Project	**IEEE 802.16 Broadband Wireless Access Working Group <http://ieee802.org/16>**
Title	**PKM Version Separation**
Date Submitted	**2004-6-21**
Source(s)	David Johnston Intel Corporation 2111 NE 25th Ave. Hillsboro 97124 Voice: +1 (503) 264-3855 [mailto:dj.johnston@intel.com]
Re:	IEEE 802.16e Security Adhoc
Abstract	Proposal to separate out PKMv1 and PKMv2 text
Purpose	To eliminate the ambiguity in the specification surrounding which functions belong to PKMv1 and which functions belong to PKMv2.
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>.

PKM Version Separation

David Johnston

802.16e, as currently defined, allows negotiation of version 2 of PKM. However there is only a single PKM section in the text and all PKM functions within this are defined independently of which version of PKM they apply to.

This proposal creates two PKM sections, one for v1 and one for v2. The PKMv2 procedures are therefore disambiguated from the PKMv1 procedures.

The RevD-D5 document, section 7 is structured as follows:

7 Security Sublayer
7.1 Architecture
7.1.1 Packet data encryption
7.1.2 Key management protocol (needs EAP)
7.1.3 Security Associations (AAID and GSA)
7.1.4 Mapping of connections to SAs (multicast GSA changes)
7.1.5 Cryptographic Suite
7.2 PKM Protocol (Title changes to PKM v1)
7.2.1 SS Authorization and AK exchange
7.2.2 TEK Exchange Overview
7.2.2.1 TEK exchange overview for PMP topology
7.2.2.2 TEK exchange overview for Mesh Mode
7.2.3 Security capabilities selection
7.2.4 Authorization state machines
7.2.4.1 States
7.2.4.2 Messages
7.2.4.3 Events
7.2.4.4 Parameters
7.2.4.5 Actions
7.2.5 TEK State Machine
7.2.5.1 States
7.2.5.2 Messages
7.2.5.3 Events
7.2.5.4 Parameters
7.2.5.5 Actions
7.3 Dynamic SA creation and mapping
7.3.1 Dynamic SA creation
7.3.2 Dynamic mapping of SA
7.4 Key usage (PAK and EAP key changes)
7.4.1 BS key usage
*
7.4.2 SS key usage
7.5 Cryptographic methods (need new crypto modes – OMAC and secure key transfer)
7.5.1 Data encryption methods

7.5.1.1 DES
7.5.1.2 CCM
*
7.5.2 Encryption of TEK (Need secure TEK key exchange)
7.5.2.1 3DES ECB
7.5.2.2 RSA
7.5.2.3 AES ECB
7.5.3 HMAC Digests (add OMAC)
7.5.4 Derivation of TEKs (need V2 key hierarchy)
7.5.4.1 DES Keys
7.5.4.2 3DES KEKs
7.5.4.3 HMAC authentication keys (OMAC auth keys)
7.5.5 Public key encryption of AK (and PAK for v2)
7.5.6 Digital signatures
7.6 Certificate profile (want BS cert as well)
*

From this list it can be seen that the PKMv2 specific changes lay partially outside the PKM section (7.2). Inserting a section 7.3 (PKMv2) will not be sufficient, since behavior outside of 7.2 must also be birfucated.

Therefore I propose that more of the existing text be brought under the PKMv1 section, so that the alternate PKMv2 text can be places in a PKMv2 section and be unambiguously attached to the PKMv2 mode.

This would look something like the following list. I have italicized the parts that have moved, an emboldened new sections

7 Security Sublayer
7.1 Architecture
7.1.1 Packet data encryption
7.1.5 Cryptographic Suite
7.1.x PKM versions
7.2 PKM Version 1 Protocol
7.2.x Architecture
7.2.x Security Associations
7.2.x Mapping of connections to SAs
7.2.x Key usage
7.2.x.1 BS key usage
*
7.4.2 SS key usage
7.5.x Key Derivation Functions
7.5.4.1 *DES Keys*
7.5.4.2 3DES KEKs
7.5.4.3 HMAC authentication keys
7.2.x Encryption of TEK
7.5.2.1 *3DES ECB*
7.5.2.2 *RSA*
7.5.2.3 *AES ECB*
7.2.x Public key encryption of AK

7.2.1 SS Authorization and AK exchange
7.2.2 TEK Exchange Overview
7.2.2.1 TEK exchange overview for PMP topology
7.2.2.2 TEK exchange overview for Mesh Mode
7.2.3 Security capabilities selection
7.2.4 Authorization state machines
7.2.4.1 States
7.2.4.2 Messages
7.2.4.3 Events
7.2.4.4 Parameters
7.2.4.5 Actions
7.2.5 TEK State Machine
7.2.5.1 States
7.2.5.2 Messages
7.2.5.3 Events
7.2.5.4 Parameters
7.2.5.5 Actions

7.3 Dynamic SA creation and mapping
7.3.1 Dynamic SA creation
7.3.2 Dynamic mapping of SA
7.5 Cryptographic methods (need new crypto modes – OMAC and secure key transfer)
7.5.1 Data encryption methods
7.5.1.1 DES
7.5.1.2 CCM
*
7.5.3 HMAC Digests
7.5.x OMAC Digests
7.5.6 Digital signatures
7.6 Certificate profile
SS Cert Profile
* - existing text
BS Cert Profile
* - new text

We should at this point have the same functionality as the base specification, with additional modes –OMAC and a BS cert defined. There is also text describing how a different PKM version is used.

We can now insert a new PKM version section after 7.2

7.3 PKM Version 2 Protocol
7.3.1 Architecture
7.3.2 Security Associations
7.3.2.1 Unicast associations
7.3.2.2 Group associations
7.3.2.3 Mapping of connections to SAs and GSAs
7.3.3 Key Hierarchy

7.3.4 Key usage
7.2.x.1 BS key usage
*
7.3.5 SS key usage
*
7.3.6 Key Derivation Functions
7.5.4.1 Generic PRF
* - all the key derivations
7.3.7 ID request
*
7.3.7 Mutual Authorization and *Secure PAK exchange*
*
7.3.7 and half – EAP Mutual Authentication
*
7.3.8 Secure EAP key exchange
*
7.3.9 Secure TEK Exchange
*
7.3.10 Security capabilities selection
7.3.11 Authorization state machines
7.2.4.1 States
7.2.4.2 Messages
7.2.4.3 Events
7.2.4.4 Parameters
7.2.4.5 Actions
7.3.12 TEK State Machine
7.2.5.1 States
7.2.5.2 Messages
7.2.5.3 Events
7.2.5.4 Parameters
7.2.5.5 Actions

Specific Text changes:

Editors instructions:
[Take existing PKMv1 text, as per 802.16 as reorder the sections according to the following structure shown below. Insert additional PKMv2 section. Changed clause 7 text in 802.16e-D3 should be moved into the PKMv2 section, in particular the EAP text]

7 Security Sublayer
7.1 Architecture
7.1.1 Packet data encryption
7.1.5 Cryptographic Suite
7.1.x PKM versions
7.2 PKM Version 1 Protocol
7.2.x Architecture
7.2.x Security Associations
7.2.x Mapping of connections to SAs

7.2.x Key usage
7.2.x.1 BS key usage
*
7.4.2 SS key usage
7.5.x Key Derivation Functions
7.5.4.1 *DES Keys*
7.5.4.2 3DES KEKs
7.5.4.3 HMAC authentication keys
7.2.x Encryption of TEK
7.5.2.1 *3DES ECB*
7.5.2.2 *RSA*
7.5.2.3 *AES ECB*
7.2.x Public key encryption of AK
7.2.1 SS Authorization and AK exchange
7.2.2 TEK Exchange Overview
7.2.2.1 TEK exchange overview for PMP topology
7.2.2.2 TEK exchange overview for Mesh Mode
7.2.3 Security capabilities selection
7.2.4 Authorization state machines
7.2.4.1 States
7.2.4.2 Messages
7.2.4.3 Events
7.2.4.4 Parameters
7.2.4.5 Actions
7.2.5 TEK State Machine
7.2.5.1 States
7.2.5.2 Messages
7.2.5.3 Events
7.2.5.4 Parameters
7.2.5.5 Actions

7.3 Dynamic SA creation and mapping
7.3.1 Dynamic SA creation
7.3.2 Dynamic mapping of SA
7.5 Cryptographic methods (need new crypto modes – OMAC and secure key transfer)
7.5.1 Data encryption methods
7.5.1.1 DES
7.5.1.2 CCM
*
7.5.3 HMAC Digests
7.5.x OMAC Digests
7.5.6 Digital signatures
7.6 Certificate profile
SS Cert Profile
* - existing text
BS Cert Profile
* - new text