| | | | |
|---|---|---|---|
| Project | **IEEE 802.16 Broadband Wireless Access Working Group** <http://ieee802.org/16> | | |
| Title | **TEK generation and update for Handover** | | |
| Date Submitted | **2008-03-17** | | |
| Source(s) | Kyeong-Tae Do<br>Eun-Sun Jung<br>Geunhwi Lim<br>Samsung Electronics Co., LTD | Voice:<br>E-mail: | +82-31-279-5748<br>kyeongtae.do@samsung.com<br>esleon.jung@samsung.com |
| Re: | LB 26b | | |
| Abstract | The effort to reduce the HO latency is currently being discussed. Main idea is to exchange in the serving BS the information which is required at the target BS. This contribution suggests the way of sharing TEKs. | | |
| Purpose | Accept the proposed specification changes on IEEE P802.16Rev2/D*2* | | |
| Notice | *This document does not represent the agreed views of the IEEE 802.16 Working Group or any of its subgroups*. It represents only the views of the participants listed in the "Source(s)" field above. It is offered as a basis for discussion. It is not binding on the contributor(s), who reserve(s) the right to add, amend or withdraw material contained herein. | | |
| Release | The contributor grants a free, irrevocable license to the IEEE to incorporate material contained in this contribution, and any modifications thereof, in the creation of an IEEE Standards publication; to copyright in the IEEE's name any IEEE Standards publication even though it may include portions of this contribution; and at the IEEE's sole discretion to permit others to reproduce in whole or in part the resulting IEEE Standards publication. The contributor also acknowledges and accepts that this contribution may be made public by IEEE 802.16. | | |
| Patent Policy | The contributor is familiar with the IEEE-SA Patent Policy and Procedures:<br><http://standards.ieee.org/guides/bylaws/sect6-7.html#6> and<br><http://standards.ieee.org/guides/opman/sect6.html#6.3>.<br>Further information is located at <http://standards.ieee.org/board/pat/pat-material.html> and <http://standards.ieee.org/board/pat>. | | |

# TEK generation and update for Handover

*Samsung Electronics.*

## Introduction – Problem Description

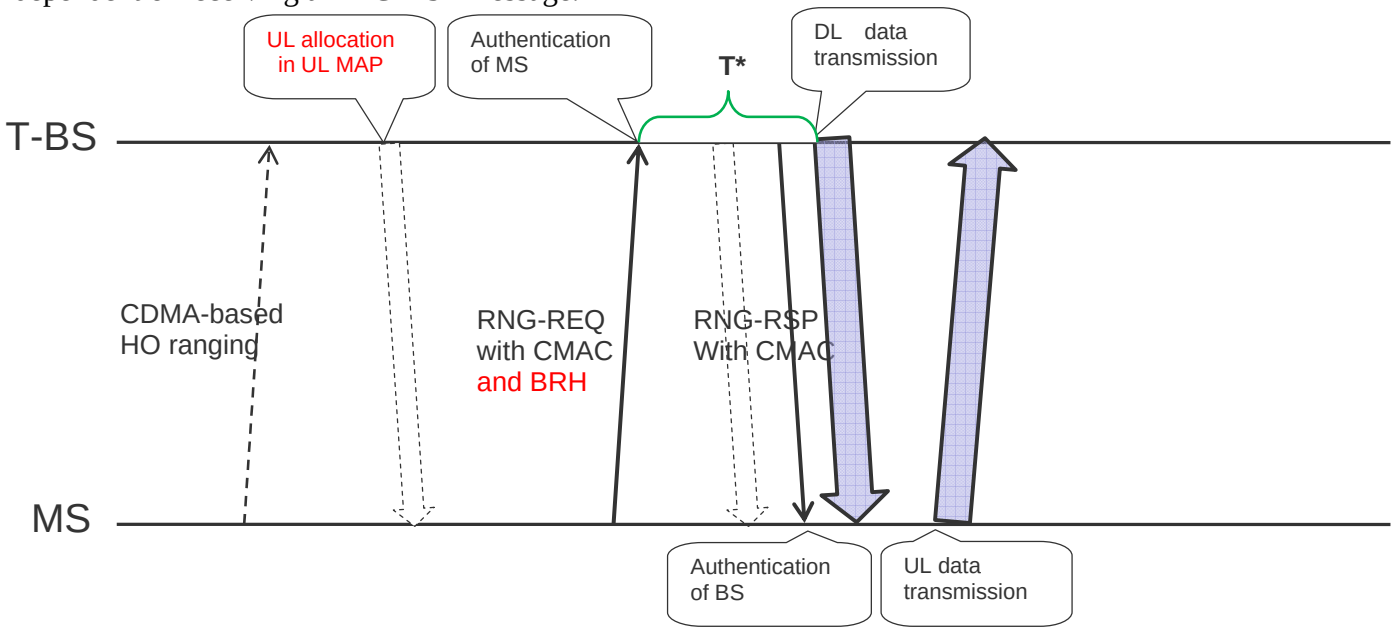
The method to reduce the HO latency is being discussed currently. The MS needs to receive the necessary information to communicate with the target BS after HO. Normally the MS receives it from the RNG-RSP message sent from the target BS as a response to a RNG-REQ message.

One of the requirements to communicate with the target BS is TEKs when the data is encrypted and transmitted. Currently, the TEKs are updated after the MS receives a RNG-RSP message which includes SA-TEK-Update TLV or SA-Challenge Tuple TLV. If the MS is required to receive data without regard to the receipt of the RNG-RSP, the TEKs shall be delivered to the MS before the traffic data is sent. If the TEKs used at the serving BS can continuously be used at the target BS, the TEKs need not to be sent to the MS. But, this method increases the possibility to compromise the connection between the BS and the MS and requires the transmission of the PN windows for AES-CCM encryption. Thus, it is needed to share TEKs, prior to the transmission of data, which will expedite data transmission after HO.

## Proposed Solution

In the current system, the BS sends encrypted TEKs to the MS directly. During the HO, new TEKs are transmitted from the target BS to the MS or the TEKs used at the serving BS shall be used continuously. If the MS receives from the serving BS the new TEKs which are going to be used at the target BS, it is less secure than receiving new TEKs at the target BS.

This contribution is based on the expedited HO scenario which enables the transmission of traffic data independent of receiving a RNG-RSP message.




In this scenario, the BS can authenticate MS by validating the CMAC-Tuple of received RNG-REQ message, allocate UL burst and send downlink traffic data. Above scenario does not include the method of TEK sharing.

In this document, we suggest changing current TEK delivery scheme to share the TEKs at the target BS. We suggest that The TEK nonces, not TEKs, should be exchanged during the network entry and TEK refresh. When TEK encryption algorithm is “generate TEKs with TEK materials” which is newly added for this scenario, PKMv2 Key-Material-Request and Key-Material-Reply messages are exchanged instead of PKMv2 Key-Request/Reply messages. PKMv2 Key-Material-Reply message includes TEK nonces which are used to generate TEKs. After exchanging these messages, both MS and BS generate TEKs separately. Upon expiration of TEK refresh timer, PKMv2 Key-Material-Request and Key-Material-Reply messages are exchanged to deliver TEK nonces.

During the HO, the latest TEK nonces at the serving BS are transferred to the target BS. The target BS generates new TEKs with the TEK nonces from the serving BS and TEK counter which is incremented for every HO trial. TEK counter prevents from using the same TEKs in the case the MS performs handover to the BS previously visited. When CMAC is supported, CMAC Key Count is used for TEK counter. This scenario does not need to expose the new TEKs to the serving BS. Another preparation for TEK sharing scheme is not needed either.

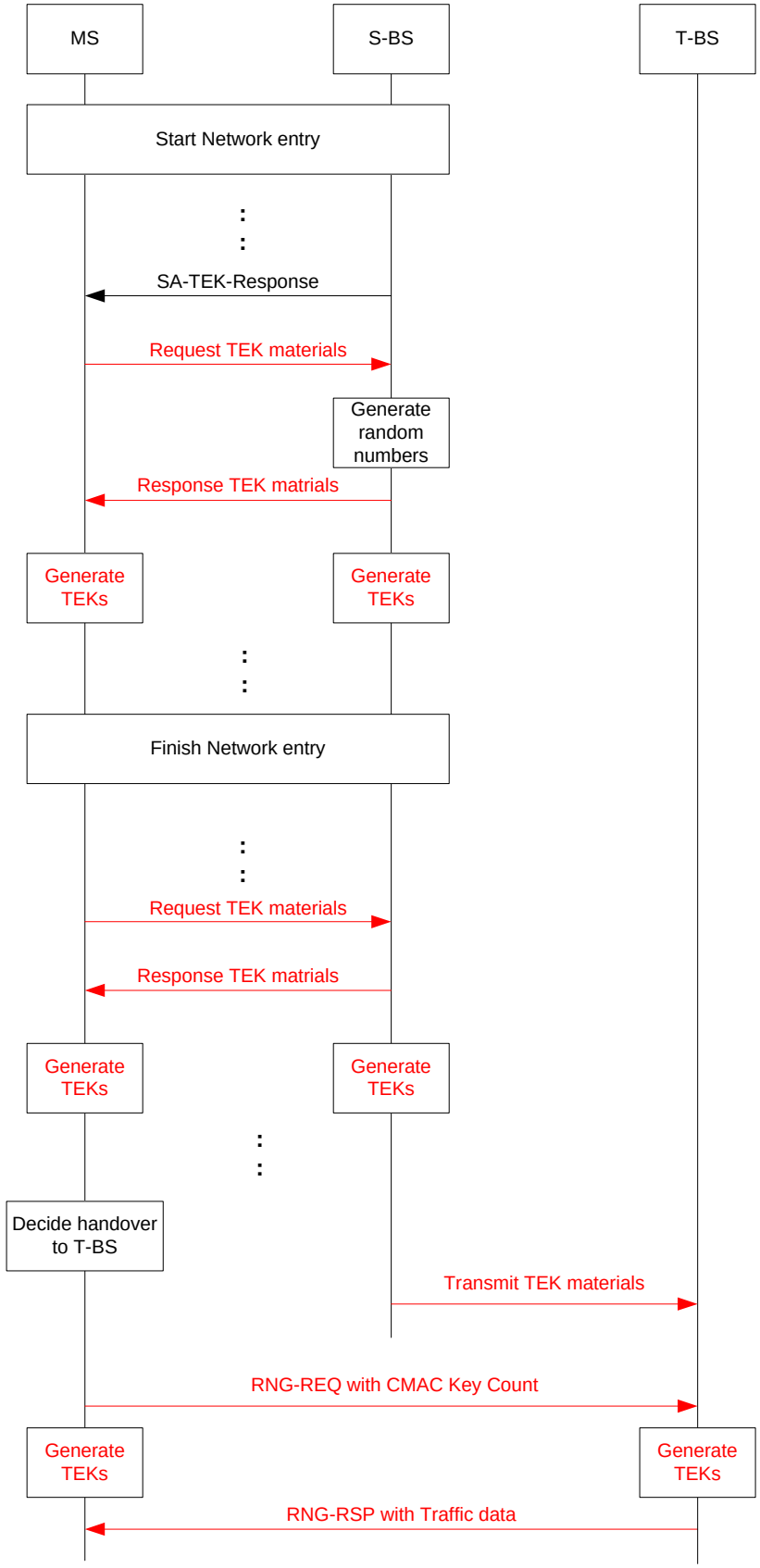



**Figure. Proposed TEK exchange scheme**

An example of generation of TEK is shown below.

Old TEK = Dot16KDF(KEK, SS MAC Address | BSID | Old TEK nonce | TEK Counter, 128)
New TEK = Dot16KDF(KEK, SS MAC Address | BSID | New TEK nonce | TEK Counter, 128)
where TEK Counter is a 16-bit counter and incremented for every HO trial or re-entry from idle mode.

## Proposed Text Changes

***Modify Table 102 in 6.3.2.3.9 as indicated:***

**Table 48—PKM message codes**

| Code | PKM message type | MAC management message type |
|---|---|---|
| … | … | … |
| 33 | MIH Comeback Response | PKM-RSP |
| 34 | PKMv2 Key Material Request | PKM-REQ |
| 35 | PKMv2 Key Material Reply | PKM-RSP |
| ~~34~~36-255 | *Reserved* | — |

***Add following sections after 6.3.2.3.9.31 as indicated:***

**6.3.2.3.9.32 PKMv2 Key-Material-Request message**

An MS sends PKMv2 Key-Material-Request message to the BS to request key materials in order to generate TEKs.

Code: 34
Attributes are shown in Table xx.

Table xx – PKMv2 Key-Material-Request message attributes

| Attribute | Contents |
|---|---|
| Key Sequence Number | AK sequence number |
| SAID | Security association identifier |
| HMAC/CMAC Digest | Message digest calculated using AK |

The HMAC/CMAC Digest attribute shall be the final attribute in the message's attribute list.

Inclusion of the HMAC/CMAC Digest attribute allows the MS and BS to authenticate the PKMv2 Key-Material-Request message. The HMAC/CMAC Digest attribute's authentication key is derived from the AK.

**6.3.2.3.9.33 PKMv2 Key-Material-Reply message**

The BS sends this message to the MS to deliver key materials in order to generate and manage TEKs as a

response to a PKMv2 Key-Material-Request message.

Code: 35
Attributes are shown in Table xy.

Table xy – PKMv2 Key-Material-Reply message attributes

| Attribute | Contents |
|---|---|
| Key Sequence Number | AK sequence number |
| SAID | Security association identifier |
| TEK-Materials | Older generation of TEK materials relevant to SAID |
| TEK-Materials | Newer generation of TEK materials relevant to SAID |
| HMAC/CMAC Digest | Message digest calculated using AK |

The TEK-Materials attribute is a compound attribute containing all the keying material corresponding to a particular generation of an SAID's TEK. This would include the TEK nonce, the TEK's remaining key lifetime, and its key sequence number. The TEK is generated. See 7.2.2.2.6 for details.

One set corresponds to the "older" generation of keying material; the second set corresponds to the "newer" generation of keying material. The newer generation has a key sequence number one greater than (modulo 4) that of the older generation. The BS distributes to a client SS both generations of active keying material. Thus, the Key Material Reply message contains two TEK-Materials attributes, each containing the keying material for one of the SAID's two active sets of keying material.

The HMAC/CMAC Digest attribute shall be the final attribute in the message's attribute list.

Inclusion of the HMAC/CMAC Digest attribute allows the MS and BS to authenticate the PKMv2 Key-Material-Reply message. The HMAC/CMAC Digest attribute's authentication key is derived from the AK.

## ***Modify the 5th paragraph of 6.3.22.2.8.1.6.6 as indicated***

Bit #1=1 AND bit#2=0: One of ~~two~~three options is allowed but option 1 and 2 are recommended:
Option 1: SA-TEK-Update TLV is included in the RNG-RSP message and updates the TEKS for all the SAs. In this way SA-TEK 3-way handshake shall not occur. SA Challenge Tuple TLV shall not be included in the RNG-RSP message.
Option 2: Neither SA-TEK-Update TLV nor SA-Challenge Tuple TLV is included in the RNG-RSP message. TEKs are generated using TEK nonces. In this case, the TEK encryption algorithm shall be "generate TEKs with TEK materials".
Option ~~2~~3: SA-TEK-Update TLV is included in a SA-TEK-Response message. In this case, SATEK 3-way handshake is performed with SA Challenge Tuple TLV included in the RNG-RSP message.

## ***Modify 7.2.2.2.6 as indicated:***

### 7.2.2.2.6 Traffic encryption key (TEK)

The TEK is generated as a random number in the BS and is encrypted using the corresponding TEK

encryption algorithm (e.g., AES key wrap for SAs with TEK encryption algorithm identifier in the cryptographic suite is equal to 0x04), keyed with the KEK and transferred between BS and SS in the TEK exchange.

Or, the TEK is generated by BS and SS based on the exchanged random number when the TEK encryption algorithm is “generate TEKs with TEK materials”.
The TEKs are generated as follows:

Old TEK = Dot16KDF(KEK, SS MAC Address | BSID | Old TEK nonce | TEK Counter, 128)
New TEK = Dot16KDF(KEK, SS MAC Address | BSID | New TEK nonce | TEK Counter, 128)
where TEK Counter is a 16-bit counter and incremented for every HO trial or re-entry from idle mode.
When CMAC is supported for message authentication, CMAC_KEY_COUNT is used as TEK Counter. When CMAC is not supported, TEK Counter is reset when the nonces are refreshed. Old/New TEK nonces are the ones included in the old/new TEK-Materials.

When TEK encryption algorithm identifier is 5 (generate TEKs with TEK materials), PKMv2 Key-Material-Request/Reply messages are used to generate TEKs for network entry and periodic key refresh. Otherwise, PKMv2 Key-Request/Reply messages are exchanged.

### 7.2.2.2.6.1 Nonce-based TEK update for HO or re-entry from Idle mode

The latest TEK nonces and key sequence numbers used at the serving BS are also used at the target BS to generate TEKs after HO. The target BS shall have the TEK nonces from the serving BS when the MS performs handover. The TEK nonces at the BS may not be the same as the ones at the MS due to the expiration of old TEK. The BS shall include TEK sequence numbers in the RNG-RSP message in order for the MS to check TEKs and trigger TEK refresh. The TEK lifetimes at the serving BS and the target BS are the same and TEK refresh timer is restarted at the target BS and MS after HO.
When the MS tries to handover to a new BS, it shall increase the TEK Counter. The TEK Counter is an input for TEK generation and shall be included in the RNG-REQ to be synchronized with the BS. When the CMAC is supported as a MAC (message authentication code) mode, the CMAC_KEY_COUNT is used as TEK Counter. If MS moves around and performs HO frequently, the same nonces are continuously used to generate TEKs which is not secure. The MS should refresh the nonces by exchanging Key-Material-Request/Reply messages The same nonces should not be used more than TekNonceMaxUsage times in order to generate TEKs.

The TEK nonces should be shared between BSs, but the target BS may not be able to share them. In this case, the BS sends RNG-RSP with SA-TEK-Update TLV where Old TEK-Materials and New TEK-Materials are used instead of Old TEK/GTEK-Parameters and New TEK/GTEK-Parameters. The BS shall not transmit downlink traffic together with RNG-RSP when SA-TEK-Update TLV is included in the RNG-RSP message.

During the network re-entry from Idle mode, the procedure of nonce exchange is the same as that of HO.

***Modify 8th paragraph of 7.2.2.5.1 as indicated:***

*Reentry Authentication Wait*: In this state the Authorization FSM has the AK context of the target BS. The MS should have the AK context of the target BS in this state before it sends a RNG-REQ message with H/CMAC Tuple during HO or reentry. During HO or reentry, the Authorization FSM is in this state when the MS sends a

RNG-REQ message. The state of Authorization FSM changes when the MS receives a RNGRSP message. The next state depends on the value of HO Process Optimization TLV included in the received RNG-RSP message. If HO Process Optimization Bit #1 set to zero, meaning the PKM Authentication phase is not omitted, the Authorization FSM receives Start Authentication event which triggers to stop all the TEK FSMs, re-initialize the Authorization FSM and change the state to Not Authenticated. The TLVs included in the RNG-RSP message also affects the next state. If HO Process Optimization Bit #1 and Bit #2 set to one and zero respectively and the SA-TEK-Update TLV is included in the RNG-RSP, the FSM receives Reentry Completed event. If HO Process Optimization Bit #1 and Bit #2 set to one and zero respectively and the SA-TEK-Update TLV is not included in the RNG-RSP, the FSM receives Reentry Completed event after generating TEKs using TEK nonces. The state of the Authorization FSM changes to Authenticated when the Reentry Completed event is issued. In the case HO Process Optimization Bit #1 and Bit #2 set to one and zero respectively and the SA-Challenge Tuple TLV is included in the RNG-RSP, the next state is Reentry SA-TEK-Response Wait.

## ***Modify 7.2.2.6 as indicated:***

The TEK state machine consists of ~~seven~~five states and ~~eleven~~ten events (including receipt of messages) that may trigger state transitions. Like the Authorization state machine, the TEK state machine is presented in both a state flow diagram (Figure 164) and a state transition matrix (Table 206). As was the case for the Authorization state machine, the state transition matrix shall be used as the definitive specification of protocol actions associated with each state transition.

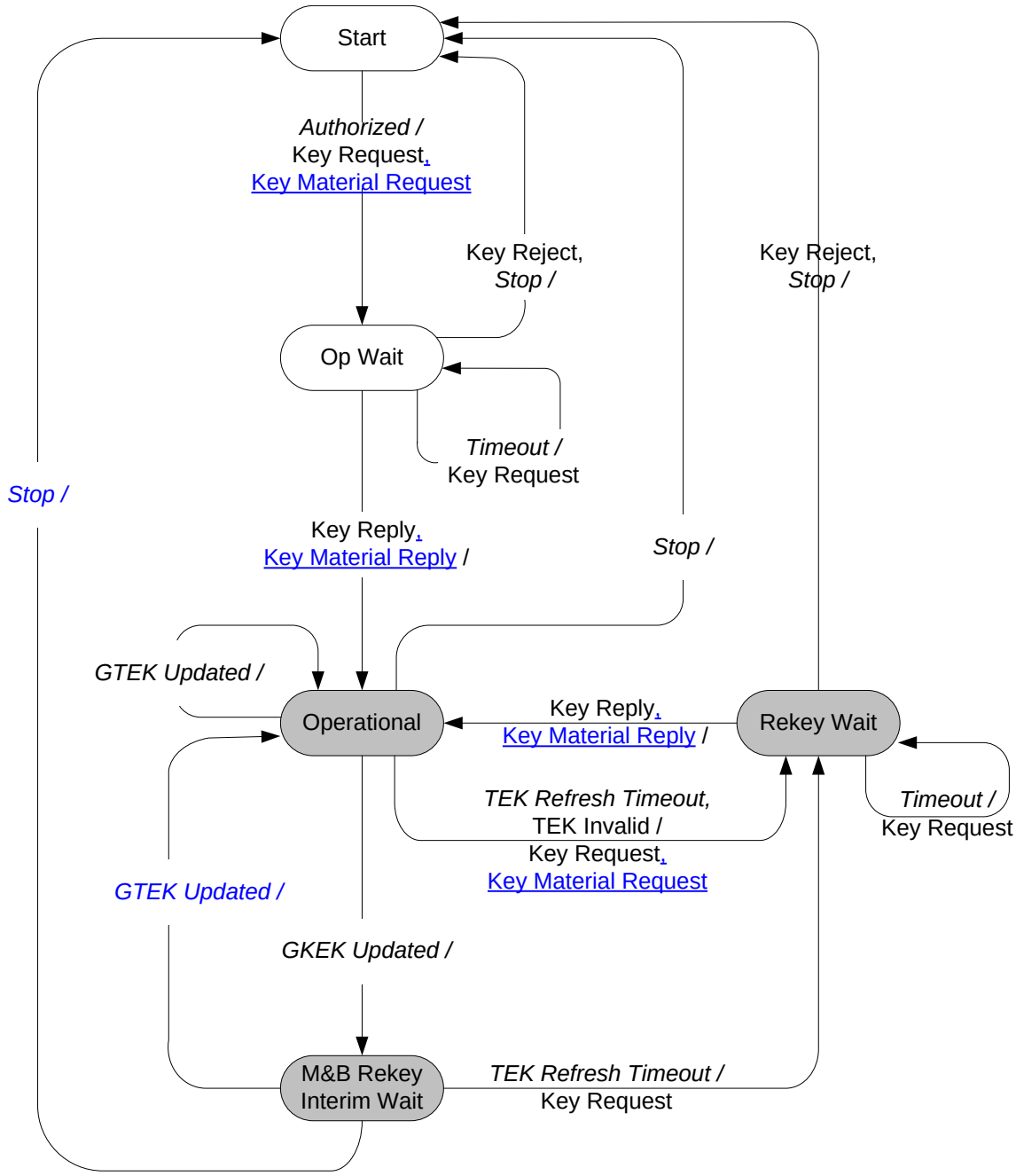



**Figure 164 – TEK state machine flow diagram**

Shaded states in Figure 164 (Operational, Rekey Wait, ~~Rekey Reauthorize Wait,~~ and M&B Rekey Interim Wait) have valid keying material and encrypted traffic may be sent.

The SAID may be replaced by the GSAID for the multicast service or the broadcast service. And, the TEK may be also replaced by the GTEK for the multicast service or the broadcast service.

The Authorization state machine starts an independent TEK state machine for each of its authorized SAIDs. As mentioned in 7.2.2, the BS maintains two active TEKs per SAID.

For the unicast service, either PKMv2 Key-Request/Reply or PKMv2 Key-Material-Request/Reply messages are used. PKMv2 Key-Material-Request/Reply messages are for TEK encryption algorithm with "generate TEKs with TEK Materials". Otherwise, PKMv2 Key-Request/Reply messages are used and the BS includes in its Key Replies both of these TEKs, along with their remaining lifetimes. The BS encrypts DL traffic with the older of its two TEKs and decrypts UL traffic with either the older or newer TEK, depending upon which of the two keys the SS was using at the time. The SS encrypts UL traffic with the newer of its two TEKs and decrypts DL traffic with either the older or newer TEK, depending upon which of the two keys the BS was using at the time. See 7.3 for details on SS and BS key usage requirements.

| **State Event or Rcvd Message** | **(A) Start** | **(B) Op Wait** | **~~(C) Op Reauth Wait~~** | **(~~D~~C) Op** | **(~~E~~D) Rekey Wait** | **~~(F) Rekey Reauth Wait~~** | **(~~G~~E) M&B Rekey Interim Wait** |
|---|---|---|---|---|---|---|---|
| (1) *Stop* | | Start | ~~Start~~ | Start | Start | ~~Start~~ | Start |
| (2) *Authorized* | Op Wait | | | | | | |
| ~~(3) *Auth Pend*~~ | | ~~Op Reauth Wait~~ | | | ~~Rekey Reauth Wait~~ | | |
| ~~(4) *Auth Comp*~~ | | | ~~Op Wait~~ | | | ~~Rekey Wait~~ | |
| (~~5~~3) *TEK Invalid* | | | | Rekey Wait | | | |
| (~~6~~4) *Timeout* | | Op Wait | | | Rekey Wait | | |
| (~~7~~5) *TEK Refresh Timeout* | | | | Rekey Wait | | | Rekey Wait |
| (~~8~~6) *Key Reply* | | Operational | | | Operational | | |
| (7) *Key Material Reply* | | Operational | | | Operational | | |
| (~~9~~8) *Key Reject* | | Start | | | Start | | |
| (~~10~~9) *GKEK Updated* | | | | M&B Rekey Interim Wait | | | |
| (~~11~~10) *GTEK Updated* | | | | | | | Operational |

**Table 206 – TEK FSM state transition matrix for PKMv2**

## ***Modify 7.2.2.6 as indicated:***

**7.2.2.6.5 Actions**

Actions taken in association with state transitions are listed by <event> (<rcvd message>) --> <state>:

1-B Op Wait (Stop) → Start
a) Clear Key Request retry timer
b) Terminate TEK FSM

~~1-C Op Reauth Wait (Stop) → Start~~
~~a) Terminate TEK FSM~~

1-~~D~~C Operational (Stop) → Start
a) Clear TEK refresh timer, which is timer set to go off "TEK Grace Time" seconds prior to the TEK's scheduled expiration time
b) Terminate TEK FSM
c) Remove SAID keying material from key table

1-~~E~~D Rekey Wait (Stop) → Start
a) Clear Key Request retry timer
b) Terminate TEK FSM
c) Remove SAID keying material from key table

~~1-F Rekey Reauth Wait (Stop) → Start~~
~~a) Terminate TEK FSM~~
~~b) Remove SAID keying material from key table~~

1-F M&B Rekey Interim Wait (Stop) → Start
a) Terminate TEK FSM
b) Remove SAID keying material from key table

2-A Start (Authorized) → Op Wait
a) Send Key Request message to BS
b) Set Key Request retry timer to Operational Wait Timeout

~~3-B Op Wait (Auth Pend) → Op Reauth Wait~~
~~a) Clear Key Request retry timer~~

~~3-E Rekey Wait (Auth Pend) → Rekey Reauth Wait~~
~~a) Clear Key Request retry timer~~

~~4-C Op Reauth Wait (Auth Comp) → Op Wait~~
~~a) Send Key Request message to BS~~
~~b) Set Key Request retry timer to Operational Wait Timeout~~

~~4-F Rekey Reauth Wait (Auth Comp) → Rekey Wait~~
~~a) Send Key Request message to BS~~
~~b) Set Key Request retry timer to Rekey Wait Timeout~~

~~5-D~~3-C Operational (TEK Invalid) → Rekey_Wait
a) Send a Key Request message to BS
b) Set Key Request retry timer to Rekey Wait Timeout

~~6~~4-B Op Wait (Timeout) → Op Wait
a) Send Key Request message to BS
b) Set Key Request retry timer to Operational Wait Timeout

~~6-E~~4-D Rekey Wait (Timeout) → Rekey Wait
a) Send Key Request message to BS
b) Set Key Request retry timer to Rekey Wait Timeout

~~7-D~~5-C Operational (TEK Refresh Timeout) → Rekey Wait
a) Send Key Request message to BS
b) Set Key Request retry timer to Rekey Wait Timeout

~~7-G~~5-E M&B Rekey Interim Wait (TEK Refresh Timeout) -> Rekey Wait
a) Send Key Request message to BS
b) Set Key Request retry timer to Rekey Wait Timeout

~~8~~6-B Op Wait (Key Reply) → Operational
a) Clear Key Request retry timer
b) Process contents of Key Reply message and incorporate new keying material into key database
c) Set the TEK refresh timer to go off “TEK Grace Time” seconds prior to the newer key’s scheduled expiration

~~8-E~~6-D Rekey Wait (Key Reply) → Operational
a) Clear Key Request retry timer
b) Process contents of Key Reply message and incorporate new keying material into key database
c) Set the TEK refresh timer to go off “TEK Grace Time” seconds prior to the newer key’s scheduled expiration

7-B Op Wait (Key Material Reply) → Operational
a) Clear Key Request retry timer
b) Process contents of Key Material Reply message and incorporate new keying material into key database
c) Set the TEK refresh timer to go off “TEK Grace Time” seconds prior to the newer key’s scheduled expiration

7-D Rekey Wait (Key Material Reply) → Operational
a) Clear Key Request retry timer
b) Process contents of Key Material Reply message and incorporate new keying material into key database
c) Set the TEK refresh timer to go off “TEK Grace Time” seconds prior to the newer key’s scheduled

expiration

~~9~~8-B Op Wait (Key Reject) → Start
a) Clear Key Request retry timer
b) Terminate TEK FSM

~~9-E~~8-D Rekey Wait (Key Reject) → Start
a) Clear Key Request retry timer
b) Terminate TEK FSM
c) Remove SAID keying material from key table

~~10-D~~9-C Operational (GKEK Updated) -> M&B Rekey Interim Wait
a) Process contents of PKMv2 Group-Key-Update-Command message for the GKEK update mode and incorporate new GKEK into key database

~~11-G~~10-E M&B Rekey Interim Wait (GTEK Updated) -> Operational
a) Clear Key Request retry timer
b) Process contents of PKMv2 Group-Key-Update-Command message for the GTEK update mode and incorporate new traffic keying material into key database
c) Set the TEK refresh timer to go off "TEK Grace Time" seconds prior to the key's scheduled expiration

***Modify 7.8.1 as indicated:***

b) If HO Process Optimization Bit #1 is set to 1 indicating that PKM Authentication phase is omitted and HO Process Optimization Bit #2 is set to 0 during network re-entry or handover, the BS has three options to update TEKs. First two options are recommended. One is BS updates TEKs by appending the SA-TEK-Update TLV to RNG-RSP message. Another option is to compute TEKs with TEK nonces which was received from the serving BS. The other option is to ~~either by~~ begin~~ning~~ the 3-way-handshake, by including the SA Challenge Tuple TLV to the RNG-RSP which is not recommended.~~or by appending the SA-TEK-Update TLV to RNG-RSP message.~~ In case the BS begins 3-wayhandsake, if the BS does not receive PKMv2 SA-TEK-Request from the MS within SaChallengeTimer, it may initiate full re-authentication or drop the MS. If the BS receives an initial RNGREQ during the period that PKMv2 SA-TEK-Request is expected, it shall send a new RNG-RSP with another SA-Challenge Tuple TLV.

***Modify 11.1.10 as indicated:***
***[In the 3rd and 4th paragraphs]***

Additionally, in case of HO, for each active SA in previous serving BS, corresponding TEK, GTEK, and GKEK parameters are also included. Thus, SA_TEK_Update provides a shorthand method for renewing active SAs used by the MS in its previous serving BS. The TLVs specify SAID in the target BS that shall replace active SAID used in the previous serving BS and also "older" TEK-Parameters and "newer" TEK Parameters relevant to the active SAIDs. The update may also include multicast/broadcast Group SAIDs (GSAIDs) and associated GTEK-Parameter pairs. When TEKs are generated at the BS and MS (e.g. TEK encryption algorithm is "generate TEKs with TEK materials"), TEK-Materials replace TEK-Parameters. The new SAID field shall refer to SAID assignments by the new BS. The mapping of these new SAIDs to the

SAIDs assigned by the previous serving BS is controlled by the SAID Update TLV (11.7.18) and is further controlled by the rules for SAID updating outlined in section 6.3.22.2.8.1.6.6.

In case of unicast SAs, the TEK-Parameters attribute contains all of the keying material corresponding to a particular generation of a SAID's TEK. T~~H~~his would include the TEK, the TEK's remaining key lifetime, its key sequence number, and the cipher block chaining (CBC) initialization vector. The TEKs are encrypted with KEK. When TEKs are generated at the BS and MS (e.g. TEK encryption algorithm is "generate TEKs with TEK materials"), TEK-materials attributes is used instead of TEK-Parameters. TEK-materials attributes include the TEK nonces, the TEK's remaining lifetime and its key sequence number.

***[In the last table in 11.1.10]***

| Name | Type | Length (byte) | Value |
|---|---|---|---|
| SA-TEK-Update-Type | 142.1 | 1 | 1: TEK parameters for an SA<br>2: GTEK parameters for a GSA<br>3-255: Reserved |
| New SAID | 142.2 | 2 | New SAID after handover to new BS |
| Old TEK/GTEK-Parameters | 142.4 | variable | "Older" generation of key parameters relevant to (G)SAID. The compound fields contains the sub-attributes as defined in Table 559. |
| New TEK/GTEK-Parameters | 142.5 | variable | "Newer" generation of key parameters relevant to (G)SAID. The compound fields contains the sub-attributes as defined in Table 559. |
| GKEK-Parameters | 142.6 | variable | GKEK, its lifetime, and its sequence number for the corresponding GSAID. |
| Old TEK-Materials | 142.7 | variable | "Older" generation of key parameters relevant to SAID. The compound fields contains the sub-attributes as defined in Table xxx. |
| New TEK-Materials | 142.8 | variable | "Newer" generation of key parameters relevant to SAID. The compound fields contains the sub-attributes as defined in Table xxx. |

***Modify Table 552 in 11.6 as indicated:***

**Table 552 – RNG-RSP message encodings**

| Name | Type (1 byte) | Length | Value (variable-length) | PHY scope |
|---|---|---|---|---|
| … | … | … | … | … |
| HO Process Optimization | 21 | 2 | For each Bit location, a value of '0' indicates the associated re-entry management messages shall be required, a | All |

| | | | | |
|---|---|---|---|---|
| | | | value of '1' indicates the re-entry management message should be omitted.<br>Bit #0: Omit SBC-REQ management messages during current re-entry processing<br>(Bit #1, Bit #2) = (0,0): Perform re-authentication and SA-TEK 3-way handshake. BS shall not include SATEK-Update TLV in the SA-TEK-Response message.<br>In addition, the RNG-RSP message does not include SA-TEK-Update TLV or SA Challenge Tuple TLV.<br>(Bit #1, Bit #2) = (0,1): Reserved.<br>(Bit #1, Bit #2) = (1,0): In this case, option A or B is recommended.<br>Option A) SA-TEK-Update TLV is included in the RNGRSP message. In this case, SA-TEK 3-way handshake is avoided and SA Challenge Tuple TLV shall not be included in the RNG-RSP message.<br>Option B) Neither SA-TEK-Update TLV nor SA-Challenge Tuple TLV is included in the RNG-RSP message. TEKs are generated using TEK nonces. In this case, the TEK encryption algorithm shall be "generate TEKs with TEK materials".<br>Option ~~B~~C) SA-TEK-Update TLV is included in a SATEK-Response message. In this case, SA-TEK 3-way handshake is performed with SA Challenge Tuple TLV included in the RNG-RSP message.<br>(Bit #1, Bit #2) = (1, 1): Re-authentication and SA-TEK 3-way handshake is not performed. The RNG-RSP message does not include SA-TEK-Update TLV nor SA Challenge Tuple TLV. All the TEKs received from the serving BS are reused.<br>… | |
| … | … | … | … | … |
| TEK Sequence number | 39 | 1 | This attribute contains the Key-Sequence-Numbers of the TEKs being used currently. The length of TEK sequence number is 2 bits. The high-order 4 bits contain the old TEK sequence number and the lower-order 4 bits the new TEK sequence number. e.g) if old and new TEK sequence numbers are 1 and 2, this value is 0x12. | All |

***Modify Table 556 in 11.9 as indicated:***

**Table 556 – PKM attributes types**

| Type | PKM Attribute |
|---|---|
| … | … |
| 35 | Encrypted pre-PAK |
| 36 | TEK Nonce |

| | |
|---|---|
| 37 | TEK Materials |
| 3~~6~~8-255 | *Reserved* |

## ***Modify Table 558 in 11.9.3 as indicated:***

**Table 558 – TEK encryption algorithm identifiers**

| Value | Description |
|---|---|
| 0 | *Reserved* |
| 1 | 3-DES EDE with 128-bit key |
| 2 | RSA with 1024-bit key |
| 3 | ECB mode AES with 128-bit key |
| 4 | AES key wrap with 128-bit key |
| 5 | Generate TEKs with TEK materials |
| ~~5~~6-255 | *Reserved* |

## ***Modify Table 564 in 11.9.14 as indicated:***

**Table 564 – TEK encryption algorithm identifiers**

| Value | Description |
|---|---|
| 0 | *Reserved* |
| 1 | 3-DES EDE with 128-bit key |
| 2 | RSA with 1024-bit key |
| 3 | ECB mode AES with 128-bit key |
| 4 | AES key wrap with 128-bit key |
| 5 | Generate TEKs with TEK materials |
| ~~5~~6-255 | *Reserved* |

## ***Modify Table 565 in 11.9.14 as indicated:***

**Table 565 – Allowed cryptographic suites**

| Value | Description |
|---|---|
| 0x000000 | *Reserved* |
| 0x010001 | 3-DES EDE with 128-bit key |
| ~~0x000002~~ | ~~RSA with 1024-bit key~~ |
| 0x020003 | ECB mode AES with 128-bit key |
| 0x020104 | AES key wrap with 128-bit key |
| 0x020105 | Generate TEKs with TEK materials |
| 0x030003 | CBC mode 128-bit AES, no data authentication, ECB mode AES with 128-bit key |

| | |
|---|---|
| 0x800003 | MBS CTR mode 128 bits AES, no data authentication, AES ECB mode with 128-bit key |
| 0x800004 | MBS CTR mode 128 bits AES, no data authentication, AES key wrap with 128-bit key |
| All remaining values | *Reserved* |

***Insert the following subsection after section 11.9.39***

**11.9.40 TEK Nonce**

The MS and BS generate TEKs with TEK Nonce if TEK encryption algorithm is "generate TEKs with TEK Materials" (See Table 558). TEK generation algorithm is described in 7.2.2.2.6.

| Type | Length (byte) | Value |
|---|---|---|
| 36 | 16 | TEK Nonce to generate TEK |

**11.9.41 TEK Materials**

The TEK-Materials attribute is a compound attribute, consisting of a collection of subattributes. These subattributes represent all security parameters relevant to a particular generation of an SAID's TEK. A summary of the TEK-Materials attribute format is shown below.

| Type | Length | Value (compound) |
|---|---|---|
| 37 | *variable* | The Compound field contains the subattributes as defined in Table xxx |

**Table xxx – TEK-Materials subattributes**

| Attribute | Contents |
|---|---|
| TEK Nonce | TEK nonce used to generate TEKs. See 7.2.2.2.6 for details |
| Key-Lifetime | TEK remaining lifetime |
| Key-Sequence-Number | TEK sequence number |

## *References*

[1] IEEE P802.16Rev2/D2

## *Revision history*

| Version | Date | Author/Editor | Comment |
|---|---|---|---|

| | | | |
|---|---|---|---|
| 1.0 | 2008.03.10 | Kyeong-Tae Do | *Initial Version* |
| | | | |