the Inventory Marker field set to the value received in the previous Inventory-Response. This indicates to the target that it should start with the key in the 79th position rather than the key in the 1st position. When the target sends an Inventory-Response containing the remainder of the keys, it shall set the Inventory Marker to zero. In this way, the KFD can retrieve all key info blocks stored in the target without exceeding the maximum size of a KMM.

3.9.2.12 Inventory-Response (List Active Keys)

Octet 0	Inventory Type	
1 - 3	Inventory Marker	
4 - 5	Number of Items	Number of Items = x
6	Keyset ID	SEQUENCE [1..x] of
7 - 8	SLN	Key Info Items
9	Algorithm ID	
10 - 11	Key ID	
12	Subsequent Key Info Items	

Table 4. Inventory-Response (List Active Keys) Message Format

Inventory Marker – See section 3.9.2.11 for a description of how this field is used. Set to 0 to indicate no additional keys. Set to an arbitrary value marking the position of the next key if all keys were not sent in the Inventory-Response.

3.9.2.13 Inventory-Command (List MNP)

Octet 0	Inventory Type

Table 5. Inventory-Command (List MNP) Message Format

3.9.2.14 Inventory-Response (List MNP)

Octet 0	Inventory Type
1 - 2	Message Number Period

Table 6. Inventory-Response (List MNP) Message Format

3.9.2.15 Inventory-Command (List KMF RSI)

Octet 0	Inventory Type

Table 7. Inventory-Command (List KMF RSI) Message Format

3.9.2.16 Inventory-Response (List KMF RSI)

Octet 0	Inventory Type
1 - 3	KMF RSI

Table 8. Inventory-Response (List KMF RSI) Message Format

3.9.2.17 Modify-Key-Command

The Modify-Key-Command used on the KFD Interface Protocol has been modified to add one additional octet. The fields shown in Table 11 are defined in Reference [1] except for the Extended Decryption Instruction Format octet and the Key field when the key is sent unencrypted.

Extended Decryption Instruction octet
The Extended Decryption Instruction Format octet is defined as follows:

	7	6	5	4	3	2	1	0
Octet 1	0	0	0	0	0	0	0	0

The most significant bit (b7) is unavailable and shall be set to zero. The other bits (b6 – b0) are reserved and should be set to zero. The reserved bits may be defined in the future.

Key field (unencrypted key transfer)
The key transmitted in the Modify Key Command is typically sent unencrypted. If the key is to be encrypted, it shall be done in accordance with Reference [1].

For DES, as described in Reference [1], the plaintext key bits shall be placed in the Key field as follows:

Octet 0	Key Bits $B_1..B_7, P_1$
1	Key Bits $B_8..B_{14}, P_2$
2	Key Bits $B_{15}..P_{21}, P_3$
3	Key Bits $B_{22}..B_{28}, P_4$
4	Key Bits $B_{29}..B_{35}, P_5$
5	Key Bits $B_{36}..B_{42}, P_6$
6	Key Bits $B_{43}..B_{49}, P_7$
7	Key Bits $B_{50}..B_{56}, P_8$

7 6 5 4 3 2 1 0

Key Field Format

Octet 0 - This octet contains the left most (most significant) 7-bits of the plaintext key and the first parity bit. The left most (most significant) key bit, B_1, is placed in the left most (most significant) position of the octet and the parity bit is placed in the right most (least significant) position of the octet.

Octet 1 - This octet contains the next 7 bits of the plaintext key and the second parity bit.

…

Octet 7 - This octet contains the last (least significant) 7 bits of the plaintext key and the last parity bit.

Table 9. DES Key Format

For algorithms that use block encryption protocol (TDES and AES), as described in Reference [1], the plaintext key shall be transmitted without the check vector. The plaintext key bits shall be placed in the Key field as follows:

Octet 0	Key bits $b_1..b_8$							
1	Key bits $b_9..b_{16}$							
k/8-1	Key bits $b_{(k/8*8)+1}..b_k$							
	7	6	5	4	3	2	1	0

Key Field Format

Octet 0 - This octet contains the left most (most significant) 8 bits of the plaintext key. The left most (most significant) key bit, b_1, is placed in the left most (most significant) position of the octet.

Octet 1 - This octet contains the next 8 bits of the plaintext key.

…

Octet k/8-1 - This octet contains the remaining bits of the plaintext key. If the remaining key bits do not fill the octet, the key bits shall be left justified and the remaining unused bits shall be filled with zeros.

Table 10. Block Encryption Protocol Key Field Format

Octet 0	7 6 5 4 3 2 1 0	Decryption Instruction Format	Decryption Instruction Block
1		Extended Decryption Instr Fmt	
2		Algorithm ID	
3		Key ID	
4			
5		Update Count (Optional) [0..1]	
5 or 6		Message Indicator (Optional) [0 or 9 octets]	
(i = 0,1,9,10) i+3			End of Block
i+4		Keyset ID	
i+5		Algorithm ID	
i+6		Key Length	
i+7		Number of Keys	Number of Keys = x
i+8		Key Format	SEQUENCE [1..x] of
i+9		Storage Location Number	Unique Key Items
i+10			
i+11		Key ID	
i+12			
i+13		Key [Key Length octets]	
i+13+Key Length			
i+14+Key Length		Checksum (Optional) [0 or 4 octets]	
		Key Name (Optional) [0..31 octets]	
variable		Subsequent Unique Key Items (if they exist)	

Table 11. Modify-Key-Command Message Format

3.9.2.18 Negative-Acknowledgment

See Reference [1].

3.9.2.19 Rekey-Acknowledgment

See Reference [1].

3.9.2.20 Zeroize-Command

See Reference [1].

3.9.2.21 Zeroize-Response

See Reference [1].

3.9.2.22 Load-Config-Command

Octet	
0 - 2	KMF RSI
3 - 4	Message Number Period

Table 12. Load-Config-Command Message Format

3.9.2.23 Load-Config-Response

Octet	
0 - 2	KMF RSI
3 - 4	Message Number Period
5	Status

Table 13. Load-Config-Response Message Format

Status – A value of 0 means KMF RSI and MNP were accepted. A value of 1 means the Command Was Not Performed.

3.9.2.24 Unable to Decrypt Response

See Reference [1]. When the Unable to Decrypt Response KMM is used on the Key Fill Interface, it shall not be outer-layer encrypted. Furthermore, the following optional blocks shall not be used: Decryption Instruction, Reverse Warm Start and Unique Key Item.

3.9.2.25 Load Authentication Key – Command

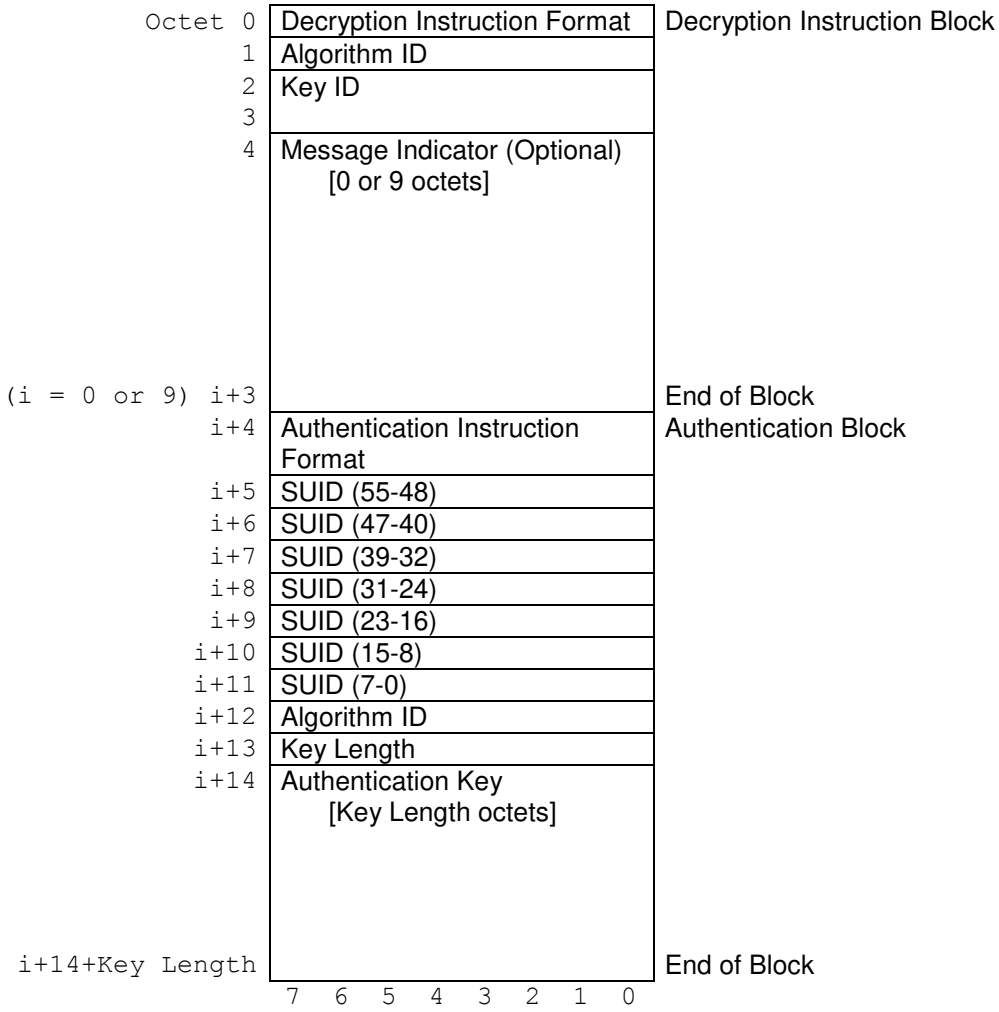

Table 14. Load Authentication Key-Command Message Format

Decryption Instruction Block

Decryption Instruction Format - Indicates which optional fields are included in the Decryption Instructions Block field. The format for this field is defined in the Primitive Field Definition section for Decryption Instruction Format.

Algorithm ID - The Algorithm ID is used in conjunction with the Key ID to uniquely select a KEK. The format for this field is defined in the Primitive Field Definition section for Algorithm ID. Algorithm ID = $80 Unencrypted value.

Key ID - The Key ID of the KEK. – when used. The format for this field is defined in the Primitive Field Definition section for Key ID.

Message Indicator (Optional) - Provides the Message Indicator (encryption synchronization) for encryption algorithms which do not support the Electronic Codebook mode of operation. The format for this field is defined in the Primitive Field Definition section for Message Indicator.

Authentication Instruction Format

B0 = SUID null or defined
A value of 0 indicates the Active SUID is targeted by the command; a value of 1 indicates the SUID specified by the SUID field is targeted by the command.B1 = Is unused and set to zero
B2 = Is unused and set to zero
B3 = Is unused and set to zero
B4 = Is unused and set to zero
B5 = Is unused and set to zero
B6 = Is unused and set to zero
B7 = Is unused and set to zero

Algorithm ID – The Algorithm ID indentifies the algorithm used with the Authentication Key. The format for this field is defined in the Primitive Field Definition section for Algorithm ID. Algorithm ID = $85 AES-128

Key Length - The number of octets used to transfer the key. The format for this field is defined in the Primitive Field Definitions section for Number.

SUID (55-48) – If assigned = WACN ID (19-12)
SUID (47-40) – If assigned = WACN ID (11-4)
SUID (39-36) – If assigned = WACN ID (3-0)
SUID (35-32) – If assigned = System ID (11-8)
SUID (31-24) – If assigned = System ID (7-0)
SUID (23-16) – If assigned = Subscriber ID (23-16)
SUID (15-8) – If assigned = Subscriber ID (15-8)
SUID (7-0) – If assigned = Subscriber ID (7-0)

If the SUID is not specified, then the SUID fields are 0.

The authentication key is made immediately active once it is successfully received by the MR in the Load Authentication Key-Command message. There is no changeover procedure for authentication keys.

For the AES algorithm the plaintext key bits shall be placed in the Key field as follows:

Octet 0	Key bits $b_1..b_8$
1	Key bits $b_9..b_{16}$
k/8-1	Key bits $b_{(k/8*8)+1}..b_k$

7 6 5 4 3 2 1 0

Table 15. Key Field Format

Key Field Format

Octet 0 - This octet contains the left most (most significant) 8 bits of the plaintext key. The left most (most significant) key bit, b_1, is placed in the left most (most significant) position of the octet.

Octet 1 - This octet contains the next 8 bits of the plaintext key.

…

Octet k/8-1 - This octet contains the remaining bits of the plaintext key

3.9.2.26 Load Authentication key – Response

Octet	Authentication Instruction Format
1	SUID (55-48)
2	SUID (47-40)
3	SUID (39-32)
4	SUID (31-24)
5	SUID (23-16)
6	SUID (15-8)
7	SUID (7-0)
8	Status
	7 6 5 4 3 2 1 0

Table 16. Load Authentication Key-Response Message Format

Authentication Instruction Format

B0 = failed/successful SUID assignment to authentication key, (K) A value of 0 indicates failed assignment of SUID to K. A value of 1 indicates successful assignment of SUID to K.

B1 = Is unused and set to zero
B2 = Is unused and set to zero
B3 = Is unused and set to zero
B4 = Is unused and set to zero
B5 = Is unused and set to zero
B6 = Is unused and set to zero
B7 = Is unused and set to zero

SUID (55-48) – WACN ID (19-12)
SUID (47-40) – WACN ID (11-4)
SUID (39-36) – WACN ID (3-0)
SUID (35-32) – System ID (11-8)
SUID (31-24) – System ID (7-0)
SUID (23-16) – Subscriber ID (23-16)
SUID (15-8) – Subscriber ID (15-8)
SUID (7-0) – Subscriber ID (7-0)

If the SUID is not assigned, then the SUID fields are 0. The Status field reflects the error status; the SUID is not always zeroed for all errors.

Status

Status field values are defined in Reference [1] and shown in Table 17

Error precedence, from highest 1) to lowest 4)

1) $0E Invalid WACN or System ID
2) $0F Invalid Subscriber ID
3) Any of
   $05 Out of memory
   $09 Invalid Algorithm ID
   $0B Module Failure
4) $01 Command could not be performed (unspecified reason)

Note that any error status found in Table 17 that is not mentioned above is not relevant to the key fill operation for Link Layer Authentication.

Status	**Reason**	**Value (Hex)**	**Values (Binary)**
Command was performed	Entire command was successfully performed	$00	0000 0000
Command could not be performed (unspecified reason)	Command could not be performed due to a reason other than specified in the Status field	$01	0000 0001
Item (Key/Keyset) does not exist	Key / Keyset to perform operation on does not exist	$02	0000 0010
Invalid Message ID	Message ID is invalid	$03	0000 0011
Invalid Checksum / MAC	MAC or Checksum is invalid	$04	0000 0100
Out of Memory	Memory unavailable to process the command / message	$05	0000 0101
Could not decrypt the message (KEK did not exist)	KEK did not exist to decrypt the message	$06	0000 0110
Invalid Message Number	Message Number is invalid	$07	0000 0111
Invalid Key ID	Key ID is not present	$08	0000 1000
Invalid Algorithm ID	Algorithm ID is not valid or present	$09	0000 1001
Invalid MFID	MFID is not valid	$0A	0000 1010
Module Failure	Encryption Hardware failure	$0B	0000 1011
MI all zeros	Received MI was all zeros	$0C	0000 1100
Keyfail	Key identified by ALGID/KEYID is erased	$0D	0000 1101
Invalid WACN or System ID	WACN ID or System ID not present	$0E	0000 1110
Invalid Subscriber ID	Subscriber ID not valid or present	$0F	0000 1111
Reserved for Future Use	Reserved	$10 - $FE	0001 0000 – 1111 1110
Unknown	Unknown	$FF	1111 1111

Table 17. Status Field Values

3.9.2.27 Delete Authentication Key – Command

Octet	7 6 5 4 3 2 1 0
0	Authentication Instruction Format
1	SUID (55-48)
2	SUID (47-40)
3	SUID (39-32)
4	SUID (31-24)
5	SUID (23-16)
6	SUID (15-8)
7	SUID (7-0)

Table 18. Delete Authentication Key-Command Message Format

Authentication Instruction Format

B0 = SUID unassigned/assigned to an authentication key, (K) A value of 0 indicates the active SUID is targeted by the command; a value of 1 indicates the SUID specified by the SUID field is targeted by the command.
B1 = Erase all or currently active
Valid if B0 = 0, A value of 1 for B1 indicates to erase all authentication keys. A value of 0 indicates to erase the currently active SUID's authentication key.
If B0 = 1, then B1 is unused and set to zero.
B2 = Is unused and set to zero
B3 = Is unused and set to zero
B4 = Is unused and set to zero
B5 = Is unused and set to zero
B6 = Is unused and set to zero
B7 = Is unused and set to zero

SUID (55-48) – WACN ID (19-12)
SUID (47-40) – WACN ID (11-4)
SUID (39-36) – WACN ID (3-0)
SUID (35-32) – System ID (11-8)
SUID (31-24) – System ID (7-0)
SUID (23-16) – Subscriber ID (23-16)
SUID (15-8) – Subscriber ID (15-8)
SUID (7-0) – Subscriber ID (7-0)

If the SUID is not assigned, then the SUID fields are 0.

3.9.2.28 Delete Authentication Key-Response

Octet	7 6 5 4 3 2 1 0
0	SUID (55-48)
1	SUID (47-40)
2	SUID (39-32)
3	SUID (31-24)
4	SUID (23-16)
5	SUID (15-8)
6	SUID (7-0)
7	Number of Keys Deleted
8	
9	Status

Table 19. Delete Authentication Key-Response Message Format

SUID (55-48) – WACN ID (19-12)
SUID (47-40) – WACN ID (11-4)
SUID (39-36) – WACN ID (3-0)
SUID (35-32) – System ID (11-8)
SUID (31-24) – System ID (7-0)
SUID (23-16) – Subscriber ID (23-16)
SUID (15-8) – Subscriber ID (15-8)
SUID (7-0) – Subscriber ID (7-0)

The Active SUID is the one that the MR uses in its current operating mode when transacting trunking services with the RFSS, and with other MRs. For erase all authentication keys the currently active SUID is specified. For erase all or currently active, if there was no currently active SUID, then SUID fields are 0. The specified SUID is located in the SUID fields.

Number of Keys Deleted

0 = No keys deleted.
1- 65535 = Number of keys deleted

If a SUID does not have a key it is not counted. Erase all authentication keys, status command was performed and no keys deleted indicates all SUID in the MR did not have keys before the Delete Key Command was received.

Status

Status field values are defined in Reference [1] and shown in Table 17. If the SUID(s) did not have a key before the command was received the Status value will be $01 Command could not be performed. If delete currently active and there is no active SUID then status indicates an invalid SUID by stating $0E Invalid WACN or System ID.

Error precedence, from highest 1) to lowest 4)

1) $0E Invalid WACN or System ID
2) $0F Invalid Subscriber ID
3) $0B Module Failure
4) $01 Command could not be performed (unspecified reason)