January 28, 2006 06-051r3 The Requirement for More than One Decryption Key

To: T10 Technical Committee
From: Dwayne Edling (dwayne.edling@sun.com)
Date: 28 Jan 2006
Subject: T10/06-051r3 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.
Revision 2 (28 Jan 2006): Remove encryption key to simplify proposal.

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.

Revision 3

Change format to use only supplemental decryption key (SDK).

Removed

- MAXIMUM NUMBER OF ENCRYPTION KEYS
- MAXIMUM NUMBER OF COMBINED KEYS (Used for both encryption and decryption)
- MAXIMUM NUMBER OF KEYS FOR ALL MODES AND SCOPES

Removed

- NUMBER OF ENCRYPTION KEYS IN USE
- NUMBER OF COMBINED KEYS IN USE
- NUMBER OF KEYS IN USE FOR ALL MODES AND SCOPES

Removed KEY TYPE and KPDK

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 reason, the data encryption key and mode are volatile in the device server and the data encryption keys are never reported to an application client. 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 values for the I_T nexus associated with the SECURITY PROTOCOL OUT command and shall clear all 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 all other I_T nexus that are affected by the loss of the keys, (i.e., any I_T nexus that is using a scope of PUBLIC and sharing the keys.)

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 a key and the SDK bit is set to zero, the device server shall release any resources that it had allocated to store ~~a~~ key values set by a previous SECURITY PROTOCOL OUT command from that I_T nexus and shall clear all 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 all 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 keys).

A device server shall save at most one key that will be used for both encryption and decryption and the MAXIMUM NUMBER OF DECRYPTION KEYS reported in the Data Encryption Capabilities page 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 and the SDK bit is set to zero, the device server shall release any resources that it had allocated to store ~~a~~ key values set by a previous Set Data Encryption page 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 (i.e. any I_T nexus that is using a scope of public and sharing the keys.)

A device server shall save at most one key that will be used for both encryption and decryption and the MAXIMUM NUMBER OF DECRYPTION KEYS reported in the Data Encryption Capabilities page with a scope of RESERVATION GROUP. If a device server processes a Set Data Encryption page with the SCOPE field set to RESERVATION GROUP and the SDK bit is set to zero, the device server shall release any resources that it had allocated to store ~~a~~ key values set by a previous Set Data Encryption page 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 established 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 keys.

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

Editor's note: DATA ENCRYPTION MODE CHANGED BY VENDOR SPECIFIC EVENT is a new ASC.

Editor's note: Do we want to make support for any particular scope settings mandatory?

If the device server supports an encryption key scope of ALL I_T NEXES, it shall save the following information for ~~one encryption~~ one set of key(s) with this scope:

a) For SCSI transport protocols where initiator port names are required, the initiator port name; otherwise, the initiator port identifier;
b) encryption mode;
c) decryption mode;
d) one key that is used for both encryption and decryption;

e) a list of the decryption keys, if supported;
f) algorithm index;
g) key generation;
h) CKOD;
i) U-KAD;
j) A-KAD; and
k) nonce.

If the device server supports an encryption key scope of RESERVATION GROUP, it shall save the following information ~~for one encryption~~ one set of key(s) with this scope:

a) For SCSI transport protocols where initiator port names are required, the initiator port name; otherwise, the initiator port identifier;
b) encryption mode;
c) decryption mode;
l) one key that is used for both encryption and decryption;
d) a list of the decryption keys, if supported;
e) algorithm index;
f) Key Generation;
g) CKOD;
h) CKORL;
i) U-KAD;
j) A-KAD; and
k) nonce.

If the device server supports an encryption key scope of LOCAL, it shall save the following information for one or more ~~encryption~~ set of key(s) with this scope:

a) For SCSI transport protocols where initiator port names are required, the initiator port name; otherwise, the initiator port identifier;
b) encryption mode;
c) decryption mode;
m) one key that is used for both encryption and decryption;
d) a list of the decryption keys if supported;
e) algorithm index;
f) Key Generation;
g) CKOD;
h) U-KAD;
i) A-KAD; and
j) nonce.

If the device server supports data encryption it shall save the following information on a per I_T nexus basis:

a) scope;
b) lock;
c) Key Generation value at lock; and
d) local Key Generation value;

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	(MSB)			PAGE CODE (0010h)				
1								(LSB)
2	(MSB)			PAGE LENGTH (n-3)				
3								(LSB)
4	(MSB)			MAXIMUM NUMBER OF DECRYPTION KEYS				
5								(LSB)
	Encryption algorithm descriptors							
6	(MSB)			Data encryption algorithm descriptor				
								(LSB)
	:							
	(MSB)			Data encryption algorithm descriptor				
N								(LSB)

See SPC-4 for a description of the PAGE LENGTH field.

The MAXIMUM NUMBER OF DECRYPTION KEYS field indicates the maximum number of keys that shall be used for decryption only that the device server has resources to store at any one time. The value in this field only applies to keys that are sent to the device server with the SDK bit set to one in the Set Data Encryption page. If the MAXIMUM NUMBER OF DECRYPTION KEYS field value is zero then the SDK field shall be set to zero in the Set Data Encryption page.

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.

8.5.2.5 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	(MSB)			PAGE CODE (0011h)				
1								(LSB)
2	(MSB)			PAGE LENGTH (n-3)				
3								(LSB)
4	SCOPE			Reserved		SOURCE		
5	DECRYPTION MODE				ENCRYPTION MODE			
6	ALGORITHM INDEX							
7	KEY GENERATION							
8	(MSB)			NUMBER OF DECRYPTION KEYS SAVED				
9								(LSB)
10	(MSB)			KEY-ASSOCIATED DATA DESCRIPTORS LIST				
N								(LSB)

The ALGORITHM INDEX field indicates which of the encryption algorithms reported by the SECURITY PROTOCOL 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 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 NUMBER OF DECRYPTION KEYS SAVED field indicates the number of keys that shall be used for decryption only that are currently being supported by the device server for this source. The value in this field only applies to keys that are sent to the device server with the SDK bit sent to one in the Set Data Encryption page.

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

If encryption or decryption is enabled, the KEY-ASSOCIATED DATA DESCRIPTORS LIST 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 8.5.4.3) 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 AUTHENTICATED field 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 8.5.4.4) 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 AUTHENTICATED field shall be set to zero. The KEY DESCRIPTOR field shall contain the A-KAD value associated with the key.

8.5.3.2 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	(MSB)			PAGE CODE (0010h)				
1								(LSB)
2	(MSB)			PAGE LENGTH (m-3)				
3								(LSB)
4	SCOPE			Reserved	SDK	LOCK	CKOD	CKORL
5	DECRYPTION MODE				ENCRYPTION MODE			
6	ALGORITHM INDEX							
7	KEY FORMAT							
8	(MSB)			Reserved				
17								(LSB)
18	(MSB)			KEY LENGTH (n-19)				
19								(LSB)
20				KEY				
N								
n+1				KEY-ASSOCIATED DATA DESCRIPTORS LIST				
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 SECURITY PROTOCOL 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 SECURITY PROTOCOL 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 another I_T nexus with a scope of ALL I_T NEXUS; or
    3) the default values.

Editor's note: the above precedence list assumes that the default scope value for each I_T nexus is PUBLIC. If this is not true, a second choice is required in entry 1 to select the default settings.

If the supplemental decryption key (SDK) bit is set to one, the key sent in this page shall be added to the list of keys used for decryption by the device server for the selected scope. The ECRYPTION MODE and LOCK fields shall be ignored and the DECRYPTION MODE shall match the current setting for this scope. If the DECRYPTION MODE does not match the current settings for this scope 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. If the scope is ALL_I_T_NEXUS or RESERVATION GROUP and an encryption or decryption key has been saved with that scope the page must have the same I_T nexus as the previously saved key. If the I_T nexus does not match, 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.

If the SDK bit is set to one and the MAXIMUM NUMBER OF DECRYPTION KEYS field in the Data Encryption capabilities page is 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 LIST.

If the device server is processing a Set Data Encryption page with the SDK 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 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 CKOD 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 SECURITY PROTOCOL 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.