# AKM Protocol Processing (Context Free Finite State Machine)

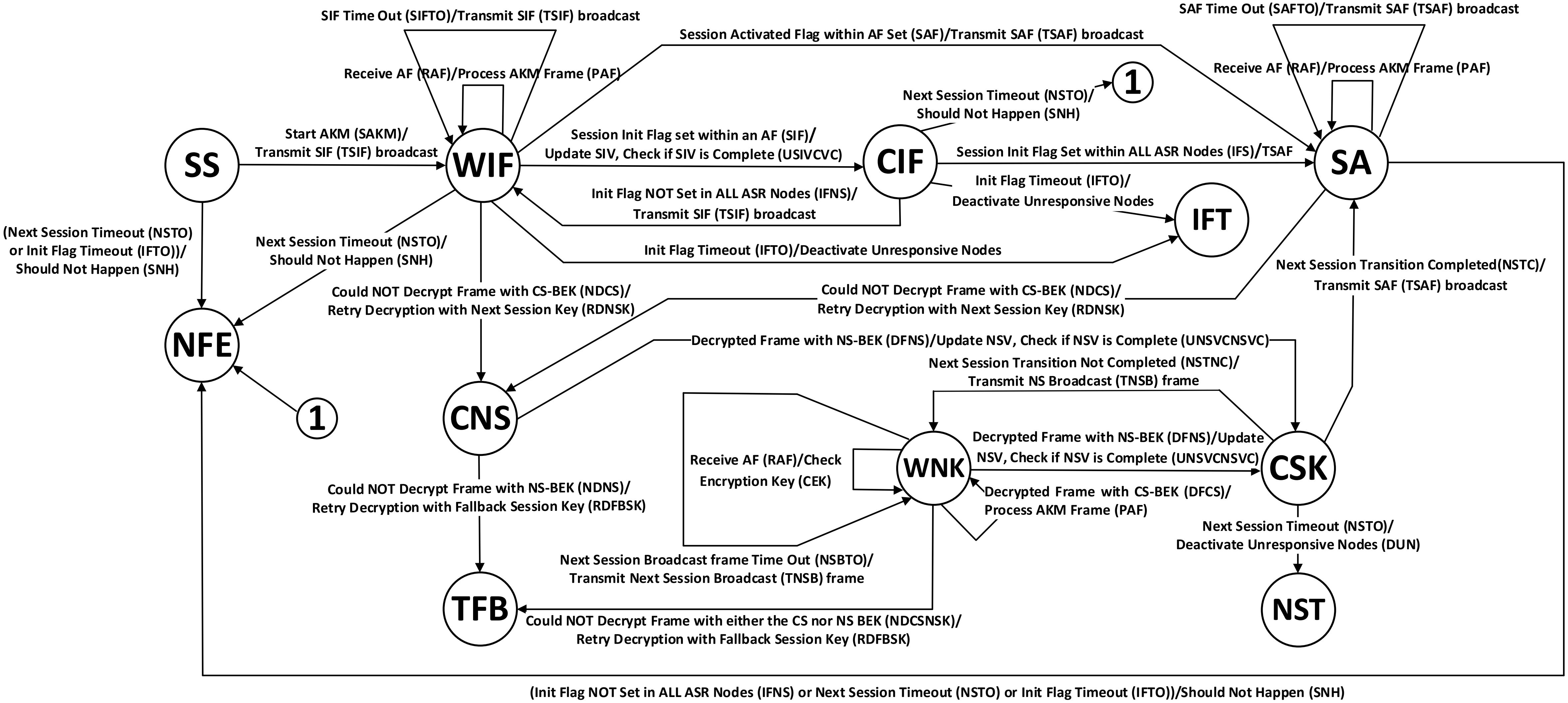
# AKM Protocol Processing (Context Free Finite State Machine)

# AKM Protocol Processing (Context Free Finite State Machine)

# AKM Protocol Processing (Context Free Finite State Machine)

# AKM Protocol Processing (Context Free Finite State Machine)

# AKM Protocol Processing (Context Free Finite State Machine)


SIF Time Out (SIFTO)/Transmit SIF (TSIF) broadcast
Receive AF (RAF)/Process AKM Frame (PAF)
Session Activated Flag within AF Set (SAF)/Transmit SAF (TSAF) broadcast
SAF Time Out (SAFTO)/Transmit SAF (TSAF) broadcast
Receive AF (RAF)/Process AKM Frame (PAF)
Next Session Timeout (NSTO)/
Should Not Happen (SNH)
1
Start AKM (SAKM)/
Transmit SIF (TSIF) broadcast
SS
WIF
Session Init Flag set within an AF (SIF)/
Update SIV, Check if SIV is Complete (USIVCVC)
CIF
Session Init Flag Set within ALL ASR Nodes (IFS)/TSAF
SA
Init Flag NOT Set in ALL ASR Nodes (IFNS)/
Transmit SIF (TSIF) broadcast
Init Flag Timeout (IFTO)/
Deactivate Unresponsive Nodes
IFT
(Next Session Timeout (NSTO)
or Init Flag Timeout (IFTO))/
Should Not Happen (SNH)
Next Session Timeout (NSTO)/
Should Not Happen (SNH)
Init Flag Timeout (IFTO)/Deactivate Unresponsive Nodes
Next Session Transition Completed(NSTC)/
Transmit SAF (TSAF) broadcast
Could NOT Decrypt Frame with CS-BEK (NDCS)/
Retry Decryption with Next Session Key (RDNSK)
Could NOT Decrypt Frame with CS-BEK (NDCS)/
Retry Decryption with Next Session Key (RDNSK)
NFE
Decrypted Frame with NS-BEK (DFNS)/Update NSV, Check if NSV is Complete (UNSVCNSVC)
Next Session Transition Not Completed (NSTNC)/
Transmit NS Broadcast (TNSB) frame
1
CNS
Decrypted Frame with NS-BEK (DFNS)/Update
NSV, Check if NSV is Complete (UNSVCNSVC)
Receive AF (RAF)/Check
Encryption Key (CEK)
WNK
CSK
Decrypted Frame with CS-BEK (DFCS)/
Process AKM Frame (PAF)
Could NOT Decrypt Frame with NS-BEK (NDNS)/
Retry Decryption with Fallback Session Key (RDFBSK)
Next Session Timeout (NSTO)/
Deactivate Unresponsive Nodes (DUN)
Next Session Broadcast frame Time Out (NSBTO)/
Transmit Next Session Broadcast (TNSB) frame
TFB
NST
Could NOT Decrypt Frame with either the CS nor NS BEK (NDCSNSK)/
Retry Decryption with Fallback Session Key (RDFBSK)
(Init Flag NOT Set in ALL ASR Nodes (IFNS) or Next Session Timeout (NSTO) or Init Flag Timeout (IFTO))/Should Not Happen (SNH)

# AKM Protocol Processing (Context Free Finite State Machine)

## Acronyms:

| | |
|---|---|
| ADF: | AKM Data Frame |
| ASR: | AKM Security Relationship |
| CS-BEK: | Current Session Bulk Encryption Key |
| FSM: | Finite State Machine |
| NS-BEK: | Next Session Bulk Encryption Key |
| SAF: | Session Activated Flag |
| SEF: | Session Establishment Frame |
| SIF: | Session Initialized Flag |

## FSM States:

| | |
|---|---|
| SS: | **S**ession **S**tart (SS) State |
| WIF: | **W**ait for **I**nitialized **F**lag (WIF) from All Nodes State |
| CIF: | **C**heck **I**nitialized **F**lag (CIF) State |
| SA: | **S**ession **A**ctive (SA) State |
| IFT: | **I**nitialized **F**lag **T**imeout (IFT) State |

-----------------------------------------------------------------------------------

| | |
|---|---|
| CNS: | **C**heck for **N**ext **S**ession (CNS) Security Credentials State |
| CSK: | **C**heck **S**ession **K**ey (CSK) State |
| WNK: | **W**ait for **N**ext Session **K**ey (WNK) State |
| NST: | **N**ext **S**ession **T**imeout (NST) State |
| TFB: | **Try** **F**all**B**ack (TFB) State |
| NFE: | **N**on-**F**atal **E**xception (NFE) State |

# 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.

**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.

**SAF: Session Activated Flag** – This is a bit within the "Flags" field of the AKM Header and is only set once all nodes have been acknowledged as having their Session Confirmed Flag bit set.

**SCF: Session Confirmed Flag** – This is a bit within the "Flags" field of the AKM Header and is only set once all nodes have set their "Session Initialized Flag" set.

**SEF: Session Establishment Frame** – This is a regular AKM data frame with the Session Initialized Bit Flag set. This term is intended to only refer to the very first frame transmitted with the Session Initialized Bit Flag set, which is determined by order of priority as configured within the ASR.

**SIF: Session Initialized Flag** – This is a bit within the "Flags" field of the AKM Header and is used by all nodes within the ASR as the first step in the session instantiation process.

# AKM FSM (State Descriptions)

Session Start (SS) State – Each ASR has an ascending order of priority  that determines which node within the ASR 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 ASR 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 SIF bit flag is set and remains set until all nodes within the ASR have transmitted at least one ADF with the SIF set.

Wait for Initialization Flag (WIF) State – The FSM remains in a loop between this state and the CIF state, as it continues to read AKM Data Frames.  All frames should fall into one of two categories.  Either their “Session Initialization Flag” is set, in which case, it will transition to the CIF.  Or, The “Session Activated Flag” is set, in which case, it will transition to the SA state.

Check Initialized Flag (CIF) State – This state checks to see if all of the nodes have transmitted at least one frame with the “Session Initialized Flag” (SIF) set.  If so, the FSM transitions to the SA state.  If not, it transitions back to the WIF state, unless an, “Initialized Flag” timeout has occurred, in which case, it transitions to the IFT state.

Initialized Flag Timeout (IFT) State – If after a configured period of time, all nodes have not responded with their, “Session Initialized Flag” being set, then the FSM transitions to the, “Initialized Flag Timeout” state.  This is  the initial state in the, “Initialized Flag Timeout” FSM subset (represented and detailed separately).

# AKM FSM (State Descriptions)

Session Activated (SA) State – The FSM remains in a loop in this state, and unless there is an error or a resynch event continues to read AKM Data Frames.  All frames should fall into one of two categories.  Either their "Session Confirmation Flag" is set, in which case, it will transition to the CCF state.  Or, The "Session Active Flag" is set, in which case, it will transition to the SA state.

Check Next Session (CNS) State – The FSM transitions to this state when the CNS state checks to see if the Next Session Key is able to decrypt the current frame.  If so, then, the FSM must  transition the Edge Node and the associated ASR to the next set of security credentials.

Check Session Key (CSK) State – This state checks the current ADF being processed to see if the ASR has completed the transition with all nodes using the Next Session set of security credentials.

Wait for Next session Key (WNK) State – The FSM remains in a loop between this state and the CSK state, as it continues to read AKM Data Frames.  All frames should fall into one of two categories.  Either they can be decrypted using Current Session security credentials or Next Session security credentials.  If it is Current Session security credentials, it remains in this state.  If it is Next Session security credentials, it transitions to the CSK state.  If it cannot decrypt the frame with either set of security credentials, it transitions to the EFB state.

# AKM FSM (State Descriptions)

Next Session Timeout (NST) State – The FSM transitions to its Next Session Timeout FSM subset.  This is the entry point of that FSM subset (represented and detailed separately).  It enters into this state after receiving an event indicating that the amount of time to wait for the entire ASR to transition to the next session BEK has expired.

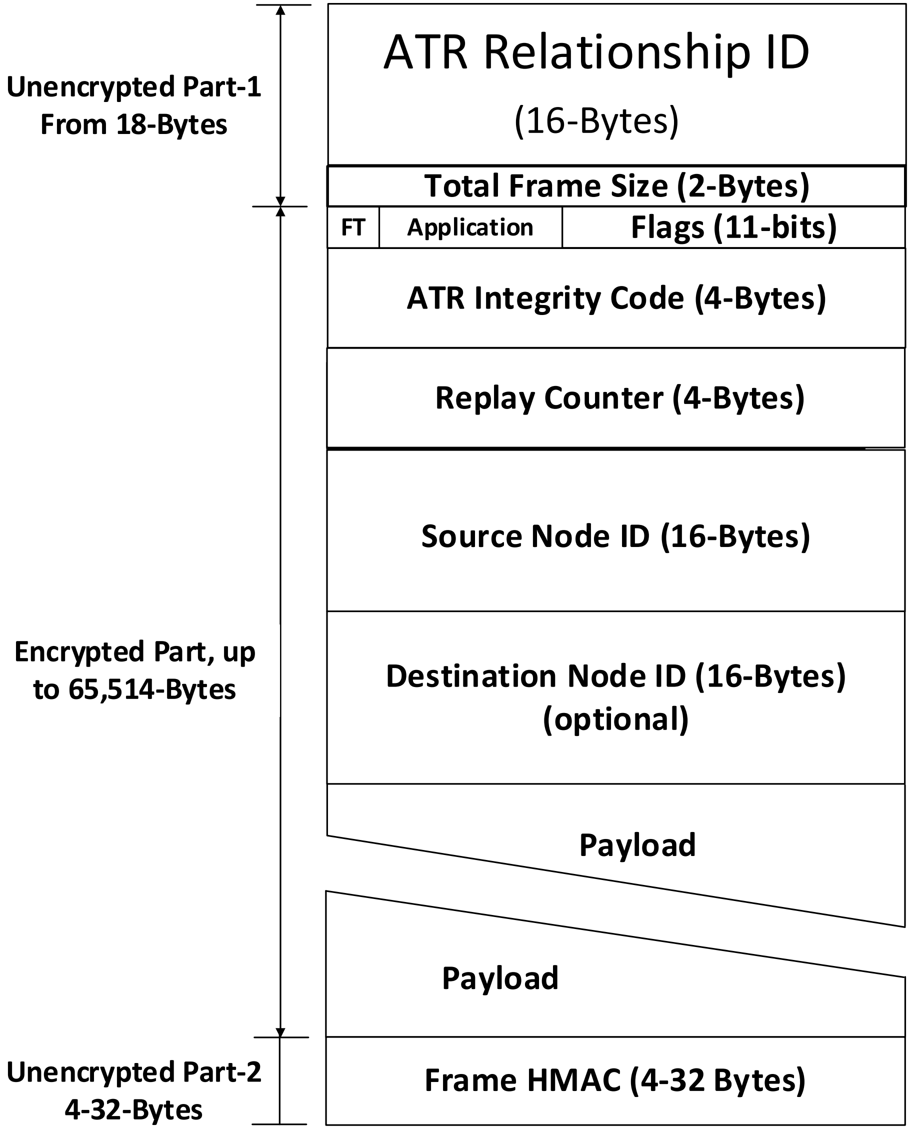
Try FallBack (TFB) State – The current ADF could not be decrypted with either the Current Session BEK nor the Next Session BEK.  Thus, the FSM transitions to the "Try FallBack" FSM subset (represented and detailed separately).

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 Layer Security (ALS) Frame Processing (Incoming)

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

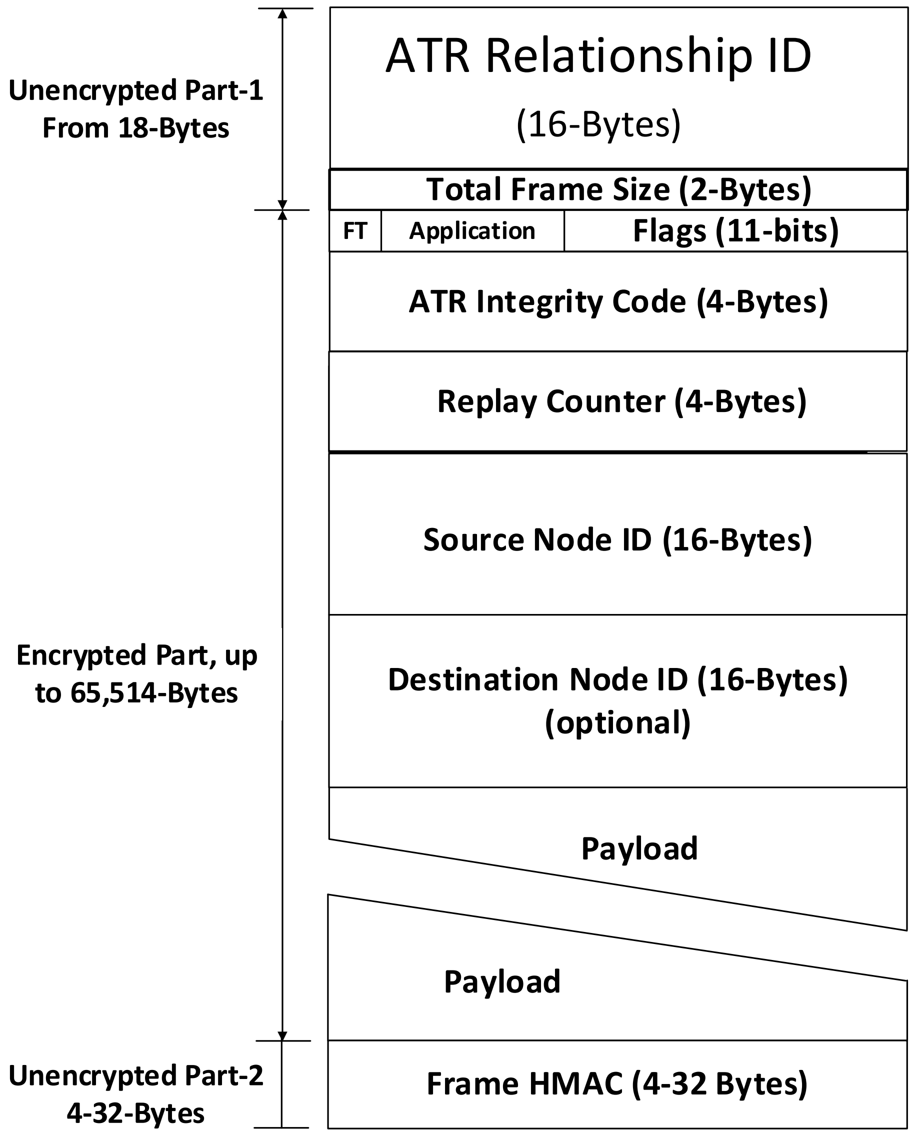
1) First, there is there is the recognition of the frame being delineated into two unencrypted parts at each end, with an encrypted part between them.
2) If the relationship identifier does not match a security relationship within the AKM Node, then the frame should be discarded.
3) The "Total Frame 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.
8) If present, validate the Destination Node Identifier information to affirm the frame is for this specific node. If it is not present, then this is a broadcast frame (even if the underlying transport layer is TCP, it is "logically" a broadcast frame).



# ALS Frame Processing (Outgoing)

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

1) Fill out the Relationship ID, Source ID, and Destination ID (if applicable).
2) Calculate and then Insert the Total Frame Size.
4) Apply application and flag bits as specified by the application.
5) Calculate the Replay Counter.
6) Insert the ATR Integrity Code (AIC) according to the modulo value of the Replay Counter. Example, suppose we are using a 256-bit HMAC, thus, the HMAC secret is 32-bytes, which given the AIC is 4-bytes, means, the AIC segment inserted into the frame is going to correspond to the modulo 8 value of the Replay Counter. Thus, the Modulo 8 value is 0, then, the frame AIC will use bytes 0-3 of the full AIC. If the Modulo 8 value is 1, then, the frame AIC will use bytes 4-7 of the full AIC, and so on.
7) Insert the previously calculated Replay Counter.
8) Add in the payload.
9) Encrypt the encrypted part of the frame with AES.
10) Calculate and append the Frame HMAC, either in total or in part, in accordance to the rules of the implementation.
11) Pass it down to TCP or UDP … context and/or implementation dependent.

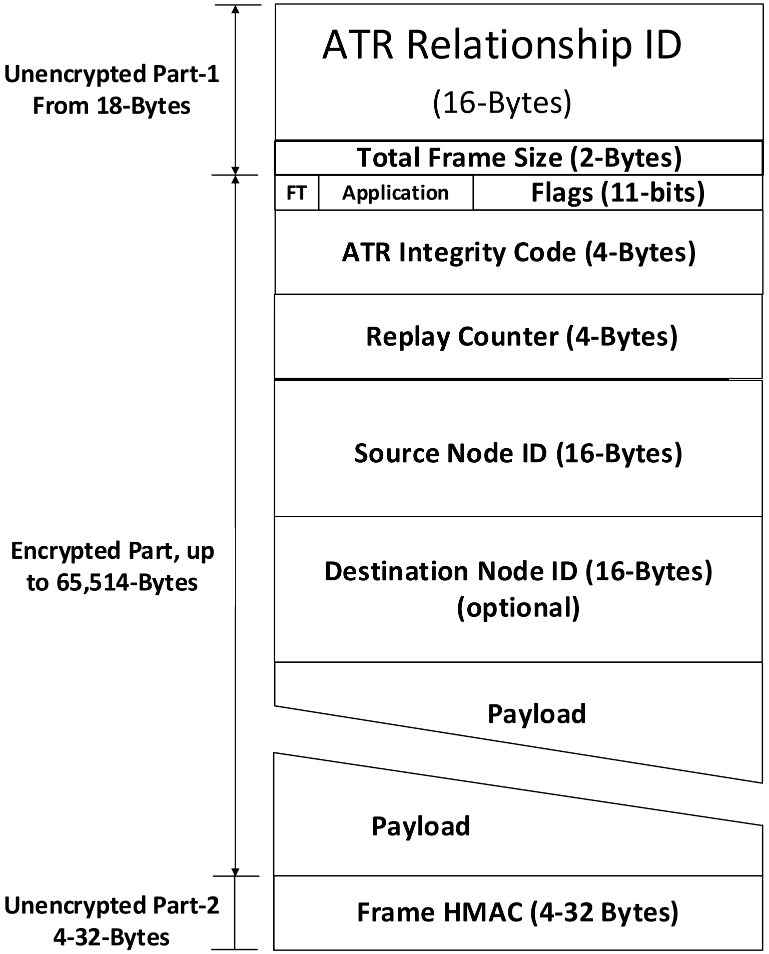


**NOTE: This software module is also in each of the AKM Edge Nodes.**

# ALS Frame Processing (Frame Header and Bit Fields)

The ALS frame header has eleven (11) 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 Initialization (Current Session BEK) – This value represents when an AKM Edge Node is initially powered on and/or just coming out of reset. The purpose of the bit is to convey to other AKM Edge Nodes it is an active participant within the AKM Security Relationship (ASR), but is still waiting for confirmation for other AKM Edge Nodes within the ASR to confirm their participation either directly (with their own Session Initialization Bit set) or indirectly (via the Session Integrity Vector (SIV)). The SIV is sent whenever this bit is set and indicates which AKM Edge Nodes it is aware of, including itself. The SIV is “OR’d” with the host Edge Node’s SIV, as a means of expediting the session to becoming fully active.
  - ❖ Value: 010 – Session Activated (Current Session BEK) – This bit is set to indicate that all, active nodes within the ASR are actively participating within the session and as far as it knows, it the ASR is still using the Current Session BEK. Thus, it has no need for the SIV and is not part of the frame header when the Session Indicator Values are set to this value.
  - ❖ Value: 011 – Session Activated (Next Session BEK) – This bit is set to indicate that all, active nodes within the ASR are actively participating within the session, but the ASR is currently transitioning to a new session and this particular node is using the Next Session BEK. This value represents that the ASR is currently transitioning to a new session. The SIV is used to facilitate completion of the Next Session transition process.
- ❑ Bit 3: AKM Address Indicator:
  - ❖ Value: 0 – Indicates an AKM Broadcast, which results in there being no Destination Node ID included within the frame. There is only the AKM Relationship ID (which in essence, is a broadcast address for the ASR), plus an AKM source identifier, representing the AKM Edge Node which sent the incoming AKM data frame.
  - ❖ Value: 1 – Indicates a regular AKM frame with both a source and destination address, in addition to the AKM Relationship Identifier, which every AKM data frame has.
- ❑ Bits 4-10: Currently, Undefined.



Unencrypted Part-1 From 18-Bytes

ATR Relationship ID (16-Bytes)

Total Frame Size (2-Bytes)

FT | Application | Flags (11-bits)

Encrypted Part, up to 65,514-Bytes

ATR Integrity Code (4-Bytes)

Replay Counter (4-Bytes)

Source Node ID (16-Bytes)

Destination Node ID (16-Bytes) (optional)

Payload

Payload

Unencrypted Part-2 4-32-Bytes

Frame HMAC (4-32 Bytes)

# ALS Frame Processing (Session Integrity Vector (SIV))

The Session Integrity Vector (SIV) uses 1-bit per AKM Edge Node to represent the associated AKM address within an ATR. The bits are ordered in the same order as to how the AKM Edge Node are ordered within the ATR's Synchronized Data Set (SDS). All nodes within a Synchronized Data Set are ordered in ascending order according to their AKM Identifier and are traversable via a balanced binary tree.

```
typedef struct _BALANCED_BINARY_TREE {                 // SizeOf: 16-bytes
    // Fields needed for keeping a balanced binary tree.
    S32  balance_factor;                  //  -1, 0, or +1       // Offset:  0 -  3 ( 4-bytes)

    // NOTE: the user of this structure should be very careful in setting and/or accessing
    // the owning data structure via these fields

    // A NULL_PTR value for the "parent_node_ptr", indicates this is the ROOT node.
    PVOID  parent_node_ptr;               // Offset:  4 -  7 (4-bytes)
    PVOID  left_subtree_ptr;              // Offset:  8 - 11 (4-bytes)
    PVOID  right_subtree_ptr;             // Offset: 12 - 15 (4-bytes)
} BALANCED_BINARY_TREE, *PBALANCED_BINARY_TREE;

struct _AKM_INFO_OBJECT {                                         // SizeOf: 36-bytes
    AKM_OBJECT_STANDARD_128_BIT_ADDRESS  AKM_Node_Address;  // Offset:  0 - 15 (16-bytes)

    ASR_OBJECT_DELINEATOR_ENUM        AKM_Object_Delineator;      // Offset: 16 - 19 ( 4-bytes)

    // Balanced Binary Tree
    // Use Methods defined to manipulate this BT, to ensure only AKM Info
    // Objects are manipulated for nodes connected via this field.
    BALANCED_BINARY_TREE              Balanced_Binary_Tree;           // Offset: 20 - 35 (16-bytes)
} AKM_INFO_OBJECT, *PAKM_INFO_OBJECT;
```

# ALS Frame Processing (Tracking Vectors, SIV, NSV, ANV, RNV)

1) The Session Initialization Vector (SIV) field within the AKM frame header is only used during state transitions coming out of power-on/reset.

2) The SIV field is also used to represent the transmitting edge node’s SIV.

3) The SIV is of an implementation dependent length, done so in increments of 2-bytes (16-bits) to reflect the maximum size of an AKM Security Relationship (ASR). So, if the implementation limit is 16-Nodes or smaller within a single ASR, only two bytes are used to represent the SIV within the header. If 32-nodes or smaller is the limit (but greater than 17), then, likewise, 4-bytes are used, and so on.

4) While not necessary to share this information between nodes, as synchronization can be accomplished without this, it would just take longer. ORing, the SIV from an incoming edge node with the SIV of the host node, will greatly expedite the overall synchronization process for obvious reasons.

5) Similarly, the Next Session Vector (NSV) is used for tracking which nodes within the ASR have transitioned to the Next Session Set of Credentials.

6) The Add Node Vector (ANV) keeps track of which nodes have been accepted a new node into the ASR.

7) The Remove Node Vector (RNV) keeps track of which nodes have deleted an existing node from the ASR.

# ALS Frame Processing (Tracking Vectors, SIV, NSV, ANV, RNV)

1) The Session Initialization Vector (SIV) field within the AKM frame header is only used during state transitions coming out of power-on/reset.

2) The SIV field is also used to represent the transmitting edge node's SIV.

3) The SIV is of an implementation dependent length, done so in increments of 2-bytes (16-bits) to reflect the maximum size of an AKM Security Relationship (ASR). So, if the implementation limit is 16-Nodes or smaller within a single ASR, only two bytes are used to represent the SIV within the header. If 32-nodes are smaller is the limit (but greater than 17), then, likewise, 4-bytes are used, and so on.

4) While not necessary to share this information between nodes, as synchronization can be accomplished without this, it would just take longer. ORing, the SIV from an incoming edge node with the SIV of the host node, will greatly expedite the overall synchronization process for obvious reasons.

5) Similarly, the Next Session Vector (NSV) is used for tracking which nodes within the ASR have transitioned to the Next Session Set of Credentials.

6) The Add Node Vector (ANV) keeps track of which nodes have been accepted a new node into the ASR.

7) The Remove Node Vector (RNV) keeps track of which nodes have deleted an existing node from the ASR.

# AKM FSM (Event Descriptions)

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

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

Session Initialized Flag (SIF) Event – This event indicates that the SIF bit was set within the current ADF being processed.

Session Activated Flag (SAF) Event – This event indicates that the SCF bit was set within all nodes and the session is now fully active and the next session BEK should now become the current session BEK.

SIF Time Out (SIFTO) Event – This event indicates that the amount of time since the last SIF broadcast frame was transmitted from the Edge Node has been exceeded.

SAF Time Out (SAFTO) Event – This event indicates that the amount of time since the last SAF broadcast frame was transmitted by the Edge Node has been exceeded.

Next Session Broadcast frame Time Out (NSBTO) Event – This event indicates that the amount of time since the last Next Session broadcast frame was transmitted by the Edge Node has been exceeded.

Initialized Flag Timeout (IFTO) Event – This event indicates that the maximum time allotted has now been exceeded for the all of the nodes within the ASR to have broadcasted at least one frame with its SIF bit set.

Next Session Timeout (NSTO) Event – This event indicates that the maximum time allotted for the entire ASR to have become active, has now been exceeded. That is, for all of them to have broadcast a frame with either their SCF or SAF bit set.

# AKM FSM (Event Descriptions)

**Initialized Flag Not Set (IFNS) Event – This event indicates that there still remains at least one or more nodes within the ASR have not joined the current session initiation.**

**Initialized Flag Set (IFS) Event – This event indicates that the Session Initialized Flag has been set in all nodes within the ASR, which means, that all nodes within the ASR are engaged in this AKM session.**

**Next Session Transition Not Completed (NSTNC) Event – This event indicates that there still remains at least one or more nodes within the ASR that is not using the next session BEK.**

**Next Session Transition Completed (NSTC) Event – This event indicates that all nodes within the ASR are now using the next session BEK.**

**Could NOT Decrypt Frame with CS-BEK (NDCS) Event – This event indicates that the current AFD cannot be decrypted using the current session BEK.**

**Check Encryption Key (CEK) Event – This event checks to see if either the current session key or next session key can decrypt the frame..**

**Decrypted Frame with NS-BEK (DFNS) Event – This event indicates that the current AFD was successfully decrypted using the next session BEK.**

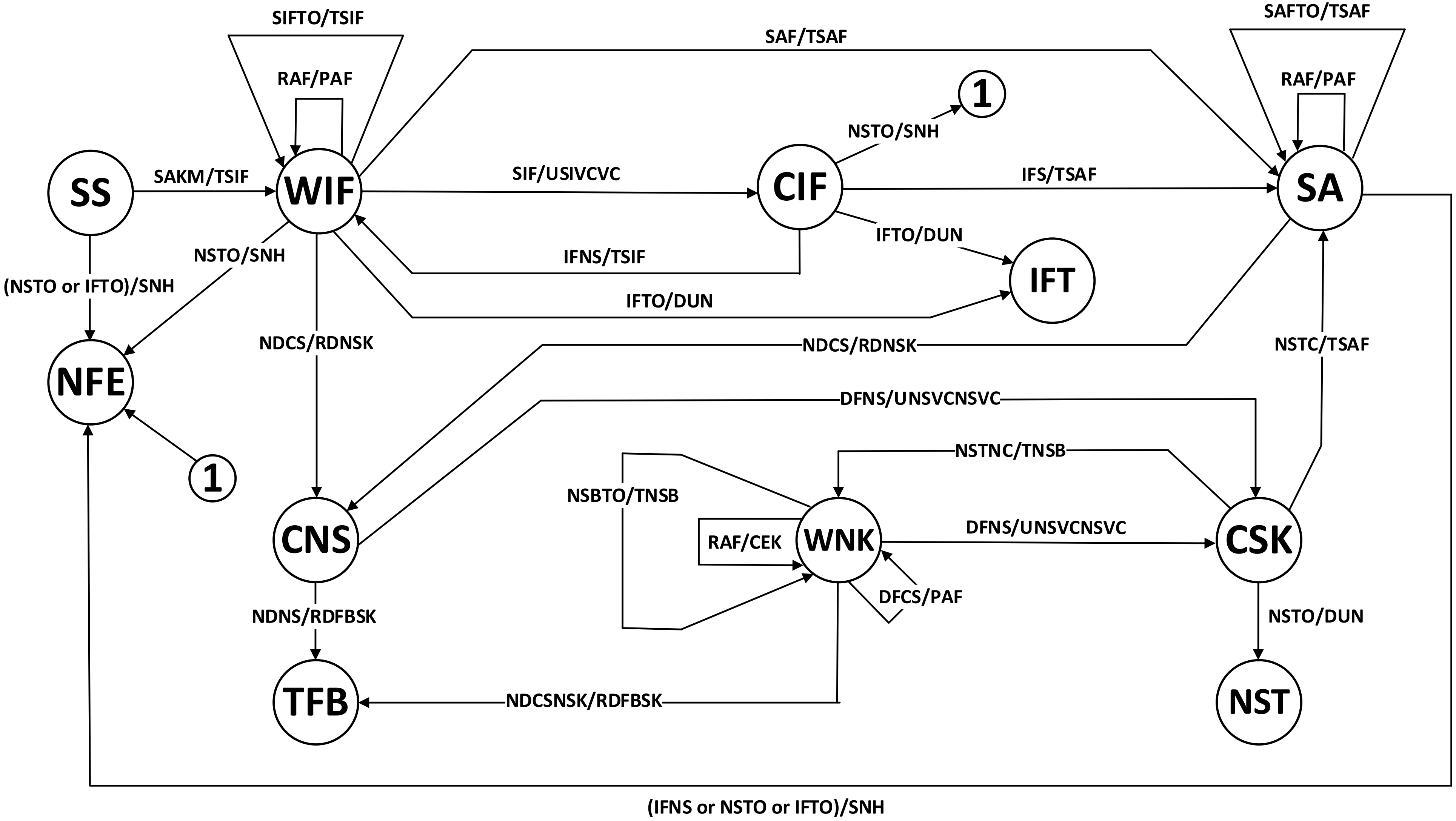
**Could NOT Decrypt Frame with NS-BEK (NDNS) Event – This event indicates that the current AFD cannot be decrypted using the next session BEK.**

# AKM FSM (Event Descriptions)

**Decrypted Frame with CS-BEK (DFCS) Event – This event indicates that the current AFD was successfully decrypted using the current session BEK.**

**Could NOT Decrypt Frame with either the CS nor NS BEK (NDCSNSK) Event – This event indicates that neither the current or next session sets of security credentials were able to decrypt the current frame.**

# AKM FSM (Updated FSM with Abbreviated State & Event Names)



# AKM FSM (Irregular Action Descriptions)

Do Nothing (DN) – This action indicates the FSM to not take any action as a result of the event/state transition process.

Process Error (ERROR) – Performs Error processing in accordance with the parameters passed into it of current state and event.

Report Exception (REPTEXCP) – Exception Processing, similar to "Process Error", but more severe. Something must be done as a consequence of this being called, whereas "Error Processing" is more of a logging of a problem, but not necessarily any action that must occur as a consequence.

Should Not Happen (SNH) – This indicates that the state machine somehow allowed an event that should never occur with the given state. Action is State/Event specific.

Deactivate Unresponsive Nodes (DUN) – Deactivate for the current session only the Edge Nodes within the ASR that have not participated in Session Initiation.

Check Encryption Key (CEK) – Checks to see if either the current session key or next session key can decrypt the frame.

Retry Decryption with Next Session Key (RDNSK) – indicates that the normal current session key does not work, so perhaps try the next session key to see if the rest of the AKM Security Relationship has started to transition to the next session.

Retry Decryption with Fallback Session Key (RDFBSK) – indicates that neither the normal current session key nor the next session key are able to decrypt the current frame, so the next logical step is to see if the Fallback Session Key is able to decrypt the frame.

# AKM FSM (Irregular Action Descriptions)

**Retry Decryption with Failsafe Session Key (RDFSSK) – indicates the current session key, the next session key, and the Fallback Session key, all failed to decrypt the frame.  Thus, the next logical step is to see if the Failsafe Session Key is able to decrypt the frame.**

**Discard Current Frame (DCF) – Indicates that the current frame should be ignored and discarded.**

# AKM FSM (Standard Action Descriptions)

**Transmit SIF (TSIF) broadcast – The Edge Node should issue a broadcast frame with the Session Initiated Flag bit set.**

**Process AKM Frame (PAF) – Process the AKM Frame, after first decrypting it.**

**Transmit SAF (TSAF) broadcast – The Edge Node should issue a broadcast frame with the Session Activated Flag bit set.**

**Transmit NS Broadcast (TNSB) frame – The Edge Node should issue a broadcast frame using the Next Session BEK.**

**Update Session Initialized Vector and Check if Session Initialized Vector is Complete (USIVCVC) – Update the current SIV with the SIV from the incoming frame and check to see if the SIV is now complete.**

**Update Next Session Vector and Check if Next Session Vector is Complete (UNSVCNSVC) – Update the current NSV with the NSV from the incoming frame and check to see if the NSV is now complete.**

# AKM FSM (Full FSM, Nominal Case)

| Context Free, Transition/Action Table | | | | | | | | | | | | | | | | | | | |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| STATE | | Frame Notification Events and Zeus Command Events | | | | | | | | | | | | | | | | | |
| | Event Source | Internal Event | AKM Frame Event | | | Broadcast Timeouts | | Anomalous Timeouts & Exceptions | | | Session Transition Related | | | | Decryption Key Related | | | | |
| ID | NAME | SAKM | RAF | SIF | SAF | SIFTO | SAFTO | IFTO | NSTO | NSBTO | IFNS | IFS | NSTNC | NSTC | NDCS | DFNS | NDNS | DFCS | NDCSNSK |
| SS | Session Start (SS) State | WIF/TSIF | 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 | NFE/SNH | NFE/SNH |
| WIF | Wait for Initialization Flag (WIF) State | NFE/SNH | WIF/PAF | CIF/USIVCVC | SA/TSAF | WIF/TSIF | NFE/SNH | IFT/DUN | NFE/SNH | NFE/SNH | NFE/SNH | NFE/SNH | NFE/SNH | NFE/SNH | CNS/RDNSK | NFE/SNH | NFE/SNH | NFE/SNH | NFE/SNH |
| CIF | Check Initialized Flag (CIF) State | NFE/SNH | NFE/SNH | NFE/SNH | NFE/SNH | NFE/SNH | NFE/SNH | IFT/DUN | NFE/SNH | NFE/SNH | WIF/TSIF | SA/TSAF | NFE/SNH | NFE/SNH | NFE/SNH | NFE/SNH | NFE/SNH | NFE/SNH | NFE/SNH |
| SA | Session Activated (SA) State | NFE/SNH | SA/PAF | NFE/SNH | NFE/SNH | NFE/SNH | SA/TSAF | NFE/SNH | NFE/SNH | NFE/SNH | NFE/SNH | NFE/SNH | NFE/SNH | NFE/SNH | CNS/RDNSK | NFE/SNH | NFE/SNH | NFE/SNH | NFE/SNH |
| IFT | Initialization Flag Timeout (IFT) State | NFE/SNH | IFT/TBD | IFT/TBD | IFT/TBD | IFT/TBD | NFE/SNH | IFT/SNH | NFE/SNH | NFE/SNH | NFE/SNH | IFT/TBD | NFE/SNH | NFE/SNH | NFE/SNH | NFE/SNH | NFE/SNH | NFE/SNH | NFE/SNH |
| CNS | Check Next Session (CNS) 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 | CSK/UNSVCNSVC | EFB/RDFBSK | NFE/SNH | NFE/SNH |
| CSK | Check Session Key (CSK) State | NFE/SNH | NFE/SNH | NFE/SNH | NFE/SNH | NFE/SNH | NFE/SNH | NFE/SNH | NST/DUN | NFE/SNH | NFE/SNH | NFE/SNH | WNK/TNSB | SA/TSAF | NFE/SNH | NFE/SNH | NFE/SNH | NFE/SNH | NFE/SNH |
| WNK | Wait for Next Session Key (WNK) State | NFE/SNH | WNK/CEK | NFE/SNH | NFE/SNH | NFE/SNH | NFE/SNH | NFE/SNH | NFE/SNH | WNK/TNSB | NFE/SNH | NFE/SNH | NFE/SNH | NFE/SNH | NFE/SNH | CSK/UNSVCNSVC | NFE/SNH | WNK/PAF | EFB/RDFBSK |
| NST | Next Session Timeout (NST) State | NFE/SNH | NFE/SNH | NFE/SNH | NFE/SNH | NFE/SNH | NFE/SNH | NFE/SNH | NFE/SNH | NST/TBD | NFE/SNH | NFE/SNH | NFE/SNH | NFE/SNH | NFE/SNH | NFE/SNH | NFE/SNH | NFE/SNH | NFE/SNH |
| EFB | Enter FallBack (EFB) State | NFE/SNH | NFE/SNH | NFE/SNH | NFE/SNH | NFE/SNH | NFE/SNH | NFE/SNH | NFE/SNH | EFB/TBD | NFE/SNH | NFE/SNH | NFE/SNH | NFE/SNH | NFE/SNH | NFE/SNH | NFE/SNH | NFE/SNH | NFE/SNH |
| NFE | Non-Fatal Exception (EFB) 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 | NFE/SNH | NFE/SNH | NFE/SNH |

**This is the full FSM for the nominal case representing the AKM communication FSM coming out of power-on/reset as well as the transition to next session security credentials. The top half of the FSM diagram represents coming out of Power-on/Reset. The bottom half represents the transition from the current session security credentials to the next session security credentials.**

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

1) **Loss of Synch (that is represented by the EFB circle and will be built out next).**

2) **Adding/Deleting a Node (to be built out after “Loss of Synch” FSM is completed. The mechanics for “hot-swap” are very similar to the mechanics of the state transition between current session credentials and next session credentials.**

# AKM FSM (Full FSM, Nominal Case-Current Session BEK)

## Context Free, Transition/Action Table

| STATE | | Frame Notification Events and Zeus Command Events | | | | | | | | |
|---|---|---|---|---|---|---|---|---|---|---|
| | Event Source | Internal Event | AKM Frame Event | | | Broadcast Timeouts | | Anomalous Timeouts & Exceptions | | |
| ID | NAME | SAKM | RAF | SIF | SAF | SIFTO | SAFTO | IFTO | NSTO | NSBTO |
| | | | | | | | | | | |
| SS | Session Start (SS) State | WIF/TSIF | NFE/SNH | NFE/SNH | NFE/SNH | NFE/SNH | NFE/SNH | NFE/SNH | NFE/SNH | NFE/SNH |
| WIF | Wait for Initialization Flag (WIF) State | NFE/SNH | WIF/PAF | CIF/USIVCVC | SA/TSAF | WIF/TSIF | NFE/SNH | IFT/DUN | NFE/SNH | NFE/SNH |
| CIF | Check Initialized Flag (CIF) State | NFE/SNH | NFE/SNH | NFE/SNH | NFE/SNH | NFE/SNH | NFE/SNH | IFT/DUN | NFE/SNH | NFE/SNH |
| SA | Session Activated (SA) State | NFE/SNH | SA/PAF | NFE/SNH | NFE/SNH | NFE/SNH | SA/TSAF | NFE/SNH | NFE/SNH | NFE/SNH |
| IFT | Initialization Flag Timeout (IFT) State | NFE/SNH | IFT/TBD | IFT/TBD | IFT/TBD | IFT/TBD | NFE/SNH | IFT/SNH | NFE/SNH | NFE/SNH |
| | | | | | | | | | | |
| | | | | | | | | | | |
| CNS | Check Next Session (CNS) State | NFE/SNH | NFE/SNH | NFE/SNH | NFE/SNH | NFE/SNH | NFE/SNH | NFE/SNH | NFE/SNH | NFE/SNH |
| CSK | Check Session Key (CSK) State | NFE/SNH | NFE/SNH | NFE/SNH | NFE/SNH | NFE/SNH | NFE/SNH | NFE/SNH | NST/DUN | NFE/SNH |
| WNK | Wait for Next Session Key (WNK) State | NFE/SNH | WNK/CEK | NFE/SNH | NFE/SNH | NFE/SNH | NFE/SNH | NFE/SNH | NFE/SNH | WNK/TNSB |
| NST | Next Session Timeout (NST) State | NFE/SNH | NFE/SNH | NFE/SNH | NFE/SNH | NFE/SNH | NFE/SNH | NFE/SNH | NFE/SNH | NST/TBD |
| EFB | Enter FallBack (EFB) State | NFE/SNH | NFE/SNH | NFE/SNH | NFE/SNH | NFE/SNH | NFE/SNH | NFE/SNH | NFE/SNH | EFB/TBD |
| NFE | Non-Fatal Exception (EFB) State | NFE/SNH | NFE/SNH | NFE/SNH | NFE/SNH | NFE/SNH | NFE/SNH | NFE/SNH | NFE/SNH | NFE/SNH |
| | | | | | | | | | | |

# AKM FSM (Full FSM, Nominal Case-Next Session State Transition)

## Context Free, Transition/Action Table

| STATE | | Frame Notification Events and Zeus Command Events | | | | | | | | |
|---|---|---|---|---|---|---|---|---|---|---|
| | Event Source | Session Transition Related | | | | Decryption Key Related | | | | |
| ID | NAME | IFNS | IFS | NSTNC | NSTC | NDCS | DFNS | NDNS | DFCS | NDCSNSK |
| | | | | | | | | | | |
| SS | Session Start (SS) State | NFE/SNH | NFE/SNH | NFE/SNH | NFE/SNH | NFE/SNH | NFE/SNH | NFE/SNH | NFE/SNH | NFE/SNH |
| WIF | Wait for Initialization Flag (WIF) State | NFE/SNH | NFE/SNH | NFE/SNH | NFE/SNH | CNS/RDNSK | NFE/SNH | NFE/SNH | NFE/SNH | NFE/SNH |
| CIF | Check Initialized Flag (CIF) State | WIF/TSIF | SA/TSAF | NFE/SNH | NFE/SNH | NFE/SNH | NFE/SNH | NFE/SNH | NFE/SNH | NFE/SNH |
| SA | Session Activated (SA) State | NFE/SNH | NFE/SNH | NFE/SNH | NFE/SNH | CNS/RDNSK | NFE/SNH | NFE/SNH | NFE/SNH | NFE/SNH |
| IFT | Initialization Flag Timeout (IFT) State | NFE/SNH | IFT/TBD | NFE/SNH | NFE/SNH | NFE/SNH | NFE/SNH | NFE/SNH | NFE/SNH | NFE/SNH |
| | | | | | | | | | | |
| | | | | | | | | | | |
| CNS | Check Next Session (CNS) State | NFE/SNH | NFE/SNH | NFE/SNH | NFE/SNH | NFE/SNH | CSK/UNSVCNSVC | EFB/RDFBSK | NFE/SNH | NFE/SNH |
| CSK | Check Session Key (CSK) State | NFE/SNH | NFE/SNH | WNK/TNSB | SA/TSAF | NFE/SNH | NFE/SNH | NFE/SNH | NFE/SNH | NFE/SNH |
| WNK | Wait for Next Session Key (WNK) State | NFE/SNH | NFE/SNH | NFE/SNH | NFE/SNH | NFE/SNH | CSK/UNSVCNSVC | NFE/SNH | WNK/PAF | EFB/RDFBSK |
| NST | Next Session Timeout (NST) State | NFE/SNH | NFE/SNH | NFE/SNH | NFE/SNH | NFE/SNH | NFE/SNH | NFE/SNH | NFE/SNH | NFE/SNH |
| EFB | Enter FallBack (EFB) State | NFE/SNH | NFE/SNH | NFE/SNH | NFE/SNH | NFE/SNH | NFE/SNH | NFE/SNH | NFE/SNH | NFE/SNH |
| NFE | Non-Fatal Exception (EFB) State | NFE/SNH | NFE/SNH | NFE/SNH | NFE/SNH | NFE/SNH | NFE/SNH | NFE/SNH | NFE/SNH | NFE/SNH |
| | | | | | | | | | | |