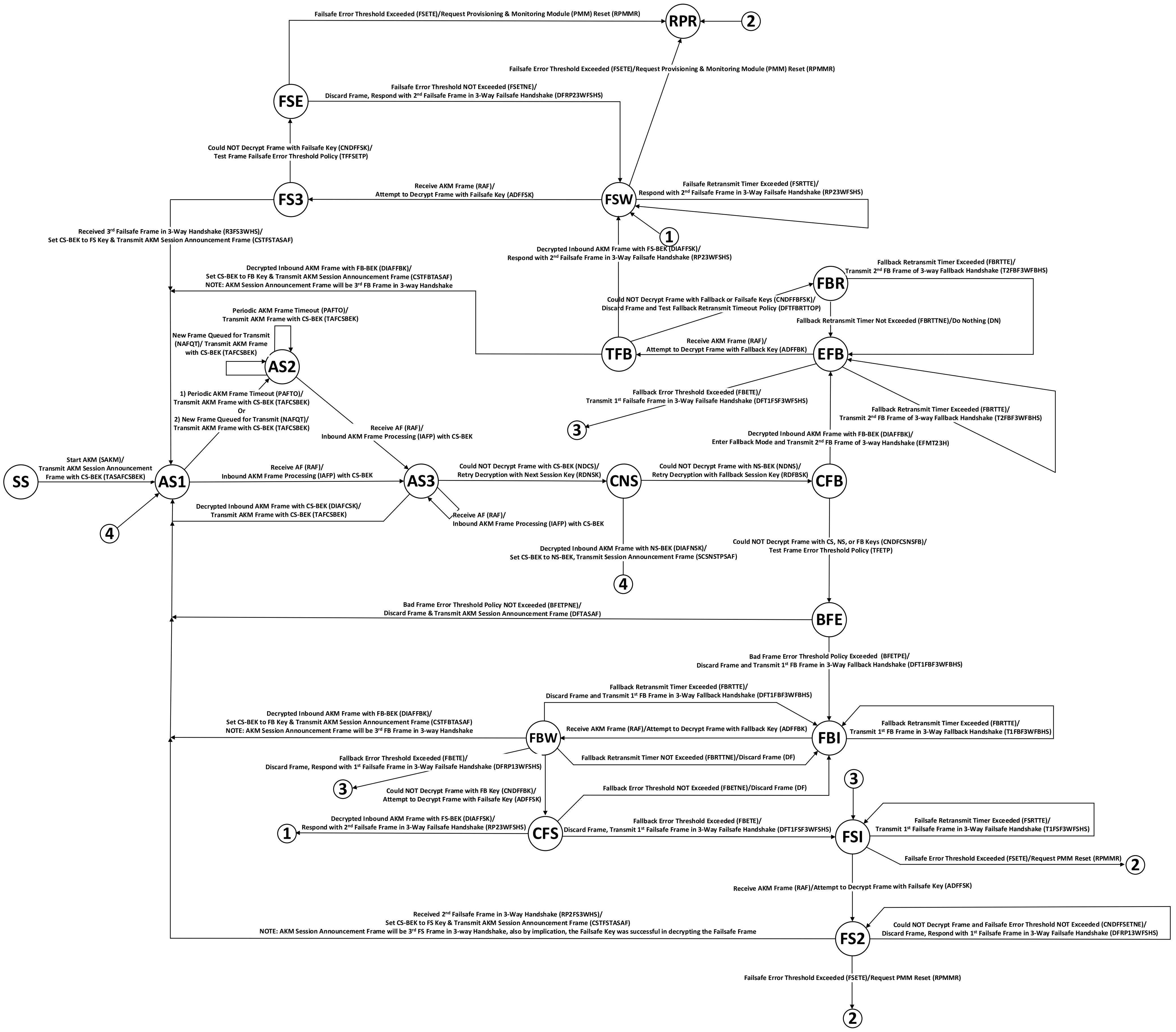
AKM Protocol Processing (Context Free Finite State Machine) Table of Contents

AKM Protocol Processing (Context Free Finite State Machine) Table of Contents

AKM Protocol Processing (Context Free Finite State Machine)


RPR
2
Failsafe Error Threshold Exceeded (FSETE)/Request Provisioning & Monitoring Module (PMM) Reset (RPMMR)
Failsafe Error Threshold Exceeded (FSETE)/Request Provisioning & Monitoring Module (PMM) Reset (RPMMR)
FSE
Failsafe Error Threshold NOT Exceeded (FSETNE)/
Discard Frame, Respond with 2nd Failsafe Frame in 3-Way Failsafe Handshake (DFRP23WFSHS)
Could NOT Decrypt Frame with Failsafe Key (CNDFFSK)/
Test Frame Failsafe Error Threshold Policy (TFFSETP)
FS3
Receive AKM Frame (RAF)/
Attempt to Decrypt Frame with Failsafe Key (ADFFSK)
FSW
Failsafe Retransmit Timer Exceeded (FSRTTE)/
Respond with 2nd Failsafe Frame in 3-Way Failsafe Handshake (RP23WFSHS)
1
Received 3rd Failsafe Frame in 3-Way Handshake (R3FS3WHS)/
Set CS-BEK to FS Key & Transmit AKM Session Announcement Frame (CSTFSTASAF)
Decrypted Inbound AKM Frame with FS-BEK (DIAFFSK)/
Respond with 2nd Failsafe Frame in 3-Way Failsafe Handshake (RP23WFSHS)
Decrypted Inbound AKM Frame with FB-BEK (DIAFFBK)/
Set CS-BEK to FB Key & Transmit AKM Session Announcement Frame (CSTFBTASAF)
NOTE: AKM Session Announcement Frame will be 3rd FB Frame in 3-way Handshake
Fallback Retransmit Timer Exceeded (FBRTTE)/
Transmit 2nd FB Frame of 3-way Fallback Handshake (T2FBF3WFBHS)
FBR
Could NOT Decrypt Frame with Fallback or Failsafe Keys (CNDFFBFSK)/
Discard Frame and Test Fallback Retransmit Timeout Policy (DFTFBRTTOP)
Fallback Retransmit Timer Not Exceeded (FBRTTNE)/Do Nothing (DN)
Periodic AKM Frame Timeout (PAFTO)/
Transmit AKM Frame with CS-BEK (TAFCSBEK)
New Frame Queued for Transmit
(NAFQT)/ Transmit AKM Frame
with CS-BEK (TAFCSBEK)
AS2
TFB
Receive AKM Frame (RAF)/
Attempt to Decrypt Frame with Fallback Key (ADFFBK)
EFB
1) Periodic AKM Frame Timeout (PAFTO)/
Transmit AKM Frame with CS-BEK (TAFCSBEK)
Or
2) New Frame Queued for Transmit (NAFQT)/
Transmit AKM Frame with CS-BEK (TAFCSBEK)
Fallback Error Threshold Exceeded (FBETE)/
Transmit 1st Failsafe Frame in 3-Way Failsafe Handshake (DFT1FSF3WFSHS)
3
Fallback Retransmit Timer Exceeded (FBRTTE)/
Transmit 2nd FB Frame of 3-way Fallback Handshake (T2FBF3WFBHS)
Receive AF (RAF)/
Inbound AKM Frame Processing (IAFP) with CS-BEK
Decrypted Inbound AKM Frame with FB-BEK (DIAFFBK)/
Enter Fallback Mode and Transmit 2nd FB Frame of 3-way Handshake (EFMT23H)
SS
Start AKM (SAKM)/
Transmit AKM Session Announcement
Frame with CS-BEK (TASAFCSBEK)
AS1
Receive AF (RAF)/
Inbound AKM Frame Processing (IAFP) with CS-BEK
AS3
Could NOT Decrypt Frame with CS-BEK (NDCS)/
Retry Decryption with Next Session Key (RDNSK)
CNS
Could NOT Decrypt Frame with NS-BEK (NDNS)/
Retry Decryption with Fallback Session Key (RDFBSK)
CFB
Decrypted Inbound AKM Frame with CS-BEK (DIAFCSK)/
Transmit AKM Frame with CS-BEK (TAFCSBEK)
Receive AF (RAF)/
Inbound AKM Frame Processing (IAFP) with CS-BEK
4
Decrypted Inbound AKM Frame with NS-BEK (DIAFNSK)/
Set CS-BEK to NS-BEK, Transmit Session Announcement Frame (SCSNSTPSAF)
Could NOT Decrypt Frame with CS, NS, or FB Keys (CNDFCSNSFB)/
Test Frame Error Threshold Policy (TFETP)
4
Bad Frame Error Threshold Policy NOT Exceeded (BFETPNE)/
Discard Frame & Transmit AKM Session Announcement Frame (DFTASAF)
BFE
Bad Frame Error Threshold Policy Exceeded (BFETPE)/
Discard Frame and Transmit 1st FB Frame in 3-Way Fallback Handshake (DFT1FBF3WFBHS)
Fallback Retransmit Timer Exceeded (FBRTTE)/
Discard Frame and Transmit 1st FB Frame in 3-Way Fallback Handshake (DFT1FBF3WFBHS)
Decrypted Inbound AKM Frame with FB-BEK (DIAFFBK)/
Set CS-BEK to FB Key & Transmit AKM Session Announcement Frame (CSTFBTASAF)
NOTE: AKM Session Announcement Frame will be 3rd FB Frame in 3-way Handshake
FBW
Receive AKM Frame (RAF)/Attempt to Decrypt Frame with Fallback Key (ADFFBK)
FBI
Fallback Retransmit Timer Exceeded (FBRTTE)/
Transmit 1st FB Frame in 3-Way Fallback Handshake (T1FBF3WFBHS)
Fallback Error Threshold Exceeded (FBETE)/
Discard Frame, Respond with 1st Failsafe Frame in 3-Way Failsafe Handshake (DFRP13WFSHS)
Fallback Retransmit Timer NOT Exceeded (FBRTTNE)/Discard Frame (DF)
3
Could NOT Decrypt Frame with FB Key (CNDFFBK)/
Attempt to Decrypt Frame with Failsafe Key (ADFFSK)
Fallback Error Threshold NOT Exceeded (FBETNE)/Discard Frame (DF)
3
Decrypted Inbound AKM Frame with FS-BEK (DIAFFSK)/
Respond with 2nd Failsafe Frame in 3-Way Failsafe Handshake (RP23WFSHS)
1
CFS
Fallback Error Threshold Exceeded (FBETE)/
Discard Frame, Transmit 1st Failsafe Frame in 3-Way Failsafe Handshake (DFT1FSF3WFSHS)
FSI
Failsafe Retransmit Timer Exceeded (FSRTTE)/
Transmit 1st Failsafe Frame in 3-Way Failsafe Handshake (T1FSF3WFSHS)
Failsafe Error Threshold Exceeded (FSETE)/Request PMM Reset (RPMMR)
2
Receive AKM Frame (RAF)/Attempt to Decrypt Frame with Failsafe Key (ADFFSK)
Received 2nd Failsafe Frame in 3-Way Handshake (RP2FS3WHS)/
Set CS-BEK to FS Key & Transmit AKM Session Announcement Frame (CSTFSTASAF)
NOTE: AKM Session Announcement Frame will be 3rd FS Frame in 3-way Handshake, also by implication, the Failsafe Key was successful in decrypting the Failsafe Frame
FS2
Could NOT Decrypt Frame and Failsafe Error Threshold NOT Exceeded (CNDFFSETNE)/
Discard Frame, Respond with 1st Failsafe Frame in 3-Way Failsafe Handshake (DFRP13WFSHS)
Failsafe Error Threshold Exceeded (FSETE)/Request PMM Reset (RPMMR)
2

NOTE: AKM utilizes a Encrypt-then-MAC (EtM) methodology when it comes to encrypting and authenticating. Thus, for purposes of simplification of the state machine, when it is testing whether or not a frame can be decrypted or not, that test includes both a successful authentication of the message, followed by a successful decryption of the message. If a message has been authenticated, and then fails to decrypt the frame, then implies there is something seriously wrong with the implementation and should go to Fatal Error state and should reflect that in a status message both to its own host log file as well as sending that to the AKM Provisioning and Monitoring module as an analytic message.

AKM FSM Acronyms and Definitions

ADF: AKM Data Frame – The AKM Data Frame refers to the normal user data frame encrypted within the AKM framework.

ATR: AKM Trust Relationship – The AKM Trust Relationship (ATR) is what defines the two nodes in the AKM PTP relationship.

CS-BEK: Current Session-Bulk Encryption Key – This is the Bulk Encryption Key associated with the current AKM session.

FSM: Finite State Machine – The AKM Protocol Processing FSM is represented by an event/state diagram illustrating the logical progression through the processing of an AKM frame and the interrelationship with other AKM Edge Nodes.

NS-BEK: Next Session-Bulk Encryption Key – This is the Bulk Encryption Key associated with the next AKM session.

PTP: Point-to-Point – Refers to the configuration of the AKM Trust Relationship. The initial implementation of AKM will ONLY support PTP.

SAF: Session Announcement Frame – This is a regular AKM data frame with the Session Announcement Bit Flag set. This is used to announce that the session is now fully active.

AKM FSM (State Descriptions)

States

AS1:	AKM Session State-1
AS2:	AKM Session State-2
AS3:	AKM Session State-3
BFE:	Bad Frame Error Threshold Policy State
CFB:	Check if Fallback Session Key can Decrypt Frame State
CFS:	Check Failsafe Key State
CNS:	Check if Next Session Key can Decrypt Frame State
EFB:	Enter Fallback Session FSM State
FBI:	Fallback Initialization State
FBR:	Fallback Retransmission Timer Check State
FBW:	Fallback Wait State
FS2:	Failsafe Check for 2nd Frame in Failsafe 3-Way Handshake State
FS3:	Failsafe Check for 3rd Frame in Failsafe 3-Way Handshake State
FSE:	Test Failsafe Error Threshold State
FSI:	Failsafe Initialization State
FSW:	Failsafe Wait State
RPR:	Request PMM Reset State
SS:	Start State
TFB:	Test Fallback Completion State

AKM Session-1 (SA1) State – The FSM enters this state upon transmission of a regular AKM frame (either a Session Announcement AKM frame or regular AKM frame).

AKM Session-2 (SA2) State – The FSM enters this state when there is a periodic AKM frame timeout .

AKM Session-3 (SA2) State – The FSM enters this state upon receipt of a regular AKM frame.

Bad Frame Error (BFE) State – The FSM traverses to this state in order to test if the "Bad Frame Error Threshold Policy" has been exceeded or not.

Check if Fallback Session Key can Decrypt Frame (CFB) State – The FSM traverses to this state in order to see if the Fallback Session Key can be used (or not) to decrypt the current frame.

Check Failsafe (CFS) State – The FSM traverses to this state to check if the current frame can be decrypted by the Failsafe Session Key. If not, it then checks to see if the Fallback Error Threshold Policy has been exceeded and if not, discards the frame and continues Fallback processing. If the Fallback Error Threshold Policy has been exceeded, then the FSM will initiate Failsafe Session processing by transmitting the 1st frame in a 3-way Failsafe protocol exchange.

Check Next Session Key (CNS) State – The FSM traverses to this state to check if the current frame can be decrypted by the Next Session Key. If not, it then it tries the Fallback Session Key. However, if it can be decrypted with the Next Session Key, then it assigns the Next Session Key (NS-BEK) to the Current Session Key (CS-BEK) and returns back to the Session Activated State, transmitting a Session Announcement Frame, which confirms a new session has successfully started.

Enter Fallback Session (EFB) State – The FSM traverses to this state to after receiving the 1st frame in the 3-way Fallback protocol exchange from the other end of the PTP connection.

Fallback Initialization (FBI) State – The FSM traverses to this state after the Edge Node has initiated a Failsafe Session by transmitting the 1st frame in the 3-Way Fallback Session Handshake protocol.

Fallback Retransmission (FBR) Timer Check State – The FSM traverses to this state when it cannot decrypt the current frame with either the Fallback Key or the Failsafe Key and checks to see if the "Fallback Retransmit Time-out" has been exceeded. Either way it discards the junk frame and if it the retransmit time-out has not been exceeded, it goes directly back to the EFB state and if it has been exceeded, it retransmits the 2nd FB Frame of the Fallback 3-way Handshake.

Fallback Wait (FBW) State – The FSM traverses to this state after the Edge Node responds with the 2nd frame in the Fallback Session 3-Way handshake protocol. It then wait there for one of four events:

1) The Edge Node receives a new AKM frame.
2) The Fallback Retransmit Time-out has been exceeded.
3) The Fallback Retransmit Time-out has not been exceeded.
4) The Fallback Error Threshold Policy has been exceeded.

Failsafe Check for 2nd Frame in Failsafe 3-Way Handshake (FS2) State – The FSM traverses to this state after the Edge Node has initiated a Failsafe Session by transmitting the 1st frame and then subsequently received an incoming AKM frame, with the expectation that the incoming frame is the 2nd frame in the Failsafe 3-Way Handshake.

Failsafe Check for 3rd Frame in Failsafe 3-Way Handshake (FS3) State – The FSM traverses to this state after the Edge Node has transmitted the 2nd frame in the Failsafe 3-Way Handshake, and has subsequently received an incoming AKM frame, with the expectation that the incoming frame is the 3rd frame in the Failsafe 3-Way Handshake. Thus, completing the Failsafe Session 3-Way Handshake.

Test Failsafe Error Threshold (FSE) State – The FSM traverses to this state after the Edge Node could not decrypt the frame with the Failsafe Session Key and checks if the Failsafe Error Threshold Policy has been exceeded, If it has, it goes to the RIR state where it will request the Provisioning & Monitor Module (PMM) to reset the AKM relationship. This can be done by either the PMM or the AKM Backend Configuration server, insofar as "autonomous" reconfigurations can occur. It can always be reconfigured manually, but doing so should never be required.

Failsafe Initialization (FSI) State – The FSM traverses to this state after the Edge Node has initiated a Failsafe Session by transmitting the 1st frame in the 3-Way Fallback Session Handshake protocol.

Failsafe Wait (FSW) State – The FSM traverses to this state after the Edge Node responds with the 2nd frame in the Failsafe Session 3-Way handshake protocol. It then wait there for one of three events:

1) The Edge Node receives a new AKM frame.
2) The Failsafe Retransmit Time-out has been exceeded.
3) The Failsafe Error Threshold Policy has been exceeded.

NOTE: that if the Failsafe Error Threshold Policy has been exceeded, the AKM relationship must be reset externally by either the PMM or the AKM Backend Configuration server, insofar as "autonomous" reconfigurations can occur. It can always be reconfigured manually, but doing so should never be required.

Request PMM Reset (RPR) State – This state is entered if both Fallback Resynchronization and Failsafe Resynchronization efforts have failed and the AKM Trust Relationship must request its state be reset by either the PMM or the backend configuration server. If there is no PMM within the network and there is no network connectivity to the backend, then, the AKM security group's designated Arbiter Node will attempt to reconfigure the AKM Trust Relationship. If one of the nodes has lost all ability to connect via AKM, then, the AKM Trust Relationship will remain disabled until a network administrator can manually refresh the AKM Trust Relationship.

Session Start (SS) State – Each ATR has an ascending order of priority that determines which node within the ATR will transmit the SEF first. If within a preconfigured time, that does not begin transmitting after power-on reset, the next node by order of priority will transmit the SEF, and so on, until finally one of the nodes within the ATR is successful at starting the session.

NOTE: The Session Establishment Frame SEF) is a normal AKM Data Frame (ADF), with whatever payload the sender wishes to send. The only difference is that the SIF bit flag is set and remains set until the other node in the PTP relationship responds, at which time, it will then set the SAF bit (which is the Session Active bit).

Test Fallback (TFB) Completion State – This state test whether or not the Fallback Resynchronization process has completed by receiving the final frame in the Fallback 3-Way protocol.

Non-Fatal Exception (NFE) State – This state is entered whenever there is a State/Event transition that is not expected within the FSM. Meaning, an event occurred within a particular state that should not have occurred while in that state. Thus, the FSM needs to go to this state as a means of capturing whatever data it can in order to determine how that happened (that the FSM had a State/Event transition that was not expected).

AKM FSM (Event Descriptions)

Bad Frame Error Policy Threshold Exceeded (BFETPE) Event – This event indicates that the policy for the "bad frame error threshold" has been exceeded.

Bad Frame Error Threshold NOT Exceeded (BFETPNE) Event – This event indicates that the policy for the "bad frame error threshold" has NOT been exceeded.

Could NOT Decrypt Frame with Fallback nor Failsafe Keys (CNDFFBFSK) Event – This event indicates that the current AKM Data Frame (ADF) was not able to be decrypted using either the Fallback or Failsafe session keys.

Could NOT Decrypt Frame with CS, NS, or FB Keys (CNDFCSNSFB) Event – This event indicates that the current frame being processed was not able to be decrypted with the CS-BEK, the NS-BEK, nor the FB-BEK.

Could NOT Decrypt Frame with Fallback Key (CNDFFBK) Event – This event indicates that the current frame being processed was not able to be decrypted with the FB-BEK.

Could NOT Decrypt Frame and Failsafe Error Threshold NOT Exceeded (CNDFFSETNE) Event – This event indicates that the current AKM frame cannot be decrypted by the Failsafe Session Key, but the Failsafe Error Threshold policy has not been exceeded. Thus, implying the FSM should remain within the Failsafe Resynchronization session.

Could NOT Decrypt Frame with Failsafe Key (CNDFFSK) Event – This event indicates that the current AKM frame cannot be decrypted by the Failsafe Session Key.

Could NOT Decrypt Frame with NS-BEK (NDNS) Event – This event indicates that the current AKM Data Frame (ADF) cannot be decrypted using the next session BEK.

Decrypted Inbound AKM Frame with CS-BEK (DIAFCSK) Event – This event indicates that the current frame was successfully decrypted using the current session's BEK (i.e., CS-BEK).

Decrypted Inbound AKM Frame with FB-BEK (DIAFFBK) Event – This event indicates that the current frame was successfully decrypted using the Fallback session's BEK (i.e., FB-BEK).

Decrypted Inbound AKM Frame with FS-BEK (DIAFFSK) Event – This event indicates that the current frame was successfully decrypted using the Failsafe session's BEK (i.e., FB-BEK).

Decrypted Inbound AKM Frame with NS-BEK (DIAFNSK) Event – This event indicates that the current frame was successfully decrypted using the current session's BEK (i.e., NS-BEK).

Fallback Retransmit Timer Exceeded (FBRTTE) Event – This event indicates that the Fallback Retransmit Time-out has been exceeded and it is now time to retransmit another Fallback Frame in an effort to get the other PTP to respond in kind with its own Fallback Frame, so that the AKM Trust Relationship can return back to normal AKM frame processing.

Fallback Retransmit Timer NOT Exceeded (FBRTTE) Event – This event indicates that the Fallback Retransmit Time-out has not yet been exceeded (i.e., has not yet expired).

Fallback Error Threshold Exceeded (FBETE) Event – This event indicates that the Fallback Error Threshold Policy has been exceeded and the FSM should transition into the Failsafe Session FSM.

Fallback Error Threshold NOT Exceeded (FRETNE) Event – This event indicates that the Fallback Error Threshold Policy has NOT been exceeded and the FSM should remain within the Fallback Session FSM.

Failsafe Error Threshold Exceeded (FSETE) Event – This event indicates that the Failsafe Error Threshold Policy has been exceeded and the FSM should transition into the Request PMM Reset (RIR) state.

Failsafe Error Threshold NOT Exceeded (FSETNE) Event – This event indicates that the Failsafe Error Threshold Policy has not been exceeded and the FSM should remain within the Failsafe Session FSM.

Failsafe Retransmit Timer Exceeded (FSRTTE) Event – This event indicates that the Failsafe Retransmit Time-out has been exceeded and the Edge Node should re-transmit another Failsafe Session Notification Frame in an effort to resynch with the other end of the AKM PTP connection.

New Frame Queued for Transmit (NAFQT) Event – This event indicates that the current frame was successfully decrypted using the Fallback session's BEK (i.e., FB-BEK).

AKM FSM (Event Descriptions)

Periodic AKM Frame Timeout (PAFTO) Event – This event indicates that the AKM Frame Timeout has expired and another AKM Keepalive frame must be transmitted.

Receive AKM Frame (RAF) Event – This event indicates that an AKM Frame has been received and is ready for processing.

Received 3rd part of Failsafe 3-Way Handshake Session Establishment Protocol (R3FS3WHS) Event – The Edge Node's FSM has received the 3rd and final frame in the Failsafe Resynchronization 3-Way Handshake session establishment protocol and can now safely transition back to normal communication.

Received 2nd part of Failsafe 3-Way Handshake Session Establishment Protocol (RP2FS3WHS) Event – The Edge Node's FSM has received the 2nd part of in the Failsafe Resynchronization 3-Way Handshake session establishment protocol and can now transmit out the 3rd and final part of the Failsafe 3-Way handshake and safely transition back to normal communication.

Start AKM (SAKM) Event – This event is used to start the AKM Finite State Machine (FSM).

Transmit AKM Frame with CS-BEK (TAFCS) Event – This event indicates that an AKM Frame has been encrypted with the current session key (CS-BEK) and subsequently transmitted.

AKM FSM (Action Descriptions)

Attempt to Decrypt Frame with Fallback Resynchronization Session Key (ADFFBK) Action – This action implicitly indicates that the current and next session keys have failed and thus, the FSM should attempt to decrypt the current frame with the Fallback Resynchronization Session key.

Attempt to Decrypt Frame with Failsafe Resynchronization Session Key (ADFFSK) Action – This action implicitly indicates that attempts to decrypt the current frame with the Fallback Resynchronization Session key.

Set CS-BEK to FB Key & Transmit AKM Session Announcement Frame (CSTFBTASAF) Action – This action updates the current session key with the current Fallback Session Key and subsequently sends out a Session Announcement Frame (by setting the Session Announcement bit in a regular frame) to let the other endpoint know that a new session has started.

Set CS-BEK to FS Key & Transmit AKM Session Announcement Frame (CSTFSTASAF) Action – This action updates the current session key with the current Failsafe Session Key and subsequently sends out a Session Announcement Frame (by setting the Session Announcement bit in a regular frame) to let the other endpoint know that a new session has started.

Discard Frame (DF) Action – This action discards the current frame.

Discard Frame, Respond with 1st Failsafe Frame in 3-Way Failsafe Handshake (DFRP13WFSHS) Action – This action discards the current Fallback frame (which could not be decrypted) and then initiates Failsafe Resynchronization by transmitting out the 1st Failsafe frame in the 3-Way Failsafe Handshake protocol.

Discard Frame and Transmit 1st FB Frame in 3-Way Fallback Handshake (DFT1FBF3WFBHS) Action – This action discards the current frame (which could not be decrypted) and then initiates Fallback Resynchronization by transmitting out the 1st Fallback frame in the 3-Way Fallback Handshake protocol.

Discard Frame and Transmit 1st FS Frame in 3-Way Failsafe Handshake (DFT1FSF3WFSHS) Action – This action discards the current frame (which could not be decrypted) and then initiates Failsafe Resynchronization by transmitting out the 1st Failsafe frame in the 3-Way Failsafe Handshake protocol.

Discard Frame and Test Fallback Resynchronization Session Fail Timer (DFTFBSFT) Action – This action discards the current frame and checks to see if the time allotted for the Fallback Resynchronization Session Fail Timer has been exceeded.

Discard Frame and Transmit AKM Session Announcement Frame (DFTASAF) Action – This action discards the current frame and then transmits an AKM session announcement frame, which is generally transmit at the beginning of a new session.

Discard Frame and Test Fallback Retransmit Timeout Policy (DFTFBRTTOP) Action – This action discards the current frame and then tests to see if the Fallback Retransmit Timeout Policy has been exceeded or not.

Do Nothing (DN) Action – This action represents that the FSM should not take any direct action as a consequence of this state/event transition.

Enter Fallback Mode and Transmit 2nd FB Frame of 3-way Handshake (EFMT23HS) Action – This action occurs after the FSM enters the Fallback 3-Way Handshake as a consequence of receiving the 1st Fallback Frame of the 3-way Fallback handshake protocol and subsequently responds with the 2nd Fallback Frame in the 3-way Fallback handshake protocol.

Inbound AKM Frame Processing (IAFP) Action – This action represents the processing of an inbound AKM frame, including the decryption.

Retry Decryption with Fallback Session Key (RDFBSK) Action – This action implicitly indicates that attempts to decrypt the current frame with the current and next session keys have failed and the Fallback Session key should now be tried for decrypting the current frame.

Retry Decryption with Next Session Key (RDNSK) Action – This action implicitly indicates that attempts to decrypt the current frame with the current session key has failed and the next session key should now be tried for decrypting the current frame.

Request PMM Reset (RPMMR) Action – As a representative of the AKM Trust Relationship, the Edge Node requests that the AKM Trust Relationship be reset by either the Provisioning Management Module (PMM) or the backend configuration server. If there is no PMM within the network and there is no network connectivity to the backend, then, the AKM security group's designated Arbiter Node will attempt to reconfigure the AKM Trust Relationship. If both nodes are no longer present within the AKM PTP Trust Relationship, then, the AKM Trust Relationship will remain disabled until a network administrator can manually refresh the AKM PTP Trust Relationship

Respond with 2nd Failsafe Frame in 3-Way Failsafe Handshake (RP23WFSHS) Action – This action occurs as a consequence of receiving the 1st Failsafe Frame of the 3-way Failsafe handshake protocol and subsequently responds with the 2nd Failsafe Frame in the 3-way Failsafe handshake protocol.

Set CS-BEK to NS-BEK & Transmit AKM Session Announcement Frame (SCNSTPAF) Action – This action occurs as a consequence of receiving the an incoming frame that can only be decrypted using the next session Bulk Encryption Key (NS-BEK).

Transmit 1st Fallback Frame in 3-Way Fallback Handshake (T1FBF3WFBHS) Action – This action initiates the Fallback 3-Way Handshake by sending the first frame in the aforementioned Fallback Session 3-Way Handshake protocol.

Transmit 1st Failsafe Frame in 3-Way Fallback Handshake (T1FSF3WFSHS) Action – This action initiates the Failsafe 3-Way Handshake by sending the first frame in the aforementioned Failsafe Session 3-Way Handshake protocol.

Transmit 2nd Fallback Frame in 3-Way Fallback Handshake (T2FBF3WFBHS) Action – This action responds to the 1st FB Frame in the Fallback 3-Way Handshake by sending the 2nd FB frame in the aforementioned Fallback Session 3-Way Handshake protocol.

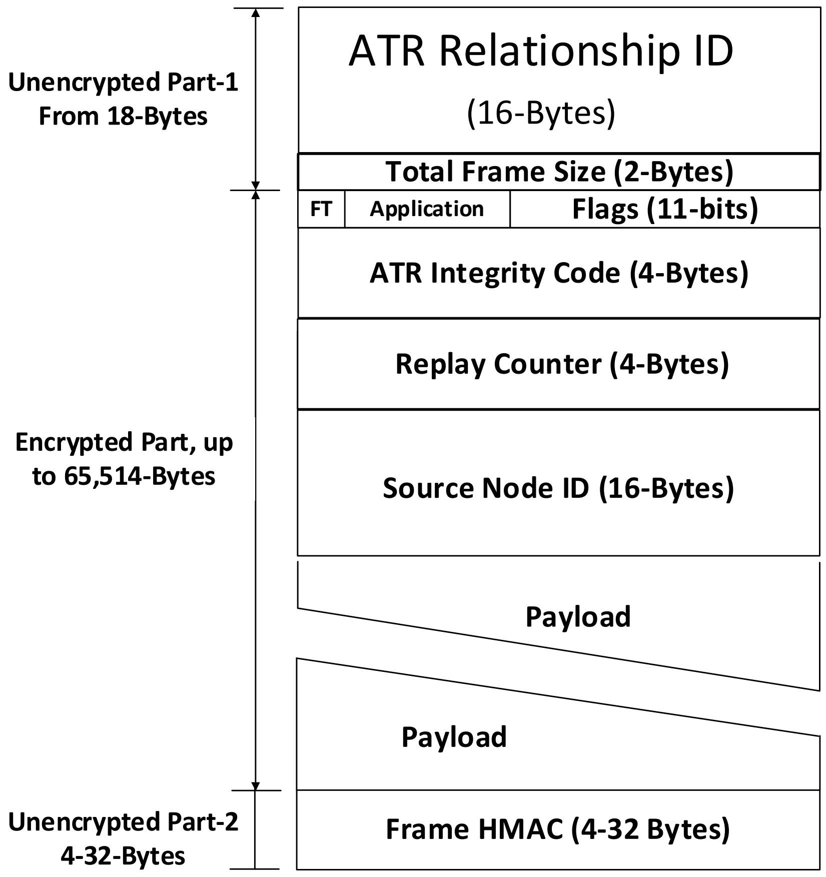
Transmit AKM Frame with CS-BEK (TAFCSBEK) Action – This action transmit a regular AKM Frame with CS-BEK.

Transmit AKM SA Frame with CS-BEK (TASAFCSBEK) Action – This action transmit an AKM Session Announcement Frame with CS-BEK.

Test Frame Error Threshold Policy (TFETP) Action – This action tests to see if the Fallback Frame Error Threshold Policy has been exceeded or not.

Test Frame Failsafe Error Threshold Policy (TFFSETP) Action – This action tests to see if the Failsafe Error Threshold policy has been exceeded.

AKM Frame Processing (Incoming)



Unencrypted Part-1
From 18-Bytes

ATR Relationship ID
(16-Bytes)

Total Frame Size (2-Bytes)

FT | Application | Flags (11-bits)

ATR Integrity Code (4-Bytes)

Replay Counter (4-Bytes)

Encrypted Part, up
to 65,514-Bytes

Source Node ID (16-Bytes)

Payload

Payload

Unencrypted Part-2
4-32-Bytes

Frame HMAC (4-32 Bytes)

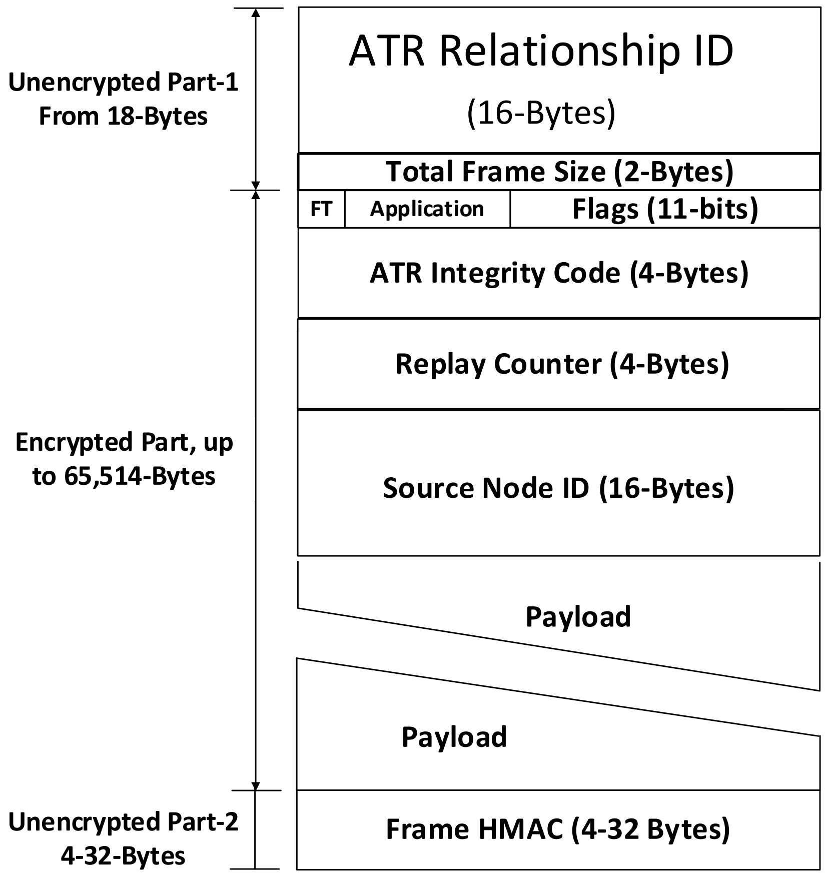
AKM Layer Security (ALS) Protocol Processing Performs:

1) Frame Header Processing.
2) Digital Signature Processing.
3) Encryption Processing.

The below is an overview of what is required in processing an incoming ALS frame:

1) First, there is there is the recognition of the frame being delineated into two unencrypted parts and an encrypted part.
2) If the relationship identifier does not match an AKM Trust Relationship within the AKM Node, then the frame should be discarded.
3) The “Total Frame Size” field provides the size of the entire frame, including the Frame HMAC, that is added to the frame after it has been encrypted, as AKM uses an EtM (i.e., Encrypt, then, MAC) methodology.
4) The first encrypted fields are the Frame-Type bit (Data-Frame or Management Frame), Application field, and Flag Bits. Process application and flags bits accordingly (i.e., this is implementation dependent).
5) The next field is the ATR Integrity Code, which is used to provide implicit zero trust functionality, given that every AKM Endpoint has previously authenticated both its endpoint and its membership within an AKM Trust Relationship.
6) Check the “Replay Counter”.
7) Process the Source Node Identifier information, which should correspond with the ATR Identifier.

AKM Frame Processing (Outgoing)



Unencrypted Part-1
From 18-Bytes

ATR Relationship ID
(16-Bytes)

Total Frame Size (2-Bytes)

FT | Application | Flags (11-bits)

ATR Integrity Code (4-Bytes)

Replay Counter (4-Bytes)

Encrypted Part, up
to 65,514-Bytes

Source Node ID (16-Bytes)

Payload

Payload

Unencrypted Part-2
4-32-Bytes

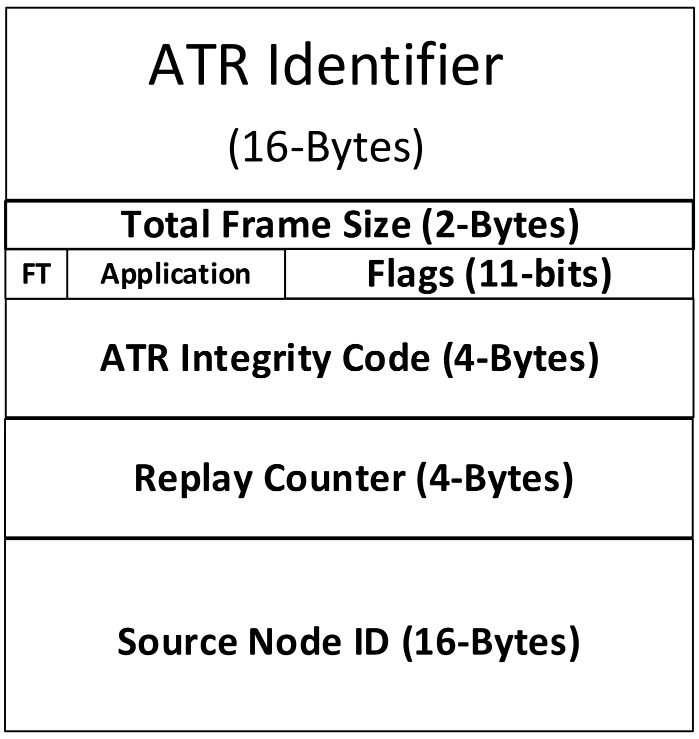
Frame HMAC (4-32 Bytes)

AKM Layer Security (ALS) Protocol Processing Performs:

1) Frame Header Processing.
2) Digital Signature Processing.
3) Encryption Processing.

The below is an overview of what is required in processing an outgoing ALS frame:

1) Fill out the Relationship ID, Source ID, and Destination ID (if applicable).
2) Calculate and insert the Total Frame Size.
3) Apply application and flag bits as specified by the application.
4) Calculate the Replay Counter.
5) Insert the specific ATR Integrity Code Segment, in accordance to the value of the Replay Counter (the ATR is divided into segments and then a Modulo Value of the Replay counter is utilized to determine which 4-bytes of the ATR IC is used.
6) Insert the Replay Counter.
7) Add in the payload.
8) Encrypt the encrypted part of the frame with AES.
9) Calculate the Frame HMAC to validate the entire frame.
10) Pass it down to TCP, UDP, or other transport layer protocol … context and/or implementation dependent.



ATR Identifier

(16-Bytes)

Total Frame Size (2-Bytes)

FT | Application | Flags (11-bits)

ATR Integrity Code (4-Bytes)

Replay Counter (4-Bytes)

Source Node ID (16-Bytes)

ATR Identifier: This 128-bit field represents the AKM Trust Relationship Identifier. In theory, because this version of AKM is point-to-point, there would be no need for either the Source Node Identifier or Destination Node Identifier given that the Relationship Identifier binds the two side together and with the exception of a "loopback" test of some sort, the AKM frame could only come from one place. However, as of this writing, only the destination node identifier is eliminated.

Payload Size: This 2-byte field has a maximum allowed value of 64K – the size of the Frame Header plus the HMAC..

AKM Frame Type: Currently, this is a 1-bit field, with '0' representing a user data frame and '1' representing a management frame. AKM management frames have yet to be defined, so at present, this field should always be '0'. At a minimum, AKM Management Frames will probably be used for resynching during Fallback and Failsafe.

The AKM frame header Application Parameter bits have sixteen bits available for use. Bit definitions that are available, include, but are not limited to the following bits:

- **Bits 0-2: Session Indicator Values indicate the "state" of the session:**
  - **Value: 000 – Undefined and does not use the SIV.**
  - **Value: 001 – Session Announcement (Current Session BEK) – This value assumes that both nodes within the ATR are actively participating within the session and as far as it knows are using the Current Session BEK.**
  - **Value: 010 – Session Activated (Next Session BEK) – This value is set to indicate that the ATR is currently transitioning to the Next Session security credentials.**
  - **Value: 011 – Fallback Resynchronization Session – This value is set to indicate that the ATR is currently within the Fallback Resynchronization Session in an effort to resynchronize its security credentials.**
  - **Value: 100 – Failsafe Resynchronization Session – This value is set to indicate that the ATR is currently within the Failsafe Resynchronization Session in an effort to resynchronize its security credentials.**
  - **Values: 101, 110, & 111 – undefined/reserved.**
- **Bits 3-15: Currently, Undefined/Reserved.**

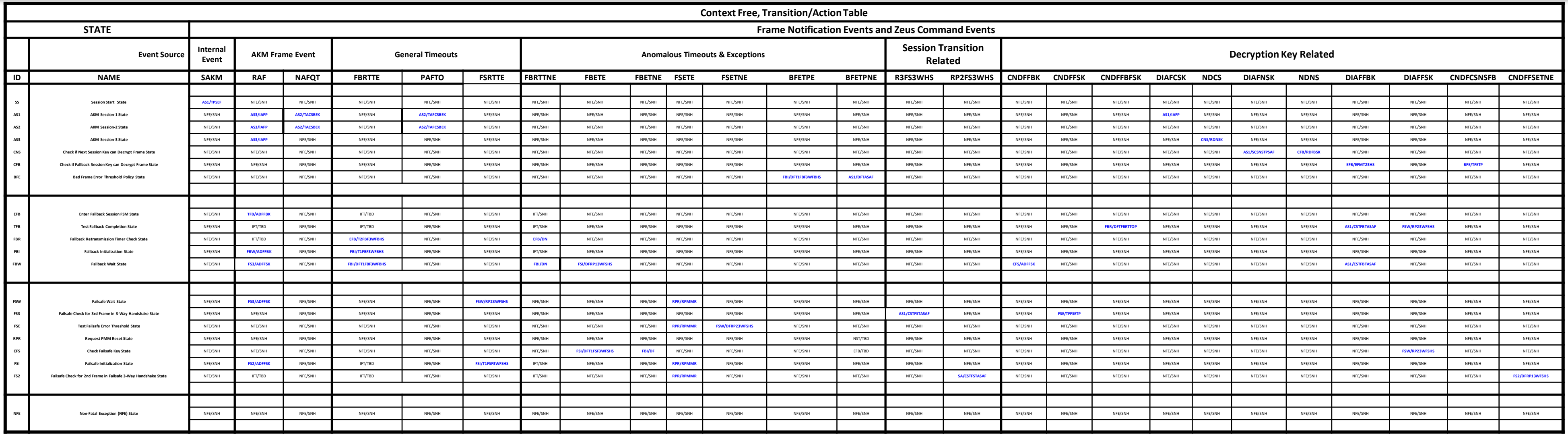
AKM Application Parameter bits will enable specific applications on opposing ends of a connection to directly communicate with each other.

ATR Integrity Code (AIC): This is used to provide implicit zero trust functionality, given that every AKM Endpoint has previously authenticated both its endpoint and its membership within an AKM Trust Relationship, this is a very simplistic and implicit mechanism for proving the sender is authenticated. The actual mechanics are beyond the scope of this document, but can be explained with a deeper dive and should be the source of a separate document on this subject.

AKM Replay Counter: This is a 32-bit field, that is always incremented from the perspective of the sender. Thus, both sides of an AKM connection will have different values for when they are sending the Replay Counter.

Source Node Identifier – This identifies the node that transmitted the frame.

AKM FSM (Full FSM)



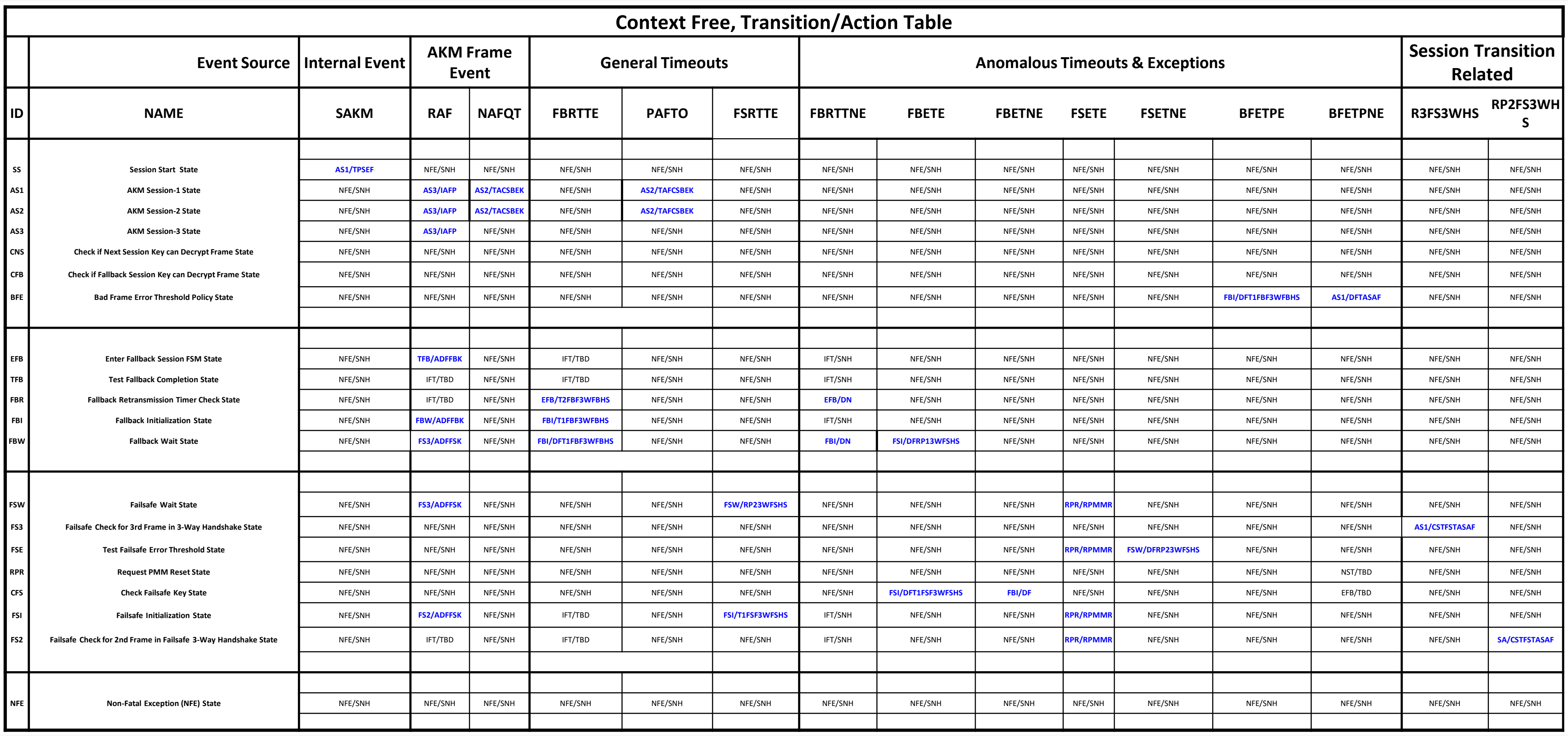
This is the full FSM representing the Point-to-Point AKM communication FSM coming out of power-on/reset as well as the transition to next session security credentials, Fallback security credentials, and Failsafe security credentials. Meaning, it is complete. The states are listed in the same order in which someone may logically traverse through the state machine, while the events are organized in accordance with their functionality grouping.

IMPORTANT: This FSM does NOT represent what goes on for:

1) Adding/Deleting a Node (this will be added later and will more than likely be a separate state machine because it does require some external intervention (i.e., loading the target device with both Edge Node applet and Edge Node AKM Identifier).

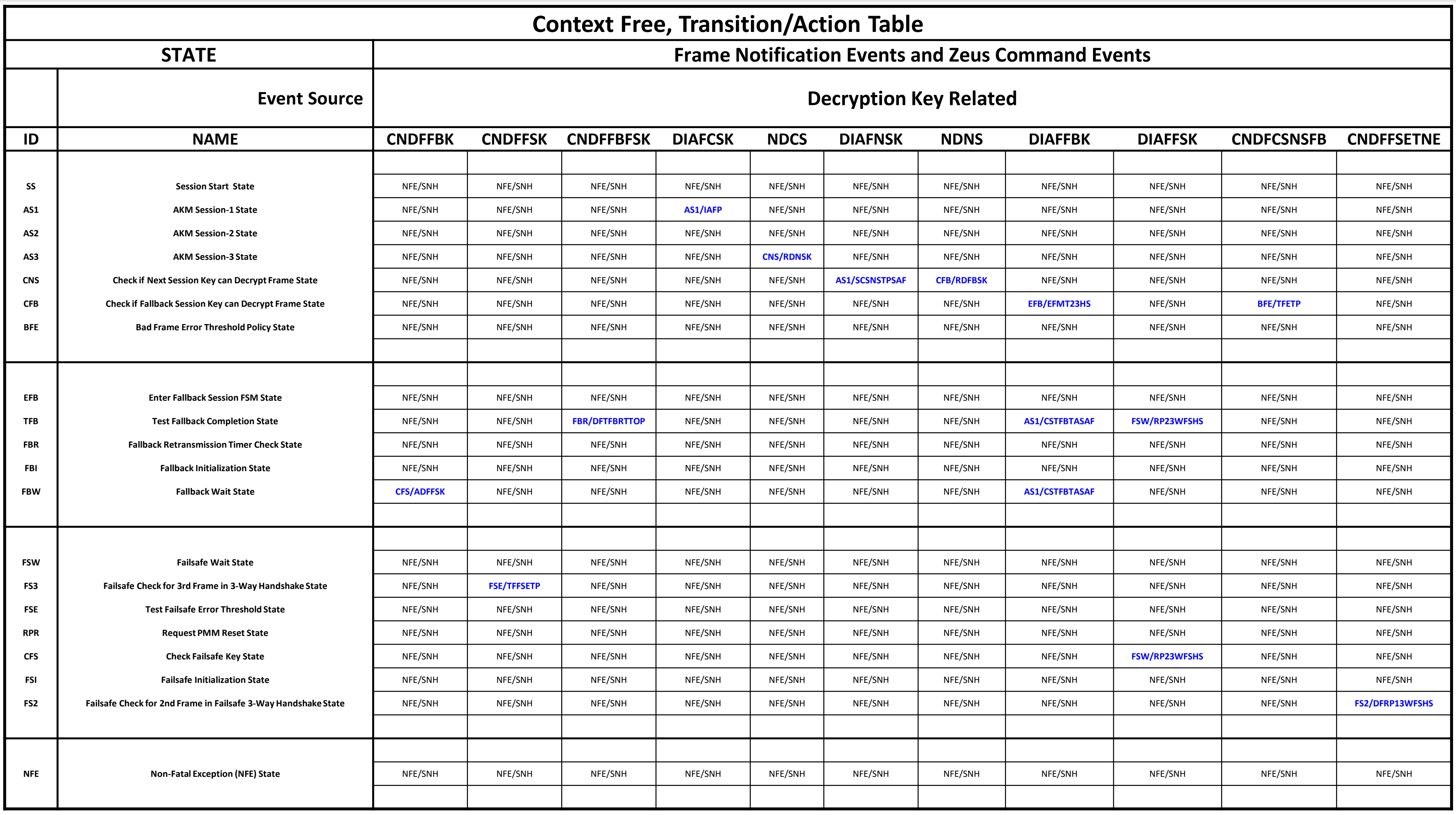
2) Hot Swap: that said, the mechanics for "hot-swap" are very similar to the mechanics of the state transition between current session credentials and next session credentials.

FSM (Left half of FSM)



Context Free, Transition/Action Table																
	Event Source	Internal Event	AKM Frame Event		General Timeouts			Anomalous Timeouts & Exceptions							Session Transition Related	
ID	NAME	SAKM	RAF	NAFQT	FBRTTE	PAFTO	FSRTTE	FBRTTNE	FBETE	FBETNE	FSETE	FSETNE	BFETPE	BFETPNE	R3FS3WHS	RP2FS3WHS
SS	Session Start State	AS1/TPSEF	NFE/SNH	NFE/SNH	NFE/SNH	NFE/SNH	NFE/SNH	NFE/SNH	NFE/SNH	NFE/SNH	NFE/SNH	NFE/SNH	NFE/SNH	NFE/SNH	NFE/SNH	NFE/SNH
AS1	AKM Session-1 State	NFE/SNH	AS3/IAFP	AS2/TACSBEK	NFE/SNH	AS2/TAFCSBEK	NFE/SNH	NFE/SNH	NFE/SNH	NFE/SNH	NFE/SNH	NFE/SNH	NFE/SNH	NFE/SNH	NFE/SNH	NFE/SNH
AS2	AKM Session-2 State	NFE/SNH	AS3/IAFP	AS2/TACSBEK	NFE/SNH	AS2/TAFCSBEK	NFE/SNH	NFE/SNH	NFE/SNH	NFE/SNH	NFE/SNH	NFE/SNH	NFE/SNH	NFE/SNH	NFE/SNH	NFE/SNH
AS3	AKM Session-3 State	NFE/SNH	AS3/IAFP	NFE/SNH	NFE/SNH	NFE/SNH	NFE/SNH	NFE/SNH	NFE/SNH	NFE/SNH	NFE/SNH	NFE/SNH	NFE/SNH	NFE/SNH	NFE/SNH	NFE/SNH
CNS	Check if Next Session Key can Decrypt Frame State	NFE/SNH	NFE/SNH	NFE/SNH	NFE/SNH	NFE/SNH	NFE/SNH	NFE/SNH	NFE/SNH	NFE/SNH	NFE/SNH	NFE/SNH	NFE/SNH	NFE/SNH	NFE/SNH	NFE/SNH
CFB	Check if Fallback Session Key can Decrypt Frame State	NFE/SNH	NFE/SNH	NFE/SNH	NFE/SNH	NFE/SNH	NFE/SNH	NFE/SNH	NFE/SNH	NFE/SNH	NFE/SNH	NFE/SNH	NFE/SNH	NFE/SNH	NFE/SNH	NFE/SNH
BFE	Bad Frame Error Threshold Policy State	NFE/SNH	NFE/SNH	NFE/SNH	NFE/SNH	NFE/SNH	NFE/SNH	NFE/SNH	NFE/SNH	NFE/SNH	NFE/SNH	NFE/SNH	FBI/DFT1FBF3WFBHS	AS1/DFTASAF	NFE/SNH	NFE/SNH
EFB	Enter Fallback Session FSM State	NFE/SNH	TFB/ADFFBK	NFE/SNH	IFT/TBD	NFE/SNH	NFE/SNH	IFT/SNH	NFE/SNH	NFE/SNH	NFE/SNH	NFE/SNH	NFE/SNH	NFE/SNH	NFE/SNH	NFE/SNH
TFB	Test Fallback Completion State	NFE/SNH	IFT/TBD	NFE/SNH	IFT/TBD	NFE/SNH	NFE/SNH	IFT/SNH	NFE/SNH	NFE/SNH	NFE/SNH	NFE/SNH	NFE/SNH	NFE/SNH	NFE/SNH	NFE/SNH
FBR	Fallback Retransmission Timer Check State	NFE/SNH	IFT/TBD	NFE/SNH	EFB/T2FBF3WFBHS	NFE/SNH	NFE/SNH	EFB/DN	NFE/SNH	NFE/SNH	NFE/SNH	NFE/SNH	NFE/SNH	NFE/SNH	NFE/SNH	NFE/SNH
FBI	Fallback Initialization State	NFE/SNH	FBW/ADFFBK	NFE/SNH	FBI/T1FBF3WFBHS	NFE/SNH	NFE/SNH	IFT/SNH	NFE/SNH	NFE/SNH	NFE/SNH	NFE/SNH	NFE/SNH	NFE/SNH	NFE/SNH	NFE/SNH
FBW	Fallback Wait State	NFE/SNH	FS3/ADFFSK	NFE/SNH	FBI/DFT1FBF3WFBHS	NFE/SNH	NFE/SNH	FBI/DN	FSI/DFRP13WFSHS	NFE/SNH	NFE/SNH	NFE/SNH	NFE/SNH	NFE/SNH	NFE/SNH	NFE/SNH
FSW	Failsafe Wait State	NFE/SNH	FS3/ADFFSK	NFE/SNH	NFE/SNH	NFE/SNH	FSW/RP23WFSHS	NFE/SNH	NFE/SNH	NFE/SNH	RPR/RPMMR	NFE/SNH	NFE/SNH	NFE/SNH	NFE/SNH	NFE/SNH
FS3	Failsafe Check for 3rd Frame in 3-Way Handshake State	NFE/SNH	NFE/SNH	NFE/SNH	NFE/SNH	NFE/SNH	NFE/SNH	NFE/SNH	NFE/SNH	NFE/SNH	NFE/SNH	NFE/SNH	NFE/SNH	NFE/SNH	AS1/CSTFSTASAF	NFE/SNH
FSE	Test Failsafe Error Threshold State	NFE/SNH	NFE/SNH	NFE/SNH	NFE/SNH	NFE/SNH	NFE/SNH	NFE/SNH	NFE/SNH	NFE/SNH	RPR/RPMMR	FSW/DFRP23WFSHS	NFE/SNH	NFE/SNH	NFE/SNH	NFE/SNH
RPR	Request PMM Reset State	NFE/SNH	NFE/SNH	NFE/SNH	NFE/SNH	NFE/SNH	NFE/SNH	NFE/SNH	NFE/SNH	NFE/SNH	NFE/SNH	NFE/SNH	NFE/SNH	NST/TBD	NFE/SNH	NFE/SNH
CFS	Check Failsafe Key State	NFE/SNH	NFE/SNH	NFE/SNH	NFE/SNH	NFE/SNH	NFE/SNH	NFE/SNH	FSI/DFT1FSF3WFSHS	FBI/DF	NFE/SNH	NFE/SNH	NFE/SNH	EFB/TBD	NFE/SNH	NFE/SNH
FSI	Failsafe Initialization State	NFE/SNH	FS2/ADFFSK	NFE/SNH	IFT/TBD	NFE/SNH	FSI/T1FSF3WFSHS	IFT/SNH	NFE/SNH	NFE/SNH	RPR/RPMMR	NFE/SNH	NFE/SNH	NFE/SNH	NFE/SNH	NFE/SNH
FS2	Failsafe Check for 2nd Frame in Failsafe 3-Way Handshake State	NFE/SNH	IFT/TBD	NFE/SNH	IFT/TBD	NFE/SNH	NFE/SNH	IFT/SNH	NFE/SNH	NFE/SNH	RPR/RPMMR	NFE/SNH	NFE/SNH	NFE/SNH	NFE/SNH	SA/CSTFSTASAF
NFE	Non-Fatal Exception (NFE) State	NFE/SNH	NFE/SNH	NFE/SNH	NFE/SNH	NFE/SNH	NFE/SNH	NFE/SNH	NFE/SNH	NFE/SNH	NFE/SNH	NFE/SNH	NFE/SNH	NFE/SNH	NFE/SNH	NFE/SNH

FSM (Right half of FSM)



Context Free, Transition/Action Table												
STATE		Frame Notification Events and Zeus Command Events										
	Event Source	Decryption Key Related										
ID	NAME	CNDFFBK	CNDFFSK	CNDFFBFSK	DIAFCSK	NDCS	DIAFNSK	NDNS	DIAFFBK	DIAFFSK	CNDFCSNSFB	CNDFFSETNE
SS	Session Start State	NFE/SNH	NFE/SNH	NFE/SNH	NFE/SNH	NFE/SNH	NFE/SNH	NFE/SNH	NFE/SNH	NFE/SNH	NFE/SNH	NFE/SNH
AS1	AKM Session-1 State	NFE/SNH	NFE/SNH	NFE/SNH	AS1/IAFP	NFE/SNH	NFE/SNH	NFE/SNH	NFE/SNH	NFE/SNH	NFE/SNH	NFE/SNH
AS2	AKM Session-2 State	NFE/SNH	NFE/SNH	NFE/SNH	NFE/SNH	NFE/SNH	NFE/SNH	NFE/SNH	NFE/SNH	NFE/SNH	NFE/SNH	NFE/SNH
AS3	AKM Session-3 State	NFE/SNH	NFE/SNH	NFE/SNH	NFE/SNH	CNS/RDNSK	NFE/SNH	NFE/SNH	NFE/SNH	NFE/SNH	NFE/SNH	NFE/SNH
CNS	Check if Next Session Key can Decrypt Frame State	NFE/SNH	NFE/SNH	NFE/SNH	NFE/SNH	NFE/SNH	AS1/SCSNSTPSAF	CFB/RDFBSK	NFE/SNH	NFE/SNH	NFE/SNH	NFE/SNH
CFB	Check if Fallback Session Key can Decrypt Frame State	NFE/SNH	NFE/SNH	NFE/SNH	NFE/SNH	NFE/SNH	NFE/SNH	NFE/SNH	EFB/EFMT23HS	NFE/SNH	BFE/TFETP	NFE/SNH
BFE	Bad Frame Error Threshold Policy State	NFE/SNH	NFE/SNH	NFE/SNH	NFE/SNH	NFE/SNH	NFE/SNH	NFE/SNH	NFE/SNH	NFE/SNH	NFE/SNH	NFE/SNH
EFB	Enter Fallback Session FSM State	NFE/SNH	NFE/SNH	NFE/SNH	NFE/SNH	NFE/SNH	NFE/SNH	NFE/SNH	NFE/SNH	NFE/SNH	NFE/SNH	NFE/SNH
TFB	Test Fallback Completion State	NFE/SNH	NFE/SNH	FBR/DFTFBRTTOP	NFE/SNH	NFE/SNH	NFE/SNH	NFE/SNH	AS1/CSTFBTASAF	FSW/RP23WFSHS	NFE/SNH	NFE/SNH
FBR	Fallback Retransmission Timer Check State	NFE/SNH	NFE/SNH	NFE/SNH	NFE/SNH	NFE/SNH	NFE/SNH	NFE/SNH	NFE/SNH	NFE/SNH	NFE/SNH	NFE/SNH
FBI	Fallback Initialization State	NFE/SNH	NFE/SNH	NFE/SNH	NFE/SNH	NFE/SNH	NFE/SNH	NFE/SNH	NFE/SNH	NFE/SNH	NFE/SNH	NFE/SNH
FBW	Fallback Wait State	CFS/ADFFSK	NFE/SNH	NFE/SNH	NFE/SNH	NFE/SNH	NFE/SNH	NFE/SNH	AS1/CSTFBTASAF	NFE/SNH	NFE/SNH	NFE/SNH
FSW	Failsafe Wait State	NFE/SNH	NFE/SNH	NFE/SNH	NFE/SNH	NFE/SNH	NFE/SNH	NFE/SNH	NFE/SNH	NFE/SNH	NFE/SNH	NFE/SNH
FS3	Failsafe Check for 3rd Frame in 3-Way Handshake State	NFE/SNH	FSE/TFFSETP	NFE/SNH	NFE/SNH	NFE/SNH	NFE/SNH	NFE/SNH	NFE/SNH	NFE/SNH	NFE/SNH	NFE/SNH
FSE	Test Failsafe Error Threshold State	NFE/SNH	NFE/SNH	NFE/SNH	NFE/SNH	NFE/SNH	NFE/SNH	NFE/SNH	NFE/SNH	NFE/SNH	NFE/SNH	NFE/SNH
RPR	Request PMM Reset State	NFE/SNH	NFE/SNH	NFE/SNH	NFE/SNH	NFE/SNH	NFE/SNH	NFE/SNH	NFE/SNH	NFE/SNH	NFE/SNH	NFE/SNH
CFS	Check Failsafe Key State	NFE/SNH	NFE/SNH	NFE/SNH	NFE/SNH	NFE/SNH	NFE/SNH	NFE/SNH	NFE/SNH	FSW/RP23WFSHS	NFE/SNH	NFE/SNH
FSI	Failsafe Initialization State	NFE/SNH	NFE/SNH	NFE/SNH	NFE/SNH	NFE/SNH	NFE/SNH	NFE/SNH	NFE/SNH	NFE/SNH	NFE/SNH	NFE/SNH
FS2	Failsafe Check for 2nd Frame in Failsafe 3-Way Handshake State	NFE/SNH	NFE/SNH	NFE/SNH	NFE/SNH	NFE/SNH	NFE/SNH	NFE/SNH	NFE/SNH	NFE/SNH	NFE/SNH	FS2/DFRP13WFSHS
NFE	Non-Fatal Exception (NFE) State	NFE/SNH	NFE/SNH	NFE/SNH	NFE/SNH	NFE/SNH	NFE/SNH	NFE/SNH	NFE/SNH	NFE/SNH	NFE/SNH	NFE/SNH