On success, both devices have an unverified, dynamically negotiated link key. It is EXPECTED that the initiator will start the verification process with APSME-VERIFY-KEY.request after the responder completes the APSME-KEY-NEGOTIATE.confirm.

On failure, both devices SHALL discard any generated material and SHALL ensure that the respective APS Key Pair Table entries are identical what they were prior to initiation of Key Negotiation, as described in section 4.4.10.

4.4.10 Secured APDU Frame

The APS layer frame format consists of APS header and APS payload fields (see Figure 4-7). The APS header consists of frame control and addressing fields. When security is applied to an APDU frame, the security bit in the APS frame control field SHALL be set to 1 to indicate the presence of the auxiliary frame header. The format for the auxiliary frame header is given in section 4.5.1. The format of a secured APS layer frame is shown in Figure 4-7. The auxiliary frame header is situated between the APS header and payload fields.

Octets: Variable	**5 or 13**	**Variable**	
Original APS header ([B6], Clause 7.1)	Auxiliary frame header	Encrypted payload	Encrypted message integrity code (MIC)
		Secure frame payload = output of CCM	
Full APS header		Secured APS payload	

Figure 4-7. Secured APS Layer Frame Format

4.4.11 Command Frames

The APS layer command frame formats are given in this section.

All APS command frames SHALL set their APS frame control field as follows:

1. Set the frame type sub-field to 0x01 (Command)
2. Set the delivery-mode sub-field to 0x00 (Unicast) or 0x10 (broadcast)
3. Set the ACK format bit to 0.
4. Set the ACK request bit to 0 for APS Command Frames sent inside Tunnel Data frames from the Trust Center to a prospective joiner. A device MAY, but is not required to, set the ACK request bit to 1 for the Relay Message Upstream and Relay Message Downstream commands. A device SHALL set the ACK request bit to 1 for all other unicast APS command frames as well as command frames within the Relay Message Upstream and Relay Message Downstream commands.
5. Set the extended nonce sub field to 1 if APS security was applied. Otherwise, set it to 0.[9]
6. Set the security bit according to section 4.4.1.3 Security Processing of APS Commands.

Command identifier values are shown in Table 4-31.

[9] CCB 2432

Table 4-31. Command Identifier Values

Command Identifier	Value
Reserved	0x01
Reserved	0x02
Reserved	0x03
Reserved	0x04
APS_CMD_TRANSPORT_KEY	0x05
APS_CMD_UPDATE_DEVICE	0x06
APS_CMD_REMOVE_DEVICE	0x07
APS_CMD_REQUEST_KEY	0x08
APS_CMD_SWITCH_KEY	0x09
Reserved	0x0A
Reserved	0x0B
Reserved	0x0C
Reserved	0x0D
APS_CMD_TUNNEL	0x0E
APS_CMD_VERIFY_KEY	0x0F
APS_CMD_CONFIRM_KEY	0x10
APS_CMD_RELAY_MESSAGE_DOWNSTREAM	0x11
APS_CMD_RELAY_MESSAGE_UPSTREAM	0x12

4.4.11.1 Transport-Key Commands

The transport-key command frame shall be formatted as illustrated in Figure 4-8. The optional fields of the APS header portion of the general APS frame format SHALL NOT be present.

Octets: 1	**1**	**1**	**1**	**Variable**
Frame control	APS counter	APS command identifier	StandardKeyType	Key descriptor
APS header		Payload		

Figure 4-8. Transport-Key Command Frame

4.4.11.1.1 Command Identifier Field

The command identifier field SHALL indicate the transport-key APS command type (APS_CMD_TRANSPORT_KEY, see Table 4-31).

4.4.11.1.2 StandardKeyType Field

This field is 8 -bits in length and describes the type of key being transported. The different types of keys are enumerated in Table 4-9.

4.4.11.1.3 Key Descriptor Field

This field is variable in length and SHALL contain the actual (unprotected) value of the transported key along with any relevant identification and usage parameters. The information in this field depends on the type of key being transported (as indicated by the StandardKeyType field — see Table 4-9) and shall be set to one of the formats described in the following subsections.

4.4.11.1.3.1 Trust Center Link Key Descriptor Field

If the key type field is set to 4, the key descriptor field SHALL be formatted as shown in Figure 4-9.

Octets: 16	**8**	**8**	**Varies**
Key	Destination address	Source address	TLVs

Figure 4-9. Trust Center Link Key Descriptor Field in Transport-Key Command

The key sub-field SHALL contain the link key that SHOULD be used for APS encryption.

The destination address sub-field SHALL contain the address of the device which SHOULD use this link key.

The source address sub-field SHALL contain the address of the Trust Center that sent the link key.

The TLVs sub-field is optional. If present, it contains one or more TLVs as described in the section 4.4.11.1.4.

4.4.11.1.3.2 Network Key Descriptor Field

If the key type field is set to 1 this field SHALL be formatted as shown in Figure 4-10.

Octets: 16	**1**	**8**	**8**
Key	Sequence number	Destination address	Source address

Figure 4-10. Network Key Descriptor Field in Transport-Key Command

The key sub-field SHALL contain a network key.

The sequence number sub-field SHALL contain the sequence number associated with this network key.

The destination address sub-field SHALL contain the address of the device which SHOULD use this network key.

If the network key is sent to a broadcast address, the destination address subfield SHALL be set to the all-zero string and SHALL be ignored upon reception.

The source address sub-field SHALL contain the address of the device (for example, the Trust Center) which originally sent this network key.

The source address field SHALL contain 0xFFFFFFFFFFFFFFFF in a distributed security network. This indicates to the receiving device this is a distributed security network with no Trust Center.

4.4.11.1.3.3 Application Link Key Descriptor Field

If the key type field is set to 2 or 3, this field SHALL be formatted as shown in Figure 4-11.

Octets: 16	**8**	**1**	**Varies**
Key	Partner address	Initiator flag	TLVs

Figure 4-11. Application Link Key Descriptor in Transport-Key Command

The key sub-field SHALL contain a link key that is shared with the device identified in the partner address sub-field.

The partner address sub-field SHALL contain the address of the other device that was sent this link key.

The initiator flag sub-field SHALL be set to 1 if the device receiving this packet requested this key. Otherwise, this sub-field SHALL be set to 0.

The TLVs sub-field is optional. If present, it contains one or more TLVs as described in the section 4.4.11.1.4.

4.4.11.1.4 TLVs

4.4.11.1.4.1 Local TLVs

This local TLV (tag ID 0x00) indicates link-key features and the peer device's link-key capabilities as shown in Figure 4-12.

Octets
Features

Figure 4-12. Format of the Link-Key Features & Capabilities TLV

The fields of the Link-Key Features & Capabilities TLV are described in Table 4-32.

Table 4-32. Fields of the Link-Key Features & Capabilities TLV

Name	Type	Valid Range	Description
Features	map8	0x00 – 0xFF	This contains the key features bitmap as specified in Table 4-36.

4.4.11.2 Update Device Commands

The APS command frame used for device updates is specified in this section. The optional fields of the APS header portion of the general APS frame format SHALL NOT be present.

The update-device command frame SHALL be formatted as illustrated in Figure 4-13.

Octets: 1	1	1	8	2	1	Varies
Frame control	APS counter	APS command identifier	Device Address	Device short address	Status	JoinerTLVs
APS Header		Payload				

Figure 4-13. Update-Device Command Frame Format

4.4.11.2.1 Command Identifier Field

The command identifier field SHALL indicate the update-device APS command type (APS_CMD_UPDATE_DEVICE, see Table 4-31).

4.4.11.2.2 Device Address Field

The device address field SHALL be the 64-bit extended address of the device whose status is being updated.

4.4.11.2.3 Device Short Address Field

The device short address field SHALL be the 16-bit network address of the device whose status is being updated.

4.4.11.2.4 Status Field

The status field SHALL be assigned a value as described for the Status parameter in Table 4-14.

4.4.11.2.5 JoinerTLVs Field

The JoinerTLVs field MAY or MAY NOT be present. This field will be one or more TLVs received during Network Commissioning by the parent router. If the joining device or parent router has implemented a version prior to R23 then the fields will not be present. Only if both joiner and router support Revision 23 or later will the Joiner TLVs field be present.

4.4.11.3 Remove Device Commands

The APS command frame used for removing a device is specified in this section. The optional fields of the APS header portion of the general APS frame format SHALL NOT be present. The remove-device command frame shall be formatted as illustrated in Figure 4-14.

Octets: 1	**1**	**1**	**8**
Frame control	APS counter	APS command identifier	Target address
APS Header		Payload	

Figure 4-14. Remove-Device Command Frame Format

4.4.11.3.1 Command Identifier Field

The command identifier field SHALL indicate the remove-device APS command type (APS_CMD_REMOVE_DEVICE, see Table 4-31).

4.4.11.3.2 Target Address Field

The target address field SHALL be the 64-bit extended address of the device that is requested to be removed from the network.

4.4.11.4 Request-Key Commands

The APS command frame used by a device for requesting a key is specified in this section. The optional fields of the APS header portion of the general APS frame format SHALL NOT be present.

The request-key command frame SHALL be formatted as illustrated in Figure 4-15.

Octets: 1	**1**	**1**	**1**	**0/8**
Frame control	APS counter	APS command identifier	RequestKeyType	Partner address
APS Header		Payload		

Figure 4-15. Request-Key Command Frame Format

4.4.11.4.1 Command Identifier Field

The command identifier field SHALL indicate the request-key APS command type (APS_CMD_REQUEST_KEY, see).

4.4.11.4.2 RequestKeyType Field

The key type field SHALL be set to the key being requested. Note this Key Type is different than the StandardKeyType values used in Table 4-9 for other APS Commands or other APSME primitives. The RequestKeyType field values for the APS Command Request Key are defined in Table 4-19.

4.4.11.4.3 Partner Address Field

When the RequestKeyType field is 2 (that is, an application key), the partner address field SHALL contain the extended 64-bit address of the partner device that SHALL be sent the key. Both the partner device and the device originating the request-key command will be sent the key.

When the RequestKeyType field is 4 (that is, a trust center link key), the partner address field will not be present.

4.4.11.5 Switch-Key Commands

The APS command frame used by a device for switching a key is specified in this section. The optional fields of the APS header portion of the general APS frame format SHALL NOT be present.

The switch-key command frame SHALL be formatted as illustrated in Figure 4-16.

Octets: 1	**1**	**1**	**1**
Frame control	APS counter	APS command identifier	Sequence number
APS Header		Payload	

Figure 4-16. Switch-key Command Frame Format

4.4.11.5.1 Command Identifier Field

The command identifier field SHALL indicate the switch-key APS command type (APS_CMD_SWITCH_KEY, see Table 4-31).

4.4.11.5.2 Sequence Number Field

The sequence number field SHALL contain the sequence number identifying the network key to be made active.

4.4.11.6 Tunnel Command

The APS command frame used by a device for sending a command to a device that lacks the current network key is specified in this section. The optional fields of the APS header portion of the general APS frame format SHALL NOT be present. The tunnel-key command frame is sent unsecured.

The tunnel-key command frame SHALL be formatted as illustrated in Figure 4-17.

Octets:1	**1**	**1**	**8**	**2**	**13**	**Variable**	**4**
Frame control	APS counter	APS command identifier	Destination address	Tunneled APS header	Tunneled auxiliary frame	Tunneled command	Tunneled APS MIC
APS Header		Payload					

Figure 4-17. Tunnel Command Frame Format

4.4.11.6.1 Command Identifier Field

The command identifier field SHALL indicate the tunnel APS command type (APS_CMD_TUNNEL, see Table 4-31).

4.4.11.6.2 Destination Address

The destination address field SHALL be the 64-bit extended address of the device that is to receive the tunneled command.

4.4.11.6.3 Tunneled Auxiliary Frame Field

The tunneled auxiliary frame field shall be the auxiliary frame (see section 4.5.1) used to encrypt the tunneled command. The auxiliary frame SHALL indicate that a link key was used and SHALL include the extended nonce field.

4.4.11.6.4 Tunneled Command Field

The tunneled command field SHALL be the APS command frame to be sent to the destination.

4.4.11.7 Verify-Key Command

This APS command is used by a joining device to verify its updated link key with the peer device, such as the Trust Center.

The Verify-Key Command frame is formatted as illustrated in Figure 4-18.

Octets:1	**1**	**1**	**1**	**8**	**16**
Frame control	APS counter	APS command identifier	Standard Key Type	Source address	Initiator Verify-Key Hash Value
APS Header		APS Payload			

Figure 4-18. Verify-Key Command Frame

4.4.11.7.1 Command Identifier Field

The command identifier field SHALL indicate the verify-key request command type (APS_CMD_VERIFY_KEY, see Table 4-31).

4.4.11.7.2 StandardKeyType Field

This is the type of key being verified. See Table 4-9.

4.4.11.7.3 Source Address

This Source address field SHALL be the 64-bit extended address of the partner device that the destination shares the link key with.

4.4.11.7.4 Initiator Verify-Key Hash Value

This value is the outcome of executing the specialized keyed hash function specified in section B.1.4 using a key with the 1-octet string ‘0x03’ as the input string. The resulting value SHALL NOT be used as a key for encryption or decryption.

4.4.11.8 Confirm-Key Command

This APS command is used by a device (such as the trust center) to confirm its updated link key with the peer device.

The Confirm-Key command frame is formatted as illustrated in Figure 4-19.

Octets:1	1	1	1	1	8
Frame control	APS counter	APS command identifier	Status	StandardKeyType	Destination address
APS Header		APS Payload			

Figure 4-19. Confirm-Key Command Frame

4.4.11.8.1 Command Identifier Field

The command identifier field SHALL indicate the Confirm-Key command type (APS_CMD_VERIFY_KEY_RESPONSE, see Table 4-31).

4.4.11.8.2 Status

This will be the 1-byte status code indicating the result of the operation. See Table 2.27.

4.4.11.8.3 StandardKeyType

This is the type of key being verified. See Table 4-9.

4.4.11.8.4 Destination Address

This destination address field SHALL be the 64-bit extended address of the source device of the Verify-Key message.

4.4.11.9 Relay Message Downstream Command

This APS command is used by a Trust Center to relay a message through a parent router to a joining node as shown in Figure 4-20.

Octets: 1	1	1	Varies
Frame Control	APS Counter	APS Command Identifier	TLVs
APS Header		APS Payload	

Figure 4-20. Relay Message Downstream Command Frame

4.4.11.9.1 Command Identifier Field

The command identifier field SHALL indicate the Relay Message command type (APS_CMD_RELAY_MESSAGE_DOWNSTREAM).

4.4.11.9.2 TLVs

This field contains one or more TLVs. This command SHALL have at a minimum the Relay Message TLV.

4.4.11.9.2.1 Local TLVs

4.4.11.9.2.1.1 Relay Message TLV (ID = 0)

This local TLV (tag ID 0x00) indicates the message to be relayed and the destination of the device it is relayed to as shown n Figure 4-21.

Octets: 8	Varies
Destination EUI64	Message to be relayed

Figure 4-21. Format of the Relay Message TLV

The fields of the Relay Message TLV are defined in Table 4-33.

Table 4-33. Fields of the Relay Message TLV

Name	Type	Valid Range	Description
Destination EUI64	EUI64	0x0000000000000000 – 0xFFFFFFFFFFFFFFFF	This contains the EUI64 of the unauthorized neighbor that is the intended destination of the relayed message.
Message to be relayed	Special	Varies	This contains the single APS message, or message fragment, to be relayed from the from the Trust Center to the Joining device. The message SHALL start with the APS Header of the intended recipient.

4.4.11.10 Relay Message Upstream Command

This APS command is used by an unauthorized joining node to relay a message through a parent router to the Trust Center as shown in Figure 4-22.

Octets: 1	1	1	Varies
Frame Control	APS Counter	APS Command Identifier	TLVs
APS Header		APS Payload	

Figure 4-22. Relay Message Upstream Command Frame

4.4.11.10.1 Command Identifier Field

The command identifier field SHALL indicate the Relay Message command type (APS_CMD_RELAY_MESSAGE_UPSTREAM , see Table 4-31).

4.4.11.10.2 TLVs

This field contains one or more TLVs. This command SHALL have at a minimum the Relay Message TLV.

4.4.11.10.2.1 Local TLVs

4.4.11.10.2.1.1 Relay Message TLV (ID = 0)

This local TLV (tag ID 0x00) indicates the message to be relayed and the source of the device it is being relayed from as show in Figure 4-23.

Octets: 8	Varies
Source EUI64	Message to be relayed

Figure 4-23. Format of the Relay Message TLV

The fields of the Relay Message TLV are defined in Table 4-34.

Table 4-34. Fields of the Relay Message TLV

Name	Type	Valid Range	Description
Source EUI64	EUI64	0x0000000000000000 – 0xFFFFFFFFFFFFFFFF	This contains the EUI64 of the unauthorized neighbor that is the source of the relayed message.
Message to be relayed	Special	Varies	This contains the single APS message, or message fragment, to be relayed from the joining device to the Trust Center. The message SHALL start with the APS Header of the intended recipient.

4.4.12 Security-Related AIB Attributes

The AIB contains attributes that are required to manage security for the APS layer. Each of these attributes can be read or written using the APSME-GET.request and APSME-SET.request primitives, respectively. The security-related attributes contained in the APS PIB are presented in Table 4-35.

Table 4-35. AIB Security Attributes

Attribute	ID	Type	Range	Description	Default
apsDeviceKeyPairSet	0xaa	Set of key-pair descriptor entries. See Table 4.39.	Variable	A set of key-pair descriptors containing link keys shared with other devices.	-
apsTrustCenterAddress	0xab	Device address	Any valid 64-bit address	Identifies the address of the device's Trust Center. If this value is 0xFFFFFFFFFFFFFFFF, this means that there is no Trust Center in the network and the network	0xFFFFFFFFFFFFFFFF