Project	**IEEE 802.16 Broadband Wireless Access Working Group <http://ieee802.org/16>**
Title	**Protect the integrity of security capability information**
Date Submitted	**2004-12-29**
Source(s)	[feng tian] [Rui Li] [DongXin Lu] [zte corporation] [ZTE Plaza , Keji Road South , Hi-tech Industrial Park , Nanshan District , Shenzhen , P.R.China , 518057] Voice: [86-0755-26772017] Fax: [86-0755-26772004] [mailto:tian.feng2@zte.com.cn]
Re:	802.16e/D5a
Abstract	Propose protect the integrity of security capability information
Purpose	Adopt
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>.

Protect the integrity of security capability information

Feng Tian
DongXin Lu
Rui Li

The PKMv2 authorization via RSA authentication doesn’t protect the integrity of the security capability information. Attacker may reduce the security strength of the security capability negotiated between SS and BS with juggling the security-capabilities field in authorization request message.

The BS should add the security-capabilities field received from authorization request message to authorization reply message, when SS receive the authorization reply , it can estimate whether the security-capabilities has been juggled by comparing the security-capabilities field in authorization request message and that in authorization reply message.

[add the following as show]

6.3.2.3.9.20 PKMv2 authorization reply (auth reply) message

Sent by the BS to a client MSS in response to an Authorization Request, the Authorization Reply message contains an AK, the key’s lifetime, the key’s sequence number, and a list of SA-Descriptors identifying the Primary and Static SAs the requesting MSS is authorized to access and their particular properties (e.g., type, cryptographic suite). The AK shall be encrypted with the MSS’s public key. The SA-Descriptor list shall include a descriptor for the Basic CID reported to the BS in the corresponding Auth Request. The SS_Random number is returned from the auth-req message, along with a random number supplied by the BS, thus enabling assurance of key liveness.

Code: 22

Attributes are shown in Table 37j.

Table 37j—PKMv2 Auth-Reply attributes

Attribute	**Contents**
MSS_Random	A 64 bit random number generated in the MSS
BS_Random	A 64 bit random number generated in the BS
MSS_Certificate	Contains the MSS’s X.509 user certificate

Security_Capabilities	Received in authorization request message
EncryptedAK	RSA-OAEP-Encrypt(PubKey(MSS), pre-PAK | Id(MSS))
AK Lifetime	AK Aging timer
AK Sequence Number	64 bit AK sequence number
AAID/SAID	Either the AAID or the Basic CID if in initial network entry
CertBS	The BS Certificate
SigBS	An RSA signature over all the other attributes in the message