Project	**IEEE 802.16 Broadband Wireless Access Working Group <http://ieee802.org/16>**	
Title	**Corrections for the 3 Way SA-TEK Exchange**	
Data Submitted	**2005-04-27**	
Source(s)	Seokheon Cho Sungcheol Chang Chulsik Yoon, ETRI 161, Gajeong-dong, Yuseong-Gu, Daejeon, 305-350, Korea	Voice: +82-42-860-5524 Fax: +82-42-861-1966 chosh@etri.re.kr
Re:	IEEE P802.16e/D7	
Abstract	The existing PKMv2 is somewhat unorganized and insecure security framework. This contribution provides a resolution for unorganized and insecure issues in the PKMv2.	
Purpose	Adoption of proposed changes into P802.16e/D7	
Notice	This document has been prepared to assist IEEE 802.16. It is offered as a basis for discussion and is not binding on the contributing individual(s) or organization(s). The material in this document is subject to change in form and content after further study. The contributor(s) 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 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>.	

Corrections for the 3 Way SA-TEK Exchange

Seokheon Cho, Sungcheol Chang, and Chulsik Yoon
ETRI

Introduction

The existing PKMv2 is somewhat in disorder and provides unorganized and insecure security framework.
This contribution supports the backward compatibility with the PKMv1 and security framework of the PKMv2.

This contribution provides a resolution for those problems in the PKMv2.

0.1 IEEE P802.16e/D7 Status

There are messages related to 3 way handshake SA-TEK exchange, e.g. SA-Challenge, SA-TEK-Request, and SA-TEK-Response. These messages are used during initial network entry, reauthorization, HO.

0.2 Problems

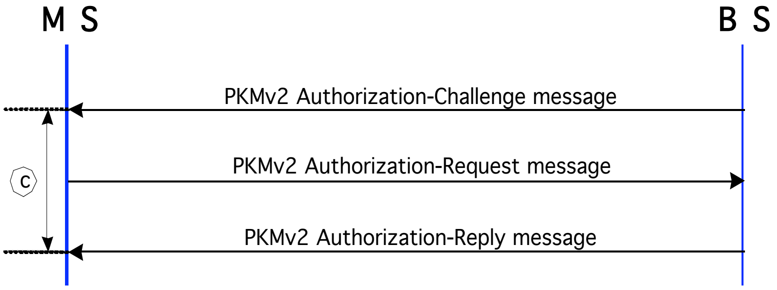
_ The Security_Capabilities, SAID, and SA-Descriptors attributes are included in SA-TEK exchange. However, negotiation of Security_Capabilities and SA-Descriptor should be done before the MS generates and distributes the TEK. It is reasonable that those attributes should be negotiated during the AK generation procedure.

_ The SA-Descriptors included in SA-TEK exchage identifies the Primary and Static SAs the requesting MS is authorized to access and their particular properties. In the case of the multicast service, it is so dangerous to distribute the information of all Static SAs (including static SAID and static TEK-parameters) without DSx-exchange procedure (= without user's use intention for the multicast service). In order to use this SA-TEK exchange procedure, all DSx-exchanges for Static SAs should be performed.

_ It is already defined that the TEK doesn't need to be updated during reauthorization in the IEEE P802.16d/D5. Thus, the TEK doesn't need to be refreshed during HO. The TEK-parameters transfer and share among BSs should be guaranteed. If not, no information shall be shared among BSs and even HO-optimization is impossible.

0.3 Solutions

a) It is appropriate that Security_Capabilities and SA-Descriptors should be transferred not during the TEK exchange procedure but during the MS's AK generation procedure. The following MS's Authorization Key Generation procedure shall support the above solution and transfer those attributes securely.


MS
BS
PKMv2 Authorization-Challenge message
C
PKMv2 Authorization-Request message
PKMv2 Authorization-Reply message

i. PKMv2 Authorization-Challenge message: BS_Nonce
ii. PKMv2 Authorization-Request message: Key Sequence Number (PAK), MS_Nonce, BS_Nonce, Security_Capabilities, SAID, OMAC Digest (from AK)
iii. PKMv2 Authorization-Reply message: Key Sequence Number (AK), Key Lifetime (AK), BS_Nonce, (one or more) SA-Descriptor(s), OMAC Digest (from AK)
iv. PKMv2 Authorization-Reject message: Error-Code, Display-String, BS_Nonce, OMAC Digest (from AK)

b) The DSx-exchange procedure (user's intention) should precede the TEK exchange procedure, especially the multicast service to use Static SA. It is appropriate to use the PKMv2 Key-Request and the PKMv2 Key-Reply message after performing DSx-exchange procedure.

Proposed Changes into IEEE P802.16e/D7

[Delete sub-clause 6.3.2.3.19]

~~6.3.2.3.9.19 SA-Chanllenge message~~

~~The BS transmits the SA-Challenge message as a first step in the 3-way 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.~~

~~Table 37i –SA-Challenge message attributes~~

~~Attribute~~	~~Contents~~
~~RandomBS~~	~~A freshly generated random number of 64bits~~
~~AKID~~	~~This identifies the AK to the BS that was used for protecting this message.~~
~~OMAC/HMAC~~	~~Message integrity tuple for this message~~

[Delete sub-clause 6.3.2.3.20]

~~6.3.2.3.9.20 SA-Chanllenge message~~

~~The MSS transmits the SA-TEK-Request message after receipt and successful HMAC/OMAC verification of an SA-Challenge from the BS. The SA-TEK_Request proves liveliness of the SS and its possession of the AK . If this message is being generated during initial network entry, then it constitutes a request for SADescriptors identifying the primary and static SAs and GSAs the requesting SS 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.~~

~~Table 37j –SA-TEK-Request message attributes~~

~~Attribute~~	~~Contents~~
~~NonceSS~~	~~A 64-bit number chosen by the SS (once per protocol run). It can be a counter or a random number.~~
~~RandomBS~~	~~A freshly generated random number of 64bits~~
~~AKID~~	~~This identifies the AK to the BS that was used for protecting this message.~~
~~Security_Capabilities~~	~~Describes requesting MSS's security capabilities~~
~~OMAC/HMAC~~	~~Message integrity tuple for this message~~

[Delete sub-clause 6.3.2.3.21]

~~6.3.2.3.9.21 SA-TEK-Response message~~

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

~~Table 37k –SA-TEK-Response message attributes~~

~~Attribute~~	~~Contents~~
~~NonceSS~~	~~The number received from the MS~~
~~RandomBS~~	~~A freshly generated random number of 64bits This is optional~~
~~AKID~~	~~This identifies the AK to the BS that was used for protecting this message.~~
~~SA_TEK_Update~~	~~A compound TLV list each of which specifies an SA identifier (SAID) and additional properties of the SA that the MSS is authorized to access. Additionally, in case of HO, for each active SA in previous serving BS, corresponding TEK, GTEK and GKEK parameters are also included.~~
~~OMAC/HMAC~~	~~Message integrity tuple for this message~~

[Delete sub-clause 6.3.2.3.22]

~~6.3.2.3.9.22 SA-TEK-Update message~~

~~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 MSS is authorized to access. In case of HO, the details of any Dynamic SAs that the requesting MSS 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 MSS 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 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 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 MSS 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.~~

~~PKMv2 Authorization Acknowledgement (Auth Ack) message~~

~~Code: X+2~~

~~Sent by the SS to BS as an acknowledgement of successful BS Authorization~~

~~Table 37k—SA-TEK-Update message attributes~~

~~Attribute~~	**~~Contents~~**
~~BS_RANDOM~~	~~A 64-bit random number generated by the BS.~~
~~SS_MAC_ADDRESS~~	~~Contains the SS's MAC address.~~
~~OMAC Tuple~~	~~OMAC calculated using OMAC key derived from PAK.~~

[Delete sub-clause 7.8.1]

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

~~Depending on mutual authorization/EAP, AK can be derived in three different ways as documented in section XXX. Before the 3-way handshake begins, the BS and MS shall both derive a shared AK, KEK and HMAC/OMAC as per 7.2.2.2.~~

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

~~1. During initial network entry or reauthorization, the BS shall send SA-Challenge to the MS after protecting it with the OMAC/HMAC tuple. If the BS does not receive SA-TEK-Request from the BS within SAChallengeTimer, it shall send another challenge. The BS may send SA-Challenge up to SAChallenge-MaxResends times. If the BS reaches its maximum number of resends, it shall discard the AK and may initiate full re-authentication or drop the MS.~~

~~2. During network re-entry or handover, the BS begins the 3-way-handshake by appending the SaChallenge TLV to the RNG-RSP. If the BS does not receive SA-TEK-Request from the BS within SaChallengeTimer, it shall discard the AK and may initiate full re-authentication or drop the MS. If the BS receives RNG-REQ during the period that SA-TEK-Request is expected, it shall send a new RNG-RSP with another SaChallenge TLV.~~
~~3. The MS shall send SA-TEK-Request to the BS after protecting it with the OMAC/HMAC. If the MS does not receive SA-TEK-Response from the BS within SATEKTimer, it shall resend the request. The MS may resend the SA-TEK-Request up to~~

~~SATEKRequestMaxResends times. If the MS reaches its maximum number of resends, it shall discard the AK and may do full re-authentication or decide to connect to another BS or take some other action. The message shall include RandomBS, NonceSS, AKID, SS's Security Capabilities and OMAC/HMAC.~~

~~4. Upon receipt of 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 OMAC/HMAC. If the OMAC/HMAC is invalid, the BS shall ignore the message.~~

~~5. Upon successful validation of the SA-TEK-Request, the BS shall send 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.~~

~~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 OMAC/HMAC shall be the final attribute in the message's attribute list.~~

~~6. Upon receipt of SA-TEK-Response, an MS shall verify the OMAC and ensure the presence of correct NonceSS. If the OMAC or NonceSS is invalid, the MS shall ignore the message. Upon successful validation of the received SA-TEK-Response, the MS shall install the received TEKs and associated parameters appropriately. Verification of OMAC is done as per section XXX. If RandomBS was present in SA-TEKResponse, the MS shall send SA-TEK-Confirm to the BS and an OMAC/HMAC digest.~~

[Delete sub-clause 11.7.21]

~~11.7.21 SA-TEK-Update~~

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

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

~~**Name**~~	~~**Type**~~	~~**Length(1 byte)**~~	~~**Value**~~
~~SA TEK Update~~	~~?~~	~~Variable~~	~~Compound~~

~~**Attribute**~~	~~**Type**~~	~~**Length(1byte)**~~	~~**Value**~~
~~SA TEK Update Type~~	~~??~~	~~1~~	~~1: TEK parameters for a SA~~ ~~2: GTEK parameters for a GSA~~ ~~3-255: *Reserved*~~
~~New SAID~~	~~20.1~~	~~2~~	~~New SAID after hand-over to new BS~~
~~Old SAID~~	~~20.1~~	~~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/GTEK Type?~~	~~Variable~~	~~"Older" generation of key parameters relevant to SAID. The Compound field contains the subattributes as defined in~~

			~~Table 370.~~
~~New TEK/GTEK Parameters~~	~~13/GTEK Type?~~	~~Variable~~	~~"Newer" generation of key parameters relevant to (G)SAID. The Compound field contains the subattributes as defined in Table 370.~~
~~GKEK Parameters~~	~~GKEK Type?~~	~~Variable~~	~~GKEK and its lifetime for the corresponding GTEK pair if this TLV is for a GSA.~~