Project	**IEEE 802.16 Broadband Wireless Access Working Group <http://ieee802.org/16>**	
Title	**Corrections for the PMK ID and the AK ID using the EAP-Session ID**	
Data Submitted	**2005-05-04**	
Source(s)	Seokheon Cho Sungcheol Chang Chulsik Yoon, ETRI Jicheol Lee Yong Chang SAMSUNG Yongjoo Tcha KT Li Rui, Tian Feng ZTE corporation	Voice: +82-42-860-5524 Fax: +82-42-861-1966 chosh@etri.re.kr 161, Gajeong-dong, Yuseong-Gu, Daejeon, 305-350, Korea
Re:	IEEE P802.16e/D7	
Abstract	The existing PKMv2 is somewhat unorganized and insecure security framework. This contribution provides a resolution for PMK ID and AK ID to use the EAP-Session ID.	
Purpose	Adoption of proposed changes into P802.16e/D7	
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:chiar@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>.	

Corrections for the PMK ID and the AK ID using the EAP-Session ID

Seokheon Cho, Sungcheol Chang, and Chulsik Yoon
ETRI

Jicheol Lee and Yong Chang
SAMSUNG

Yongjoo Tcha
KT

Li Rui and Tian Feng
ZTE corporation

Introduction

The existing PKMv2 is somewhat in disorder and provides unorganized and insecure security framework.
This contribution supports the backward compatibility with the PKMv1 and security framework of the PKMv2.

This contribution provides a resolution for those problems in the PKMv2.

0.1 IEEE P802.16e/D7 Status
The value of the EAP session-id is used to compute the value of PMKID (=> hash64(EAP session-id)) and AKID (=> hash64(EAP sessionid|PAKID|BSID)).

0.2 Problems

- The EAP session-id is an attribute used in the EAP Method (e.g., EAP-TLS). This EAP session-id is out of scope and is a value only used in the EAP Method. So, it is unreasonable that the IEEE 802.16 PKM sublayer adopts and uses this value.
- In the general EAP Method, the value of the EAP session-id is not changed, even though the new AAA-key is refreshed. That is, even if PMK is updated, the value of PMKID (=> hash64(EAP session-id)) and AKID (=> hash64(EAP sessionid|PAKID|BSID)) is also not changed. In addition, since both an SS and a BS shall be able to support up to two simulataneously active Authorization Keys (AKs), the AKID should be able to distinguish two active AKs. Therefore, AKID is unsuitable as the identifier or sequence number needed to distinguish new AK from old AK.
- The size of AKID (64bits), used to distinguish only two AKs, is too long.

0.3 Solutions

- To solve the AKID, the AK sequence number as an AK identifier is newly defined. The BS generates the AK sequence number and informs it to an MS, whenever the AK is updated.
- If the size of AK sequence number is 8bits as defined in the PKMv1, then the size is enough to distinguish two AKs and efficient to transmit not 64bits AKID but 8bits AK sequence number in radio link.
- Using the AK sequence number (8bits) is able to support backward compatibility with the PKMv1.

Proposed Changes into IEEE P802.16e/D7

[Modify Table 133 in the sub-clause 7.2.2.4.1 as follows:]
7.2.2.4.1 AK Context

The AK context is described in the table:

Table 133-AK Context in PKMv2

Parameter	Size	Usage
Primary AK (PAK)	160bits	A key yielded from the ~~mutual authorization exchange~~ RSA-based authorization. ~~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~~	~~64bits~~	~~Derived from the mutual authorization, present when PAK is present.~~
PAK Sequence Number	8bits	PAK sequence number, when the RSA-based authorization is achieved.
PAK lifetime		~~Derived from the mutual authorization, present when PAK is present.~~ PAK lifetime, when the RSA-based authorization is achieved.
PMK	160bits	A key yielded from the EAP-based authentication
PMK lifetime		~~The lifetime of PMK derived from EAP.~~ 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 be set by a vendor.
~~PMKID~~	~~64bits~~	~~hash 64(EAP session-id)~~
AK	160bits	~~The authentication key, calculated as f(PAK,PMK), if only EAP, AK=f(PMK).~~ The authorization key, calculated as defined in 7.2.2.2.3
~~AKID~~	~~64bits~~	~~Calculated according to the keys that contributed to AK:~~ ~~-If AK=f(PMK,PAK) then AKID=hash 64(EAP sessionid | PAKID | BSID)~~ ~~-If AK=f(PMK) then AKID=hash 64(EAP session-id | BSID)~~ ~~-If AK=PAK then AKID = PAKID~~
AK Sequence Number	8bits	AK sequence number
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 bits/128 bits	The key which is used for signing UL management messages.
H/OMAC_PN_U	32 bits	Used to avoid UL replay attack on management messages – when this expires re-authentication is needed.
H/OMAC_KEY_D	160 bits/128 bits	The key which is used for signing DL management messages.
H/OMAC_PN_D	32 bits	Used to avoid DL replay attack on management messages – when this expires re-authentication is needed.
KEK	160 bits	Used to encrypt ~~transport keys~~ TEK or GKEK from the BS to the SS.

[Modify Table 133 in the sub-clause 7.2.2.4.1 as follows:]
7.2.2.4.1 AK Context

The AK context is described in the table:

Table 133-AK Context in PKMv2

Parameter	Size	Usage
Primary AK (PAK)	160bits	A key yielded from the ~~mutual authorization exchange~~ RSA-based authorization. ~~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~~	~~64bits~~	~~Derived from the mutual authorization, present when PAK is present.~~
PAK Sequence Number	8bits	PAK sequence number, when the RSA-based authorization is achieved.
PAK lifetime		~~Derived from the mutual authorization, present when PAK is present.~~ PAK lifetime, when the RSA-based authorization is achieved.
PMK	160bits	A key yielded from the EAP-based authentication
PMK lifetime		~~The lifetime of PMK derived from EAP.~~

		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 be set by a vendor.
~~PMKID~~	~~64bits~~	~~hash 64(EAP session-id)~~
AK	160bits	~~The authentication key, calculated as f(PAK,PMK), if only EAP, AK=f(PMK).~~ The authorization key, calculated as defined in 7.2.2.2.3
~~AKID~~	~~64bits~~	~~Calculated according to the keys that contributed to AK:~~ ~~-If AK=f(PMK,PAK) then AKID=hash 64(EAP sessionid | PAKID | BSID)~~ ~~-If AK=f(PMK) then AKID=hash 64(EAP session-id | BSID)~~ ~~-If AK=PAK then AKID = PAKID~~
AK Sequence Number	8bits	AK sequence number
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 bits/128 bits	The key which is used for signing UL management messages.
H/OMAC_PN_U	32 bits	Used to avoid UL replay attack on management messages – when this expires re-authentication is needed.
H/OMAC_KEY_D	160 bits/128 bits	The key which is used for signing DL management messages.
H/OMAC_PN_D	32 bits	Used to avoid DL replay attack on management messages – when this expires re-authentication is needed.
KEK	160 bits	Used to encrypt ~~transport keys~~ TEK or GKEK from the BS to the SS.