Project	**IEEE 802.16 Broadband Wireless Access Working Group <http://ieee802.org/16>**
Title	PMK context separation from AK context
Date Submitted	**2005-07-21**
Source(s)	Yigal Eliaspur Avishai Shraga ~~Avishay.shraga@intel.com~~ ~~Avishay Shraga~~ ~~Voice: +972-54-5551063~~ ~~Yigal Eliaspur~~ ~~Yigal.Eliaspur@intel.com~~ ~~Intel corp~~ ~~Voice: +972-54-7884877~~ Jeff Mandin jeff@streetwaves-networks.com Streetwaves Networking Amatzia 5 Jerusalem, Israel -
Re:	IEEE P802.16e/D9~~8~~
Abstract	Define a separate context for PMK and remove it from AK
Purpose	Define a separate context for PMK and remove it from AK
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>.

PMK context separation from AK context

~~Jeff Mandin (based on r1 by~~ Yigal Eliaspur(Intel), Jeff Mandin(Streetwaves Networking), Avishay Shrag(Intel~~a~~)

1. Motivation

According to EAP-review (http://www.drizzle.com/~aboba/EAP/review.txt):

PMK is maintained in a higher and a separate entity then the AK (e.g. BS/Authenticator vs. BS port).
_Thus the PMK context definition shall be separated from the AK one,

2. Proposed solution

Extract PMK from the AK context. Create a separate PMK context and define the way it should be used and managed

3. Changes ~~summary~~to 802.16e / D9

[Delete editorial instruction on page 220 line 1 "[Modify as Table 133 indicated:]" – the table is new and not a modification to the base standard]

[then ~~change~~ modify the contents of table 133 ~~7.2.2.4.1~~ so that it appears like the following:~~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 RSA authentication 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, 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 must be initiated by this side in order to create fresh PMK and AKs. In addition the Old PMK shall not be used any more to create or derive new AK contexts (including the one lost).~~

~~The AK context is described in the table:~~

Table 133 – AK context for PKMv2

context **Parameter**	**Size**	**Usage**
~~Primary AK (PAK)~~	~~160-bit~~	~~A key yielded from the RSA authorization~~
~~PAK sequence number~~	~~4-bits~~	~~PAK sequence number, when the RSA-based authorization is achieved. The least significant 2 bits are the sequence counter, and the most significant 2 bits are set to zero.~~
~~PAK lifetime~~		~~PAK lifetime, when the RSA-based authorization is achieved.~~
~~PMK~~	~~160-bits~~	~~A key yielded from the EAP-based authentication~~
~~PMK lifetime~~		~~PMK lifetime, when the EAP-based authorization is achieved and the AAA-key is obtained. The value of PMK lifetime may be transferred from the EAP method or may be set by a vendor.~~

~~PMK sequence number~~	~~4 bits~~	~~PMK sequence number, when the EAP-based authorization is achieved and a key is generated. The most significant 2 bits are the sequence counter. And the least significant 2 bits set to 0.~~
AK	160 bit	The authorization key, calculated as defined in 7.2.2.2.3
AKID	64 bits	AKID = Dot16KDF (AK, AK SN|SSID|BSID|"AK", 64)
AK sequence number	4 bits	Sequence number of root keys (PAK and PMK) for the AK. This value is the least significant 2-bit of PAK sequence number concatenated with the least significant 2-bit of PMK sequence number. If AK = f (PAK and PMK), then AK SN = PAK SN + PMK SN If AK = f (PAK), then AK SN = PAK SN If AK = f (PMK), then AK SN = PMK SN

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.
PMK Sequence Number	4 bits	The sequence number of the PMK that this AK is derived from
H/~~OMAC~~CMAC_KEY_U	160/128 bit	The key which is used for signing UL management messages
H/~~OMAC~~CMAC_PN_U~~H/OMAC_KEY_U~~	32 bit ~~160/128 bit~~	Used to avoid UL replay attack on the management connection – when this expires re-authentication is needed~~The key which is used for signing UL management messages~~
H/~~OMAC~~CMAC_KEY_D~~H/OMAC_PN_U~~	160/128 bit ~~32 bit~~	The key which is used for signing DL management messages~~Used to avoid UL replay attack on management – when this expires re-authentication is needed~~

H/~~OMAC~~CMAC_PN_D~~H/OMAC_KEY_D~~	32 bit ~~16 0/ 12 8 bit~~	Used to avoid DL reply attack on the management connection – when this expires re-authentication is needed~~The key which is used for signing DL management messages~~
KEK~~H/OMAC_PN_D~~	16 0 bit ~~32 bit~~	Used to encrypt transport keys from the BS to the SS~~Used to avoid DL reply attack on management – when this expires re-authentication is needed~~
~~KEK~~	~~16 0 bit~~	~~Used to encrypt transport keys from the BS to the SS~~

[Insert new section 7.2.2.4.2:]

7.2.2.4.~~X~~ 2 PMK C~~-e~~ontext

The PMK context ~~of PMK~~ includes all ~~the~~ parameters ~~connected to~~associated with the PMK.
This context is created ~~once~~ when EAP Authentication completes~~d~~.

~~The parameters that affect the validity of this context is the PMK lifetime.~~The PMK (and its context) ~~have a lifetime.~~
~~There are~~ PMK key has ~~two~~ lifetime update phases ~~of the lifetime: the first is~~ begins ~~once~~ the ~~context been created and the second is~~ begins ~~after the 3-way handshake have~~ has ~~completed successfully.~~

~~The phases ensures that once~~ a ~~PMK is created it will be defined with the~~ a particular ~~default lifetime.~~

~~and after successful 3-way handshake, this lifetime may be enlarged~~ lengthened ~~using the PMK life time TLV within the 3-way handshake.~~

~~In order to maintain security and connectivity, when this context is about to expire re-authentication must be initiated.~~

The PMK context is described in the table XXX

Table xxx

Parameter	Size	Usage
PMK	160 bits	A key yielded from the EAP-based authentication.
PMK sequence number~~Remaining PMK lifetime~~	4 bits	PMK sequence number, when the EAP-based authorization is achieved and a key is generated. The most significant 2 bits are the sequence counter. And the least significant 2 bits set to 0. ~~PMK lifetime, effective from the time when the EAP-based authorization is achieved and the AAA-key is obtained.The lifetime remaining for the PMK.~~ ~~The value of PMK lifetime is initially set to the a default value.~~ ~~The 3-way handshake may subsequently change this value~~
~~PMK sequence number~~	~~4 bits~~	~~PMK sequence number, when the EAP-based authorization is achieved and a key is generated. The most significant 2 bits are the sequence counter. And the least significant 2 bits set to 0.~~

7.2.2.4.3 PAK-context

The PAK context includes all parameters associated with the PAK. This context is created when RSA Authentication completes.

Parameter	Size	Usage
PAK	160 bits	A key yielded from the RSA-based authentication.
PAK Lifetime	-	PAK lifetime, from when the RSA-based authorization is achieved. The value of PAK lifetime is initially set to a default value. The 3-way handshake may subsequently change this value
PAK sequence number	4 bits	PAK sequence number, when the RSA-based authorization is achieved and a key is generated. The most significant 2 bits are the sequence counter. And the least significant 2 bits set to 0.

~~10.2 PKM parameter values~~

~~Insert to table 343~~

~~System~~	~~Name~~	~~Description~~	~~Min value~~	~~Default value~~	~~Max value~~
~~SS+BS~~	~~PMK lifetime~~	~~The lifetime assigned to a PMK when created or received from AAA server~~	~~5sec~~	~~10sec~~	~~15min900 sec~~

~~11.9.19 PKM configuration settings~~

~~Type~~	~~Length~~	~~Value~~	~~Scope~~
~~27~~	~~Variable~~	~~Compound~~	~~Auth replay PMKv2-rsa reply sa-tek-response~~

~~-~~

-
-
11.9.19.8 PMK lifetime

7.2.2.4.3 PAK-context

The PAK- context includes all parameters associated with the PAK. This context is created when RSA Authentication completes.

Parameter	Size	Usage
PAK	160 bits	A key yielded from the RSA-based authentication.
PAK Lifetime		PAK lifetime, when the RSA-based authorization is achieved.
PAK sequence number	4 bits	PMK sequence number, when the EAP-based authorization is achieved and a key is generated. The most significant 2 bits are the sequence counter. And the least significant 2 bits set to 0.