Project	**IEEE 802.16 Broadband Wireless Access Working Group <http://ieee802.org/16>**
Title	**SA-TEK Procedure Optimization during HO**
Data Submitted	**2005-07-14**

Source(s)	Seokheon Cho Jaesun Cha Chulsik Yoon	Voice: +82-42-860-5524 Fax: +82-42-861-1966 chosh@etri.re.kr
	ETRI 161, Gajeong-dong, Yuseong-Gu, Daejeon, 305-350, Korea	

Re:	IEEE P802.16e/D9
Abstract	The 3 way SA-TEK procedure is used during HO. In case of omitting the authorization procedure during HO, the 3 way SA-TEK procedure is somewhat inefficient to update TEK or SA-ID.
Purpose	Adoption of proposed changes into P802.16e/D9

Patent Policy and Procedures	The contributor is familiar with the IEEE 802.16 Patent Policy and Procedures <http://ieee802.org/16/ipr/patents/policy.html>, including the statement "IEEE standards may include the known use of patent(s), including patent applications, provided the IEEE receives assurance from the patent holder or applicant with respect to patents essential for compliance with both mandatory and optional portions of the standard. "Early disclosure to the Working Group of patent information that might be relevant to the standard is essential to reduce the possibility for delays in the development process and increase the likelihood that the draft publication will be approved for publication. Please notify the Chair <mailto:chiar@wirelessman.org> as early as possible, in written or electronic form, if patented technology (or technology under patent application) might be incorporated into a draft standard being developed within the IEEE 802.16 Working Group. The Chair will disclose this notification via the IEEE 802.16 web site <http://ieee802.org/16/ipr/patents/notices>.

SA-TEK Procedure Optimization during HO

Seokheon Cho, Jaesun Cha, and Chulsik Yoon

ETRI

Introduction

0.1 IEEE P802.16e/D9 Status and Problems

The 3 way SA-TEK procedure is used during HO.

In case of achieving the full authorization procedure during HO, the 3 way SA-TEK exchange procedure followed by the RSA-based authorization procedure or the EAP-based authorization procedure shall be used.

In case of omitting the authorization procedure, such as the RSA-based authorization procedure and the EAP-based authorization procedure, the 3-way SA-TEK exchange is used. A target BS and an MS can omit the authorization procedure, only if the pre-PAK (from the RSA-based authorization procedure) and the MSK (from the EAP-based authorization procedure) can be shared between a serving BS and a target BS. Moreover, a target BS receives information related to an MS's security-capabilities from a serving BS in this case. It means that an MS doesn't need to transmit security-capabilities information to a target BS.

The 3-way SA-TEK procedure consists of a PKMv2 SA-TEK-Challenge message, a PKMv2 SA-TEK-Request message, and a PKMv2 SA-TEK-Response message. A BS sends a PKMv2 SA-TEK-Challenge message to an MS for transmitting the PMK lifetime. An MS sends a PKMv2 SA-TEK-Request message to a BS for transmitting the MS's security-capabilities. A BS sends a PKMv2 SA-TEK-Response message for transmitting the SA-Descriptor, negotiated cryptographic suite, updated SAIDs, and updated TEK.

In case of omitting the authorization procedure, it is more reasonable that a target BS transmits negotiated cryptographic suite, updated SAIDs, and updated TEK through a PKMv2 SA-TEK-Response message to an MS than exchanging 3-way SA-TEK-related messages. Therefore, a PKMv2 SA-TEK-Request message and a PKMv2 SA-TEK-Response message are unnecessary during HO. The SA-Challenge tuple attribute included in the RNG-RSP message is also unnecessary.

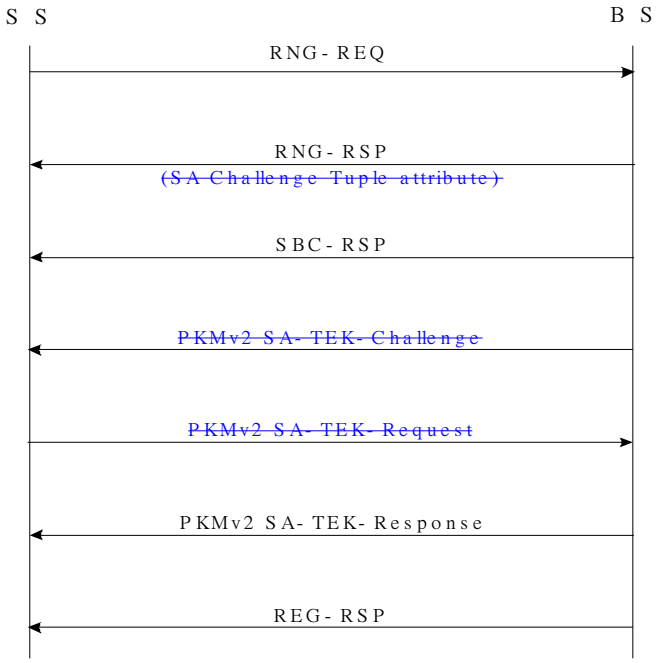
In addition, the function and attributes of a PKMv2 SA-TEK-Response message are duplicated with those of SA TEK Update field included in the REG-RSP message.

0.2 Solutions

Only in case of omitting the authorization procedure, it is more reasonable that a target BS transmits negotiated cryptographic suite, updated SAIDs, and updated TEK through a PKMv2 SA-TEK-Response message to an MS. Therefore, a PKMv2 SA-TEK-Request message and a PKMv2 SA-TEK-Response message are unnecessary during HO. The SA-Challenge tuple attribute

included in the RNG-RSP message is also unnecessary.

The following figure shows the flow diagram, in case of optimizing Handover process (i.e., the case of omitting SBC-REQ, REG-REQ, and authorization procedure.) It is more efficient to skip PKMv2 SA-TEK-Challenge and PKMv2 SA-TEK-Request messages and to use only PKMv2 SA-TEK-Response message.



In addition, since the function and attributes in a PKMv2 SA-TEK-Response message are duplicated with those of SA TEK Update field included in the REG-RSP message, the SA TEK Update attribute is not necessary.

Proposed Changes into IEEE P802.16e/D9

[Remedy 1]

[Change sub-clauses 7.8.1 as follows]

7.8.1 PKMv2 3-way SA-TEK ~~3-way~~ handshake

The AK can be derived in one of three different ways depending on the authentication scheme used as documented in 7.2.2.2.3. Before the 3-way SA-TEK handshake begins, the BS and MS shall both derive a shared KEK and HMAC/CMAC keys as per 7.2.2.2.

The PKMv2 ~~SA-TEK~~ 3-way SA-TEK handshake sequence proceeds as follows:

1. During initial network entry or reauthorization, the BS shall send PKMv2 SA-TEK-Challenge (including a random number BS_Random) to the MS after protecting it with the CMAC/HMAC-Digest ~~tuple~~. If the BS does not receive PKMv2 SA-TEK-Request from the MS within SAChallengeTimer, it shall resend the previous PKMv2 SA-TEK-Challenge.

The BS may send PKMv2 SA-TEK-Challenge up to SAChallengeMaxResends times. If the BS reaches its maximum number of resends, it may initiate full re-authentication or drop the MS.

2. If HO Process Optimization bit #1 is set indicating that PKM Authentication phase is omitted during network re-entry or handover, the BS doesn't need to send a PKMv2 SA-TEK-Challenge message. ~~the BS begins the 3-way-handshake by appending the SA-Challenge Tuple TLV to the RNG-RSP. If the BS does not receive PKMv2 SA-TEK-Request from the MS within SaChallengeTimer (suggested to be several times greater than the length of SaChallengeTimer), it may initiate full re-authentication or drop the MS. If the BS receives an initial RNG-REQ during the period that PKMv2 SA-TEK-Request is expected, it shall send a new RNG-RSP with another SaChallenge TLV.~~

3. The MS shall send PKMv2 SA-TEK-Request to the BS after protecting it with the CMAC/HMAC-Digest. If the MS does not receive PKMv2 SA-TEK-Response from the BS within SATEKTimer, it shall resend the request. The MS may resend the PKMv2 SA-TEK-Request up to SATEKRequestMaxResends times. If the MS reaches its maximum number of resends, it may initiate full re-authentication or decide to connect to another BS or take some other action. The MS must include, through the Security Negotiation Parameters attribute, the security capabilities that it included in the SBC-REQ message during the basic capabilities negotiation phase.

4. If HO Process Optimization bit #1 is set indicating that PKM Authentication phase is omitted during network re-entry or handover, the MS doesn't need to send a PKMv2 SA-TEK-Request message.

~~4~~ 5. Upon receipt of PKMv2 SA-TEK-Request, a BS shall confirm that the supplied AKID refers to an AK that it has available. If

the AKID is unrecognized, the BS shall ignore the message. The BS shall verify the CMAC/HMAC-Digest. If the CMAC/HMAC-Digest is invalid, the BS shall ignore the message. The BS shall verify that the BS_Random in the PKMv2 SA-TEK-Request matches the value provided by the BS in the PKMv2 SA-TEK-Challenge message. If the BS_Random value does not match, the BS shall ignore the message. In addition, the BS must verify the MS's security capabilities encoded in the Security Negotiation Parameters attribute against the security capabilities provided by the MS through the SBC-REG message. If security capabilities don't match, the BS should log the problem.

~~5~~ 6. Upon successful validation of the PKMv2 SA-TEK-Request, the BS shall send PKMv2 SA-TEK-Response back to the MS. The message shall include a compound TLV list each of which identifies the Primary and static SAs, their SA identifiers (SAID) and additional properties of the SA (e.g., type, cryptographic suite) that the MS is authorized to access. ~~In case of HO, the details of any Dynamic SAs that the requesting MS was authorized in the previous serving BS are also included.~~ In addition, the BS must include, through the Security Negotiation Parameters attribute, the security capabilities that it wishes to specify for the session with the MS (these will generally be the same as the ones insecurely negotiated in SBC-REQ/RSP).

If HO Process Optimization bit #1 is set indicating that PKM Authentication phase is omitted during network re-entry or handover, the BS shall send a PKMv2 SA-TEK-Response message followed by sending an SBC-RSP message in order to transmit the negotiated MS's cryptographic suite, updated SAIDs, and updated keys (such as TEKs, GTEKs, and GKEKs). The MS_Random and BS_Random shall not be included in this case.

In case of HO, the details of any Dynamic SAs that the requesting MS was authorized in the previous serving BS are also included.

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" TEKParameters relevant to the active SAIDs. The update may also include multicast/broadcast Group SAIDs (GSAIDs) and associated GTEK-Paramters pairs.

In case of unicast SAs, the TEK-Parameters attribute contains all of the keying material corresponding to a particular generation of an SAID's TEK. This 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.

In case of group or multicast SAs, the TEK-Parameters attribute contains all of the keying material corresponding to a particular generation of a GSAID's GTEK. This would include the GTEK, the GKEK, the GTEK's remaining key lifetime, the GTEK's key sequence number, and the cipher block chaining (CBC) initialization vector. The type and length of the GTEK is equal to ones of the TEK. The GKEK should be identically shared within the same multicast group or the broadcast group. Contrary Key-Update Command, the GTEKs and GKEKs are encrypted with KEK because they are transmitted as a unicast here.

Multiple iterations of these TLVs may occur suitable to re-creating and re-assigning all active SAs and their (G)TEK pairs for the

MS from its previous serving BS. If any of the Security Associations parameters change, then those Security Associations parameters encoding TLVs that have changed will be added.

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

~~6~~ 7. Upon receipt of PKMv2 SA-TEK-Response, an MS shall verify the CMAC/HMAC-Digest. If the CMAC/HMAC-Digest is invalid, the MS shall ignore the message. Upon successful validation of the received PKMv2 SATEK-Response, the MS shall install the received TEKs and associated parameters appropriately. Verification of CMAC/HMAC-Digest is done as per section XXX. The MS also must verify the BS's security capabilities encoded in the Security Negotiation Parameters attribute against the security capabilities provided by the BS through the SBC-RSP message. If security capabilities don't match, the MS should log the problem.

[Delete sub-clauses 11.6.1:]

~~**11.6.1 SA Challenge Tuple**~~

~~This compound TLV enables the BS to abbreviate the 3-way handshake during handover by appending the initial challenge to the RNG-RSP message.~~

~~Name~~	~~Type~~	~~Length (1 byte)~~	~~Value~~	~~Scope~~
~~SA Challenge~~	~~?~~	~~X~~	~~Compound~~	~~RNG-RSP~~

~~The following TLV values shall appear in each SA Challenge TLV:~~

~~Name~~	~~Type~~	~~Length (1 byte)~~	~~Value~~
~~BS_Random~~	~~??~~	~~8 bytes~~	~~-~~
~~AKId~~	~~??~~	~~8 bytes~~	~~-~~

[Change contents in sub-clauses 6.3.2.3.9.18 as follows]

6.3.2.3.9.18 PKMv2 SA-TEK-Challenge message

The BS transmits the PKMv2 SA-TEK-Challenge message as a first step in the 3-way SA-TEK handshake at initial network entry and at reauthorization. ~~It identifies an AK to be used for the Secure Association, and includes a random number challenge to be included by the MSS in its SA-TEK-Request.~~ If HO Process Optimization bit #1 is set indicating that PKM Authentication phase is omitted during network re-entry or handover, this message shall not be used.

[Change contents in sub-clauses 6.3.2.3.9.19 as follows]

6.3.2.3.9.19 PKMv2 SA-TEK-Request message

The MS transmits the PKMv2 SA-TEK-Request message after receipt and successful HMAC/CMAC verification of an SA-Challenge from the BS. The PKMv2 SA-TEK_Request proves liveliness of the MS and its possession of the AK to the BS. If this message is being generated during initial network entry, then it constitutes a request for SA-Descriptors identifying the primary and static SAs and GSAs the requesting MS is authorized to access and their particular properties (e.g., type, cryptographic suite).

If this message is being generated upon HO, then it constitutes a request for establishment (in the target BS) of TEKs, GTEKs and GKEKs at the MSS and renewal of active primary, static and dynamic SAs and associated SAIDs used by the MSS in its previous serving BS.

If HO Process Optimization bit #1 is set indicating that PKM Authentication phase is omitted during network re-entry or handover, this message shall not be used.

[Change contents in sub-clauses 6.3.2.3.9.20 as follows]

6.3.2.3.9.20 PKMv2 SA-TEK-Request message

The BS transmits the PKMv2 SA-TEK-Response message as a final step in the 3-way SA-TEK handshake.

If HO Process Optimization bit #1 is set indicating that PKM Authentication phase is omitted during network re-entry or handover, the BS sends only this message in the 3-way SA-TEK exchange to transmit negotiated MS's cryptographic suite, updated SAIDs, and updated keys (such as TEKs, GTEKs, and GKEKs.) Also, the MS_Random and BS_Random attributes shall not be included in this case.

[Remedy 2]

[Delete sub-clauses 11.7.20 as follows]

~~**11.7.20 SA TEK Update**~~

~~The 'SA TEK Update' field provides a translation table that allows an MS to update its security associations and TEK pairs so that it may continue security service after a hand-over to a new serving BS.~~

~~A compound TLV list each of which identifies the primary and static SAs, their SA identifiers (SAID) and additional properties of the SA (e.g., type, cryptographic suite) that the MS is authorized to access. In case of HO, the details of any Dynamic SAs that the requesting MS was authorized in the previous serving BS are also included.~~

~~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" TEKParameters relevant to the active SAIDs. The update may also include multicast/ broadcast Group SAIDs (GSAIDs) and associated GTEK-Parameters pairs.~~

~~In case of unicast SAs, the TEK-Parameters attribute contains all of the keying material corresponding to a particular generation of an SAID's TEK. This 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.~~

~~In case of group or multicast SAs, the TEK-Parameters attribute contains all of the keying material corresponding to a particular generation of a GSAID's GTEK. This would include the newer GTEK parameter pairs, GTEK's remaining key lifetime, the GTEK's key sequence number, and the cipher block chaining (CBC) initialization vector. The type and length of the GTEK is equal to ones of the TEK. The GKEK should be identically shared within the same multicast group or the broadcast group. The GTEKs are encrypted with GKEK and GKEKs are encrypted with KEK.~~

~~Multiple iterations of these TLVs may occur suitable to re-creating and re-assigning all active SAs and their (G)TEK pairs for the MS from its previous serving BS. If any of the Security Associations parameters change, then those Security Associations parameters encoding TLVs that have changed will be added.~~

~~This TLV may be sent in a single frame along with unsolicited REG-RSP.~~

~~The following TLV values shall appear in each SA TEK Update TLV~~

~~Name~~	~~Type~~	~~Length (1 byte)~~	~~Value~~	~~Scope~~
~~SA_TEK_Update~~	~~?~~	~~Variable~~	~~Compound~~	~~REG-RSP~~

~~Name~~	~~Type~~	~~Length (1 byte)~~	~~Value~~
~~SA_TEK_Update Type~~	~~??~~	~~1~~	~~1 : TEK parameters for a SA~~ ~~2 : GTEK parametes for a GSA~~ ~~3 to 255: Reserved, Not used~~
~~New SAID~~	~~12~~	~~2~~	~~New SAID after hand-over to new BS~~
~~Old SAID~~	~~12~~	~~2~~	~~Old SAID before hand-over from old BS. In case of initial network entry, old SAID is same as new SAID~~
~~Old TEK Parameters~~	~~13~~	~~variable~~	~~"Older" generation of key parameters relevant to SAID. The Compound field contains the sub-attributes as defined in Table 370.~~
~~New TEK/GTEK –Parameters~~	~~13~~	~~variable~~	~~"Newer" generation of key parameters relevant to (G)SAID. The Compound field contains the sub-attributes as defined in Table 370.~~

GKEK Parameters	13	Variable	GKEK and its lifetime for the corresponding GTEK pair if this TLV is for a GSA

and [Delete sub-clauses 11.7.21 as follows]

11.7.21 GKEK Parameters

Description: This attribute is a compound attribute, consisting of a collection of sub-attributes. These subattributes represent all security parameters relevant to a particular generation of an GSAID's GKEK. A summary of the KEK-Parameters attribute format is shown below.

Name	Type	Length (1 byte)	Value	Scope
GKEK Parameters	38	Variable	Compound	REG-RSP

Attribute	Contents
GKEK	GKEK, encrypted with KEK
Key-Lifetime	GKEK remaining lifetime