Project	**IEEE 802.16 Broadband Wireless Access Working Group <http://ieee802.org/16>**
Title	**Corrections for the 3 Way SA-TEK Exchange**
Data Submitted	**2005-05-04**

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) In order to use the 3-way SA Exchange at the initial network entry, some parameters should be included in the 3-way SA exchange messages.

Proposed Changes into IEEE P802.16e/D7

[Modify sub-clause 6.3.2.3.16]
~~6.3.2.3.9.16~~ 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.

Code: 21

Attributes are shown in Table 37i

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

Attribute	Contents
RandomBS	A freshly generated random number of 64bits
~~AKID~~ AK Sequence Number	~~This identifies the AK to the BS that was used for protecting this message.~~ BS transmits newly assigned Authorization Key sequence number
OMAC Tuple/HMAC Tuple	Message integrity tuple for this message

The OMAC key sequence number/HMAC key sequence number included in the OMAC Tuple/HMAC Tuple should be equal to the newly assigned AK sequence number.

[Modify sub-clause 6.3.2.3.17]
~~6.3.2.3.9.17~~ 6.3.2.3.9.20 SA-TEK-Request 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 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.

Code: 22

Attributes are shown in Table 37j.

Table ~~37g~~ 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 Tuple /HMAC Tuple	Message integrity tuple for this message

[Change sub-clause 6.3.2.3.18 as follows]
~~6.3.2.3.9.18~~ 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.

Code: 23

Attributes are shown in Table 37k.

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

Attribute	Contents
NonceSS	The number received from the MS
~~RandomBS-~~BS_Random	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. This compound field is present at the reentry. Additionally, in case of HO, for each active SA in previous serving BS, corresponding TEK, GTEK and GKEK parameters are also included.
(one or more) SA-Descriptor(s)	Each compound SA-Descriptor attribute specifies an SA idenfier (SAID) and additional properties of the SA. This attribute is present at the initial network entry.
OMAC Tuple /HMAC Tuple	Message integrity tuple for this message

[Move whole contents of sub-clause 6.3.2.3.19 into sub-clause 11.7.21 as follows :]

11.7.21 SA TEK Update

The ‘SA TEK Update’ 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.

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-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 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.

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