Project	**IEEE 802.16 Broadband Wireless Access Working Group <http://ieee802.org/16>**
Title	AK context refinements
Date Submitted	**2005-03-09**

Source(s)	Avishay Shraga	Avishay.shraga@intel.com
	David Ayoun	Voice: +972-54-5551063
	Yigal Eliaspur	Yigal.Eliaspur@intel.com
	Intel corp.	Voice: +972-54-7884877

Re:	IEEE P802.16e/D6
Abstract	Remove all higher keys than AK from AK context and clarify Context usage
Purpose	Keys AK derived from may be located in different entity than AK to avoid key-sharing thus these keys should not be part of the context
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>.

AK context refinements

Avishay Shraga

1. Motivation

The AK context defined in the standard to hold parameters related to AK key and sub-keys.
Keys which AK is derived from are higher hierarchy keys which may be used to derive AKs for other BSs.
In order to avoid key-sharing between BSs, these keys may be in different entity than the AK thus they should not be part of the context.

2. Proposed solution

remove PMK and PAK from AK context

3. Changes summary

[change 7.2.2.4.1 ak-context]

7.2.2.4.1 AK-context

The context of AK includes all the parameters connected to AK and keys derived directly from it.
When one parameter from this context expires, a new AK should be obtained in order to start a new context.
Obtaining of new AK means re-authentication - doing the whole EAP ~~and~~/or PAK due to the authorization
policies negotiated between the MS and BS until obtaining a new PMK ~~and~~/or PAK which AK may be derived from.
Derivation of AK after HO is done separately in the MS and network from a common PMK or PAK, SSID and BSID. The PMK ~~and~~/or PAK may be used to derive keys to several BSs sharing the same PMK ~~and~~/or PAK.
In HO scenario, if the MS was previously connected to the TBS, the derived AK will be identical to the last one, as long as the PMK stays the same. In order to maintain security in this scenario: the context of the AK must be cached by both sides and to be used from the point it stopped, if context lost by one side, ~~re-authentication is needed to establish new PMK and new AK context~~, this side must validate that this PMK or PAK will never be used to derive AK again for this SS-BS tuple.
The AK context is described in the table:

Table 133 – AK context **Parameter**	**Size**	**Usage**

~~Primary AK (PAK)~~	~~160 bit~~	~~A key yielded from the mutual authorization exchange. Only present at initial network entry and only if the certificated RSA exchange took place, as a result of the mutual authorization policy negotiation.~~
~~PAKID~~	~~64 bits~~	~~Derived from the mutual authorization, present when PAK is present.~~
~~PAK lifetime~~		~~Derived from the mutual authorization, present when PAK is present.~~
~~PMK~~	~~160 bits~~	~~A key yielded from the EAP authentication.~~
~~PMK lifetime~~		~~The lifetime of PMK derived from EAP~~
~~PMKID~~	~~64 bits~~	~~hash 64(EAP session-id)~~
AK	160 bit	The authentication key, calculated as f(PAK,PMK), if only EAP, AK=f(PMK).

AKID	64 bits	Calculated according to the keys that contributed to AK: - If AK=f(PMK,PAK) then AKID=hash 64(EAP session-id | PAKID | BSID) - If AK=f(PMK) then AKID=hash 64(EAP session-id | BSID) - If AK=PAK then AKID = PAKID
AK lifetime		This is the time this key is valid, it is calculated AK lifetime=MIN(PAK lifetime, PMK lifetime) – when this expires re-authentication is needed
H/OMAC_KEY_U	160/128 bit	The key which is used for signing UL management messages
H/OMAC_PN_U	32 bit	Used to avoid UL replay attack on management – when this expires re-authentication is needed
H/OMAC_KEY_D	160/128 bit	The key which is used for signing DL management messages
H/OMAC_PN_D	32 bit	Used to avoid DL reply attack on management – when this expires re-authentication is needed

KEK	160 bit	Used to encrypt transport keys from the BS to the SS