	IEEE 802.16 Broadband Wireless Access Working Group <http://ieee802.org/16>
Title	**PKM configuration settings in EAP Establish-Key Confirm message**
Date Submitted	**2004-08-16**
Source(s)	Dongkie Lee, DongIl Moon, DongRyul Lee, JongKuk Ahn, KangIl Koh, Sihun Ryu, Sungho Ha SK Telecom 15F, Seoul Finance Center, 84, Taepyungpro 1 ga, Chung-gu, Seoul, 100-768, Korea Voice: +82-2-6323-3147 Fax: +82-2-6323-4493 [mailto: {galahad,dimoon,drlee,jgahn,ss23}@sktelecom.com]
Re:	Recirculation Ballot #14c Announcement
Abstract	PKM configuration settings defined for Auth Reply should also be applied to EAP Establish-Key Confirm message because Auth Reply and EAP Establish-Key Confirm is analogously quite similar.
Purpose	Discuss and Adopt as the baseline text
Notice	s 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>.

1

PKM configuration settings in EAP Establish-Key Confirm message

Dongkie Lee, DongRyul Lee, DongIl Moon, JongKuk Ahn, KangIl Koh, Sihun Ryu
SK Telecom

1. Problem Statements

PKM timer values(or PKM configuration settings defined in 11.9.19 of REVd/D5) such as below listed in Table 1 may be contained in Auth Reply and override the default timer values. But EAP authorization section of REVe/D4 does not specified this mechanics. With EAP authorization, PKM timer values should be specified for EAP Establish-Key Confirm message in line with Auth Reply.

Table 1 PKM configuration settings

	Timer Value
1	Authorize wait timeout
2	Reauthorize wait timeout
3	Authorization grace time
4	Operational wait timeout
5	Rekey wait timeout
6	TEK grace time
7	Authorize reject wait timeout

2 Proposed Changes

[Change into the following:]

6.3.2.3.9.16 EAP Establish-Key confirm message

The BS transmits the EAP Establish-Key-Confirm message as the third step in the 4-step sequence of establishing an AK after EAP-based authentication. The EAP Establish-Key confirm may also contain PKM configuration settings that override the default timer values.

Code: 18

Attributes are shown in Table 37f.

Table 37f—EAP Establish-Key Confirm attributes

Attribute	Contents
Nonce	Same values as in the Establish-Key Request
Key-Sequence-Number	Sequence Number for established AK
(one or more) SA descriptors	Each Compound SA-Descriptor attribute specifies an SAID and additional properties of the SA
PKM Configuration settings(optional)	PKM timer values

HMAC-Tuple	The cryptographic hash for the message. The key used to generate the hash is the KCK (key confirmation key) as described in xx

1