Project	**IEEE 802.16 Broadband Wireless Access Working Group <http://ieee802.org/16>**
Title	**Uniform Pkmv2 Authorization Flow**
Date Submitted	**2005-04-24**
Source(s)	Tian Feng, Li Rui Voice: [86-0755-26772016] Fax: [86-0755-26772004] [mailto:li.rui2@zte.com.cn] ZTE corporation ZTE Plaza , Keji Road South , Hi-tech Industrial Park , Nanshan District , Shenzhen , P.R.China , 518057
Re:	Response to Sponsor Ballot on IEEE802.16e/D7 document
Abstract	This contribution describes the uniform PKMv2 authorization flow.
Purpose	To incorporate the text changes proposed in this contribution into the 802.16e/D8 draft.
Notice	
Release	
Patent Policy and Procedures	

Uniform Pkmv2 Authorization Flow

Tian Feng, Li Rui
ZTE corporation

1. Problem Statement

There are two issues in PKMv2 RSA authentication:

1. In PKMv2, There are different procedures of RSA authentication for different authorization policy. In authorization based on RSA authentication and EAP authentication, BS and MS do not negotiate SAs in RSA authentication. But in authorization based on RSA-only authentication, BS and MS need negotiate SAs in RSA authentication. This causes PKMv2 authorization flow disorder, it needs to uniform PKMv2 authorization flow. To uniform PKMv2 authorization flow, SAs should be negotiated through 3 way SA-TEK exchange in every authorization policy. This contribution proposes a uniform PKMv2 authorization flow:
    a) BS and MS mutual authenticate the other's identity in RSA and/or EAP authentication. Several attributes (such as security-capabilities, SAID, and SA-Descriptors) are omitted in RSA authentication.
    b) BS and MS derive AK from PAK and/or PMK.
    c) BS and MS negotiate SAs and TEKs through 3 way SA-TEK exchange.
2. In PKMv1 RSA authentication, if BS fails to authenticate MS, BS will inform MS by sending Auth-reject message. But in PKMv2 RSA authentication, there doesn't define PKMv2 Auth-reject message.

2. Proposed solutions

See **Specific text changes** for details.

3. Specific text changes

=== Start text changes ====

6.3.2.3.9.12 Auth-Request message

Code: 21

Attributes are shown in Table 37b.

Table 37b— Auth-Request attributes

Attribute	Contents
SS_Random	A 64-bit random number generated in the MS
SS_Certificate	Contains the MS's X.509 user certificate
~~Security_Capabilities~~	~~Describes requesting MS's security capabilities~~

AAID/SAID	Either the AAID or the Basic CID if in initial network entry

The MS-certificate attribute contains an X.509 MS certificate (see 7.6) issued by the MS's manufacturer. The MS's X.509 certificate and Security Capabilities attribute is as defined in 6.3.2.3.9.2.

6.3.2.3.9.13 Auth-Reply message

Sent by the BS to a client MS in response to an Authorization Request, the Authorization Reply message contains an pre-AK, the key's lifetime, the key's sequence number~~, and a list of SA-Descriptors identifying the Primary and Static SAs the requesting MS is authorized to access and their particular properties (e.g., type, cryptographic suite)~~. The pre-AK shall be encrypted with the MS'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 37c.

Table 37c— Auth-Reply attributes

Attribute	contents
MS_Random	A 64-bit random number generated in the MS
BS_Random	A 64-bit random number generated in the BS
Encryptedpre-AK	RSA-OAEP-Encrypt(PubKey(MS), pre-PAK | Id(MS))
PAK Lifetime	PAK Aging timer
PAK Sequence Number	64-bit PAK sequence number
~~(one or more) SA-Descriptor(s)~~	~~The primary SA and zero or more static SAs . Each compound SA-Descriptor attribute specifies an SAID and additional properties of the SA (optional, only if there is no EAP phase afterwards)~~
CertBS	The BS Certificate
SigBS	An RSA signature over all the other attributes in the PKMv2 Auth reply message.

6.3.2.3.9. x Authorization Reject (Auth Reject) message

The BS responds to an SS's authorization request with an Authorization Reject message if the BS rejects the SS's authorization request.

Code : x

Attributes are shown in Table x.

Table x – Auth Reject attributes

Attribute	Contents
MS_Random	A 64-bit random number generated in the MS
BS_Random	A 64-bit random number generated in the BS
Error-Code	Error code identifying reason for rejection of authorization request

Display-String(optional)	Display String providing reason for rejection of authorization request
CertBS	The BS Certificate
SigBS	An RSA signature over all the other attributes in the PKMv2 Auth reply message.

The Error-Code and Display-String attributes describe to the requesting SS the reason for the authorization failure.

7.8.2 BS and MS mutual authentication and AK exchange overview

The BS mutual authentication can take place in one of two modes of operation. In one mode, only mutual authentication is used. In the other mode, the mutual authentication is followed by EAP authentication. In this second mode, the mutual authentication is performed only for initial network entry and only EAP authentication is performed in the case that authentication is needed in re-entry.

MS mutual authorization, controlled by the PKMv2 Authorization state machine, is the process of

a) The BS authenticating a client MS's identity
b) The MS authenticating the BS's identity
c) The BS providing the authenticated MS with an ~~AK~~ pre-PAK, from which a key encryption key (KEK) and message authentication keys are derived
~~d) The BS providing the authenticated MS with the identities (i.e., the SAIDs) and properties of primary and static SAs the MS is authorized to obtain keying information for.~~

After achieving initial authorization, an MS periodically seeks reauthorization with the BS; reauthorization is also managed by the MS's PKMv2 Authorization state machine. An MS must maintain its authorization status with the BS in order to be able to refresh aging TEKs and GTEKs. TEK state machines manage the refreshing of TEKs.

The MS sends an Authorization Request message to its BS immediately after sending the Authentication Information message. This is a request for an AK , ~~as well as for the SAIDs identifying any Static Security SAs the MS is authorized to participate in.~~ The Authorization Request includes (see 6.3.2.3.9.19)

a) A manufacturer-issued X.509 certificate.
~~b) A description of the cryptographic algorithms the requesting MS supports; an MS's cryptographic capabilities are presented to the BS as a list of cryptographic suite identifiers, each indicating a particular pairing of packet data encryption and packet data authentication algorithms the MS supports.~~
~~c)~~ b)~~T~~the MS's Basic CID. The Basic CID is the first static CID the BS assigns to an MS during initial ranging-the primary SAID is equal to the Basic CID.
~~d)~~ c)A 64-bit random number generated in the MS.

In response to an Authorization Request message, a BS validates the requesting MS's identity, ~~determines the encryption algorithm and protocol support it shares with the MS~~, activates an ~~AK~~ pre-PAK for the MS, encrypts it with the MS's public key, and sends it back to the MS in an Authorization Reply message. Random numbers are included in the exchange to ensure liveness. The Authorization Reply includes (see 6.3.2.3.9.20)

a) The BS's X.509 certificate, used to verify the BS's identity.
b) A pre-PAK encrypted with the MS's public key.
c) A 64-bit PAK sequence number, used to distinguish between successive generations of AKs.
d) A PAK lifetime.
~~e) The identities (i.e., the SAIDs) and properties of the single primary and zero ormore static SAs the MS is authorized to obtain keying information for.~~
~~f)~~ e) The 64-bit random number generated in the MS.
~~g)~~ f) A 64-bit random number generated in the BS, used to ensure key of liveness along with the random number of MS.
~~h)~~ g) The RSA signature over all the other attributes in the auth-reply message by BS, used to assure the reality of two PKMv2 authorization messages.

An MS shall periodically refresh its AK by reissuing an Authorization Request to the BS. Reauthorization is identical to authorization. To avoid service interruptions during reauthorization, successive generations of the MS's AKs have overlapping lifetimes. Both MS and BS shall be able to support up to two simultaneously active AKs during these transition periods. The operation of the Authorization state machine's Authorization Request scheduling algorithm, combined with the BS's regimen for updating and using a client ~~MS~~MS's AKs (see 7.4), ensures that the MS can refresh TEK keying information without interruption over the course of the MS's reauthorization periods.

=== End text changes ====

4. References

[1] IEEE Standard 802.16e/D7-2004
[2] IEEE Standard 802.16-2004