Project	**IEEE 802.16 Broadband Wireless Access Working Group <http://ieee802.org/16>**	
Title	Optimizing authorization phase during Handover	
Date Submitted	**2004-11-18**	
Source(s)	Avishay Shraga	avishay.shraga@intel.com
	Yigal Eliaspur	Voice: +972-54-5551063
	DJ Johnson	yigal.eliaspur@intel.com
	Intel Corp.	Voice: +972-54-7884877
Re:	IEEE P802.16e/D5	
Abstract	Defines messages to send all SAs keying material in one message after HO instead of one message for each SA, HO process optimization TLV is updated to support partial authorization phase skipping after HO.	
Purpose	Minimize authorization phase duration in network re-entry.	
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:chair@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>.	

Optimizing authorization phase during Handover

Avishay Shraga
Yigal Eliaspur
Intel Corp.

Motivation

In order to achieve good mobility performance, the HO process should be as short as possible.
One of the main time-consuming phases in the network (re)entry is the authorization and key exchange phase.
If the SS will be able to skip or shorten this phase it will be a major step towards seamless HO.
This phase is composed of 2 sub-phases:

- The authentication phase which may be done before HO using pre-authentication
- The key (tek) exchange phase which there is no defined mechanism to skip over it.

The standard today gives the BS a way to inform the SS that the security phase can be skipped. However there may be situations that only one of the 2 sub-phases can be skipped and even this will shorten the total re-entry time.
This contribution describes the way to notify the SS to shorten only one of the security sub-phases and a mechanism to be able to skip the key-exchange phase.

Proposed solution

The proposal is to define a new PKM-REQ/RSP MAC messages in which the SS can send all its SAs needs including TEKs and their associated security context (keys lifetime etc…)/ Each SA context will be a TLV in the message.
This message will be encrypted using the KEK of the SS-BS tupple which was established before this phase (pre-authentication).
In addition the proposal adds a bit to the HO process optimization TLV (11.6) to separate the skip bit of the authentication and the key-exchange.
The assumption of this contribution is that the authentication phase takes much more time than the key exchange.
Therefore, the key-exchange bit is valid only if authentication phase was skipped after HO.
Otherwise a full PKM phase should be done.

Changes summary

[Update the following in table 365a sec 11.6]

Name	Type	Length	Value
HO Process Optimization	nn	2	For each Bit location, a value of '0' indicates the associated re-entry management messages shall be required, a value of '1' indicates the re-entry management message ~~may~~ be omitted. Regardless of the HO Process Optimization TLV settings, the Target BS may send unsolicited SBC-RSP and/or REG-RSP management messages and/or PKM-HO_SA_RSP Bit #0: Omit SBC-REQ/RSP management messages during current re-entry processing Bit #1: Omit Authentication management messages during current re-entry processing Bit #2: Omit Key-Exchange management messages during current re-entry processing (this bit is valid only if Bit#1 is set). Bit #3 : Omit REG-REQ/RSP management during current reentry processing Bit #4 : Omit Network Address Acquisition management messages during current reentry processing Bit #5 : Omit Time of Day Acquisition management messages during current reentry processing Bit #6 : Omit TFTP management messages during current re-entry processing Bit #7 : Full service and operational state transfer or sharing between Serving BS and Target BS (ARQ, timers, counters, MAC state machines, etc…) Bit #8 : post-HO re-entry MSS DL data pending at Target BS

Insert the following rows to table 26a in section 6.3.2.3.9]

Table 26a – PKM message codes

23	HO_SA_REQ	PKM-REQ
24	HO_SA_RSP	PKM-RSP
25-255	reserved	

[Insert the following section in 6.3.2.3.9]

6.3.2.3.9.21 HO_SA_REQ
Sent by the SS to the BS during network re-entry (after HO), if Key-Exchange should not be omitted (Bit #2 in the HO Process Optimization field).
This message contains a TLV for each SA with that was established on the source BS with its security suite.
All the message body is encrypted using KEK and signed with OMAC/HMAC which is the last attribute of the message.

Code: 23
Attributes are shown in Table 37k

Table 37k-HO_SA_REQattributes

Attribute	Contents
One or more SA-descriptors	The SAs supported by source BS including SAID, type and cryptographic suite as defined in 11.9.17

HMAC/OMAC tupple	Cryptographic signature for this message

6.3.2.3.9.22 HO_ SA_RSP
Sent by the BS to the SS, as a response to the HO_ SA_REQ.
This message contains the answer of the BS to the SS_HO_TEK with all the SAs that the BS decided to support, mapping between old SAID and new SAID and the keying material for each SA.
All the message body is encrypted with KEK and signed with OMAC/HMAC which is the last attribute of the message.
This message should be unsolicited sent by target BS in case the omit management bit is on in the HO Process Optimization field (Bit #2) is set.

Code: 24
Attributes are shown in Table 37l

Table 37l-HO_ SA_REQ attributes

Attribute	Contents
One or more SA-parameters mapper	A mapping between an source SAID to a new SAID with it's keying material i.e. TEK and counters as defined in 11.9.33
HMAC/OMAC tupple	Cryptographic signature for this message

[Insert the following section in 11.9.33]

11.9.33 SA-parameters mapper

Description: This attribute contains a mapping of an old SA to and SA and also include the keying material of the new SA: Both TEK keys and their relevant parameters.

Table 379e-SA-parameters mapper subattributes

Attribute	Contents
SAID	Source BS SAID as defined in 11.9.7
SAID	New assigned SAID as defined in 11.9.7
TEK parameters	TEK0 parameters as defined in 11.9.8
TEK parameters	TEK1 parameters as defined in 11.9.8

Type	Length	Value
41	Variable	The Compound field contains subattributes shown in table 379e.