Project	IEEE 802.16 Broadband Wireless Access Working Group <**http://ieee802.org/16**>
Title	Fix some problems with AK Context in Table 133a, 802.16e-2005
Date Submitted	2006-09-22
Source(s)	Changhong Shan, Huawei, ritatv@huawei.com Phillip Barber, Huawei, pbarber@huawei.com
Re:	Fix some problems with AK Context in Table 133a, 802.16e-2005
Abstract	
Purpose	Fix some problems with AK Context in Table 133a, 802.16e-2005
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>.

Fix some problems with AK Context in Table 133a, 802.16e-2005

Changhong Shan, Phillip Barber
Huawei

Problem:
Fix some problems with AK Context in Table 133a, 802.16e-2005
Missing support for Double-EAP
Missing reference for PAK
Other minor errors

Remedy:
In IEEE802.16e-2005, Page 287, Table 133a-AK context in PKMv2, Modify table as:

Parameter	Size (bits)	Usage
AK	160	The authorization key, calculated as defined in 7.2.2.2.3 .
AKID	64	AKID = Dot16KDF(AK, AK SN|SS MAC Address|BSID|"AK", 64). The AK_SN in the Dot16KDF function is an 8-bit number which consists of leading 4 zero bits and appending 4-bit AK_SN in MSB first order.
AK Sequence Number	4	Sequence number of root keys (PAK ~~,and~~ PMK and PMK2) for the AK. ~~This value is the most 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 (PMK and PMK2), then AK SN = (PMK SN + PMK2 SN) Modulo 4 If AK = f (PAK), then AK SN = PAK SN If AK = f (PMK), then AK SN = PMK SN
AK Lifetime		~~This is t~~The time this key is valid.~~; it is calculated~~ If AK = f (PAK and PMK), then AK lifetime = MIN(PAK lifetime, PMK lifetime) If AK = f (PMK and PMK2), then AK lifetime = MIN(PMK lifetime ,PMK2 lifetime) If AK = f (PAK), then AK lifetime = PAK lifetime If AK = f (PMK), then AK lifetime = PMK lifetime. ~~when~~ Before this expires, when AK Grace time expires, re-authentication is needed.
PAK Sequence Number	4	The sequence number of the PAK that this AK is derived from. If RSA authentication is not used, this value shall be set to zero.
PMK Sequence	4	The sequence number of the PMK from which this AK is

Number		derived. If EAP authentication is not used, this value shall be set to zero.
PMK2 Sequence Number	4	The sequence number of the PMK2, the second-round EAP result in Double-EAP, that this AK is derived from. In Single-EAP or if EAP authentication is not used, this value shall be set to zero.
HMAC/CMAC_ KEY_U	160/128	The key which is used for signing UL management messages
HMAC/CMAC_ PN_U	32	Used to avoid UL replay attack on the management connection—~~when~~ before this expires, re-authentication is needed.
HMAC/CMAC_ KEY_D	160/128	The key which is used for signing DL management messages
HMAC/CMAC_ PN_D	32	Used to avoid DL replay attack on the management connection—~~when~~before this expires, re-authentication is needed.
KEK	160	Used to encrypt transport keys from the BS to the SS
EIK	160	EAP Integrity Key for authenticating Authenticated EAP message. It is only used in Double-EAP.