DECRYPTION MODE field values

Value	Name	Description
0h	DISABLE	Data decryption is disabled. If the device server encounters an encrypted block while reading, it shall not allow access to the block (see 4.2.19.3)
1h	RAW	Data decryption is disabled. If the device server encounters an encrypted block while reading, it shall pass the block and any additional metadata affixed to the block to the host without decrypting it (see 4.2.19.3)
2h	DECRYPT	The device server has been configured to decrypt all data that is read from the medium in response to a READ(6) or READ(16) command or verifying when processing a VERIFY(6) or VERIFY(16) command. The data shall be decrypted using the algorithm specified in the ALGORITHM INDEX field and the key provided in the KEY field. If the device server encounters unencrypted data when processing a READ(6), READ(16), VERIFY(6), or VERIFY(16) command, the device server shall terminate the command with CHECK CONDITION status, with the sense key set to DATA PROTECT, and the additional sense code set to UNENCRYPTED DATA ENCOUNTERED WHILE DECRYPTING. The device server shall leave the medium positioned in front of the unencrypted block.
3h	MIXED	The device server has been configured to decrypt all data that is read from the medium that it determines was encrypted in response to a READ(6) or READ(16) command or verifying when processing a VERIFY(6) or VERIFY(16) command. The data shall be decrypted using the algorithm specified in the ALGORITHM INDEX field and the key provided in the KEY field. If the device server encounters unencrypted data when processing a READ(6), READ(16), VERIFY(6), or VERIFY(16) command, the data shall be processed without decrypting.
4h – Fh		Reserved

The scope field (see table S4) indicates the scope of the data encryption key and mode set by this I_T nexus.

Table S4 - SCOPE field values

Value	Description
0	The data encryption key and mode are default values.
1	The data encryption key and mode are unique to this I_T nexus.
2	The data encryption key and mode set by this I_T nexus are shared with all I_T Nexus that share in a reservation for the logical unit.
3	The data encryption key and mode set by this I_T nexus are shared with all other I_T nexuses.
4 – 7	Reserved

The SOURCE field (see table S5) indicates the source of the encryption key and data encryption mode for this I_T nexus.

Table S5 - SOURCE field values

Value	Description
0	The data encryption key and mode are default values.
1	The data encryption key and mode are unique to this I_T nexus.
2	The data encryption key and mode were established by another I_T nexus and are being shared with other reservation holds.
3	The data encryption key and mode were established by another I_T nexus and are being shared globally.
4- 7	Reserved

The KEY GENERATION field contains the value of the Key Generation counter (see 4.2.19.6) assigned to the key indicated by the SOURCE field value.

The ALGORITHM INDEX field indicates which of the encryption algorithms reported by the DATA SECURITY IN command Data Encryption Capabilities page is selected. If the ENCRYPT and DECRYPT bits are both set to zero, the value in the ALGORITHM INDEX field is undefined.

The NUMBER OF ENCRYPTION KEYS SAVED ~~IN USE~~ field indicates the number of write encryption keys that are currently being supported by the device server for the mode and SCOPE indicated for this page.

The NUMBER OF COMBINED KEYS SAVED ~~IN USE~~ field indicates the number of keys which can be used for both write encryption and read decryption that are currently being supported by the device server for the mode and SCOPE indicated for this page.

The NUMBER OF DECRYTION KEYS SAVED ~~IN USE~~ field indicates the number of read decryption keys that are currently being supported by the device server for the mode and SCOPE indicated for this page.

The NUMBER OF KEYS SAVED ~~IN USE~~ FOR ALL MODES AND SCOPES field indicates the number of keys of any type being stored by the device server. This value shall indicate the number of keys being used for all the modes and SCOPES supported by the device server.

If encryption and decryption are both disabled, the KEY-ASSOCIATED DATA DESCRIPTORS field shall be not be included in the page.

If encryption or decryption is enabled, the KEY-ASSOCIATED DATA DESCRIPTORS field shall contain data security descriptors (see 8.5) describing attributes assigned to the key defined by the SCOPE and SOURCE fields at the time the key was established in the device server by processing a Set Data Encryption page. If more than one key associated descriptor is included, they shall be order of increasing value of the DESCRIPTOR TYPE field. Descriptors shall be included as defined by the following paragraphs.

An unauthenticated key-associated data descriptor (see 8.5.2) shall be included if an unauthenticated key-associated data descriptor was included in the Set Data Encryption page that established the key in the device server. The VALID bit shall be set to one and the AUTH bit shall be set to zero. The KEY DESCRIPTOR field shall contain the U-KAD value associated with the key.

An authenticated key-associated data descriptor (see 8.5.3) shall be included if an authenticated key-associated data descriptor was included in the Set Data Encryption page that established the key in the device server. The VALID bit shall be set to one and the AUTH bit shall be set to one. The KEY DESCRIPTOR field shall contain the A-KAD value associated with the key.

A nonce value descriptor (see 8.5.4) shall be included if a nonce value descriptor was included in the Set Data Encryption page that established the key in the device server. The VALID bit shall be set to one and the AUTH bit shall be set to one. The KEY DESCRIPTOR field shall contain the nonce value associated with the key. A nonce value descriptor may be included if no nonce value descriptor was included in the Set Data Encryption page that established the key in the device server. In this case, the KEY DESCRIPTOR field shall be set to the nonce value established by the device server for use with the selected key.

7.Y.2 Set data encryption page

Table Y1 shows the parameter list format of the set data encryption page.

Table Y1 – Set Data Encryption page

Bit / Byte	7	6	5	4	3	2	1	0
0	PAGE CODE (10h)							
1	Reserved							
2	(MSB)	PAGE LENGTH (m-3)						
3								(LSB)
4	SCOPE			Reserved		LOCK	CKOD	CKORL
5	DECRYPTION MODE				ENCRYPTION MODE			
6	ALGORITHM INDEX							
7	Reserved					KEY USE		KPDK
8	KEY FORMAT							
9	(MSB)	Reserved						
18								(LSB)
19	(MSB)	KEY LENGTH (n-19)						
20								(LSB)
21		KEY						
N								
n+1		KEY-ASSOCIATED DATA DESCRUPTORS						
M								

The page length field indicates the number of bytes of parameter data to follow. If the page length value results in the truncation of any field, the device server shall terminate the command with CHECK CONDITION status, with the sense key set to ILLEGAL REQUEST, and the additional sense code set to INVALID FIELD IN PARAMETER LIST.

The SCOPE field (see table Y2) indicates the scope of the data encryption mode and key.

Table Y2 – SCOPE field values

Value	Name	Description
0	PUBLIC	The data encryption mode and key shall be ignored. The I_T nexus shall use values that are shared by other I_T nexuses. If no I_T nexuses are sharing values, the device server shall use default values.
1	LOCAL	The data encryption mode and key are unique to the I_T nexus associated with the DATA SECURITY OUT command and shall not be shared with other I_T nexuses.
2	RESERVATION GROUP	The data encryption mode and key shall be shared with all participants in a reservation.
3	ALL I_T NEXUS	The data encryption mode and key shall be shared with all I_T nexuses.
4 – 7		Reserved

The data encryption mode and key that shall be used for an I_T nexus shall be established by the following order of precedence:

1. If the scope for the I_T nexus is not PUBLIC, the values set by a DATA SECURITY OUT command associated with the I_T nexus; or
2. If the scope for the I_T nexus is PUBLIC:
    1) If the I_T nexus is participating in a reservation for the logical unit, the values set by another participant in the reservation with a scope of RESERVATION GROUP;
    2) the values set by anther I_T nexus with a scope of ALL I_T NEXUS; or
    3) the default values.

If the clear key on dismount (CKOD) bit is set the device server shall set the encryption key and encryption mode to default values after completing a dismount of a volume. If the CKD bit is set to zero, the dismounting of a volume shall not affect the encryption key or encryption mode. If the CKOD bit is set to one and there is no volume mounted in the device, the device server shall terminate the command with CHECK CONDITION status, with the sense key set to ILLEGAL REQUEST, and the additional sense code set to INVALID FIELD IN PARAMETER DATA.

If the clear key on reservation loss (CKORL) bit is set the device server shall set the encryption key and encryption mode to default values on the loss or change in scope of the reservation. If the CKORL bit is set to zero, the loss of a reservation shall not affect the encryption key or encryption mode. If the CKORL bit is set to one and there is no reservation in affect for the I_T nexus associated with the DATA SECURITY OUT command, the device server shall terminate the command with CHECK CONDITION

status, with the sense key set to ILLEGAL REQUEST, and the additional sense code set to INVALID FIELD IN PARAMETER DATA.

Table Y3 defined the values for the ENCRYPTION MODE field.

Table Y3 – ENCRYPTION MODE field values

Value	Name	Description
0h	DISABLE	Data encryption is disabled.
1h	EXTERNAL	The data associated with WRITE(6) and WRITE(16) commands has been encrypted by a system that is compatible with the algorithm specified by the ALGORITHM INDEX field.
2h	ENCRYPT	The device server shall encrypt all data that it receives for a WRITE(6) or WRITE(16) using the algorithm specified in the ALGORITHM INDEX field and the key provided in the KEY field.
3h – Fh		Reserved

Table Y4 defined the values for the DECRYPTION MODE field.

Table Y4 – DECRYPTION MODE field values

Value	Name	Description
0h	DISABLE	Data decryption is disabled. If the device server encounters an encrypted block while reading, it shall not allow access to the block (see 4.2.19.3)
1h	RAW	Data decryption is disabled. If the device server encounters an encrypted block while reading, it shall pass the block and any additional metadata affixed to the block to the host without decrypting it (see 4.2.19.3)
2h	DECRYPT	The device server shall decrypt all data that is read from the medium in response to a READ(6) or READ(16) command or verifying when processing a VERIFY(6) or VERIFY(16) command. The data shall be decrypted using the algorithm specified in the ALGORITHM INDEX field and the key provided in the KEY field. If the device server encounters unencrypted data when processing a READ(6), READ(16), VERIFY(6), or VERIFY(16) command, the device server shall terminate the command with CHECK CONDITION status, with the sense key set to DATA PROTECT, and the additional sense code set to UNENCRYPTED DATA ENCOUNTERED WHILE DECRYPTING. The device server shall leave the medium positioned in front of the unencrypted block.
3h	MIXED	The device server shall decrypt all data that is read from the medium that it determines was encrypted in response to a READ(6) or READ(16) command or verifying when processing a VERIFY(6) or VERIFY(16) command. The data shall be decrypted using the algorithm specified in the ALGORITHM INDEX field and the key provided in the KEY field. If the device server encounters unencrypted data when processing a READ(6), READ(16), VERIFY(6), or VERIFY(16) command, the data shall be processed without decrypting.
4h – Fh		Reserved

If the ENCRYPTION MODE field is set to ENCRYPT and the key length field is set to zero, the device server shall terminate the command with CHECK CONDITION status, with the sense key set to ILLEGAL REQUEST, and the additional sense code set to INVALID FIELD IN PARAMETER DATA.

If the DECRYPTION MODE field is set to DECRPT or MIXED and the key length field is set to zero, the device server shall terminate the command with CHECK CONDITION status, with the sense key set to ILLEGAL REQUEST, and the additional sense code set to INVALID FIELD IN PARAMETER DATA.

The ALGORITHM INDEX field indicates which of the encryption algorithms reported by the DATA SECURITY IN command Data Encryption Capabilities pages shall be used to encrypt and decrypt data.

Table YX defined the values for the KEY USE field.

Table YX – KEY USE field values

Value	Name	Description
0h	COMBINED	The key being sent in this page may be used for both write encryption and read decryption.
1h	ENCRYPT	The key being sent in this page shall be used only for write encryption. The Decryption Mode field shall be ignored and not saved with the key.
2h	DECRYPT	The key being sent in this page shall be used only for read decryption. The Encryption Mode a LOCK fields shall be ignored and not saved with the key.
3h		Reserved

~~If a key has previously been sent to the device server with the KEY USE field set to ENCRYPT and another key is sent with the KEY USE field set to ENCRYPT with the same mode and SCOPE as the previously sent key, the device server shall remove the previously sent key and replaced it with the new key.~~

~~If a key has previously been sent to the device server with the KEY USE field set to COMBINED and another key is sent with the KEY USE field set to COMBINED with the same mode and SCOPE as the previously sent key, the device server shall remove the previously sent key and replaced it with the new key.~~

If a key has previously been sent to the device server with the KEY USE field set to ENCRYPT or COMBINED and another key is sent with the KEY USE field set to ENCRYPT or COMBINED with the same mode and the same SCOPE for either ALL I_T NEXUS or RESERVSATION GROUP as the previously sent key, the device server shall remove the previously sent key and replaced it with the new key.

If a key has previously been sent to the device server with the KEY USE field set to ENCRYPT or COMBINED and another key is sent with the KEY USE field set to ENCRYPT or COMBINED with the same mode and the SCOPE is LOCAL with the same I_T Nexus as the previously sent key, the device server shall remove the previously sent key and replaced it with the new key.

~~If a key has previously been sent to the device server with the KEY USE field set to COMBINED and another key is sent with the KEY USE field set to COMBINED with~~

~~the same mode and SCOPE as the previously sent key, the device server shall remove the previously sent key and replaced it with the new key.~~

If the keep previous decryption key (KPDK) bit is set and the KEY USE field is set to DECRYPT, the device server shall retain the previously sent decryption keys for this mode and SCOPE.

If the KPDK bit is set to zero and the KEY USE field is set to DECRYPT, all previously sent decryption keys for this mode and SCOPE shall be removed and replaced with the new key.

If the KPDK bit is set to one and the KEY TYPE field is not set to DECRYPT, the device server shall terminate the command with CHECK CONDITION status, with the sense key set to ILLEGAL REQUEST, and the additional sense code set to INVALID FIELD IN PARAMETER DATA.

~~If the number of decryption keys sent to the device server, with the KPDK bit set, exceed the value provided in the MAXIMUM NUMBER OF DECRYPTION KEYS field in the Data encryption algorithm descriptor page,~~ If the device server is processing a Set Data Encryption page with the KPDK bit set to one and has already saved the number of keys specified in the MAXIMUM NUMBER OF DECRYPTION KEYS field in the Data Encryption capabilities page, the device server shall terminate the command with CHECK CONDITION status, with the sense key set to ILLEGAL REQUEST, and the additional sense code set to MAXIMUM NUMBER OF DECRYPTION KEYS EXCEEDED. The previously sent decryption keys shall not be affected by this error.

Editors Note: MAXIMUM NUMBER OF DECRYPTION KEYS EXCEEDED is a new ASC.

~~If the number of decryption keys sent to the device server, with the KPDK bit set, exceed the value provided in the MAXIMUM NUMBER OF KEYS FOR ALL MODES AND SCOPES field in the Data encryption algorithm descriptor page,~~ If the device server is processing a Set Data Encryption page with the KPDK bit set to one and has already saved the number of keys specified in the MAXIMUM NUMBER OF KEYS FOR ALL MODES AND SCOPES field in the Data Encryption capabilities page, the device server shall terminate the command with CHECK CONDITION status, with the sense key set to ILLEGAL REQUEST, and the additional sense code set to MAXIMUM NUMBER OF KEYS FOA ALL MODES AND SCOPES EXCEEDED. The previously sent decryption keys shall not be affected by this error.

Editors Note: MAXIMUM NUMBER OF KEYS FOR ALL MODES AND SCOPES EXCEEDED is a new ASC.

~~It is possible for all the keys that can be supported by the device server to be utilized by other modes and SCOPES. In this case, if a ENCRYPT or COMBINED keys sent to the device server exceeds the value provided in the MAXIMUM NUMBER OF KEYS FOR ALL MODES AND SCOPES field of the Data Encryption capabilities page, the device server shall remove the key that has been held by the device server the longest length of time. A unit attention condition with the additional sense of DATA ENCRYPTION MODE CHANGED BY ANOTHER INITIATOR shall be establish for any other I_T nexus that is affected by the change of the key.~~