Project	**IEEE 802.16 Broadband Wireless Access Working Group** <http://ieee802.org/16>
Title	**Clarification on AAI-PKM-REQ/RSP message over IEEE 802.16.1a**
Date Submitted	**2012-03-14**
Source(s)	Eunkyung Kim, Sungcheol Chang, Won-Ik Kim, Seokki Kim, Sungkyung Kim, Miyoung Yun, Hyun Lee, Chulsik Yoon, Kwangjae Lim ETRI Voice: +82-42-860-5415 E-mail: ekkim@etri.re.kr scchang@etri.re.kr
Re:	"IEEE 802.16-12-0142," in response to Letter Ballot #38 on P802.16.1a/D1
Abstract	AAI-PKM-REQ/RSP message on GRIDMAN Draft Standard
Purpose	To discuss and adopt the proposed text in the draft amendment document on GRIDMAN
Notice	*This document does not represent the agreed views of the IEEE 802.16 Working Group or any of its subgroups*. It represents only the views of the participants listed in the "Source(s)" field above. It is offered as a basis for discussion. It is not binding on the contributor(s), who reserve(s) the right to add, amend or withdraw material contained herein.
Copyright Policy	The contributor is familiar with the IEEE-SA Copyright Policy <http://standards.ieee.org/IPR/copyrightpolicy.html>.
Patent Policy and Procedures	The contributor is familiar with the IEEE-SA Patent Policy and Procedures: <http://standards.ieee.org/guides/bylaws/sect6-7.html#6> and <http://standards.ieee.org/guides/opman/sect6.html#6.3>. Further information is located at <http://standards.ieee.org/board/pat/pat-material.html> and <http://standards.ieee.org/board/pat>.

Clarification on AAI-PKM-REQ/RSP message over IEEE 802.16.1a

Eunkyung Kim, Sungcheol Chang, Won-Ik Kim, Seokki Kim, Sungkyung Kim, Miyoung Yun, Hyun Lee, Chulsik Yoon, Kwangjae Lim
ETRI

1. Introduction

This document provides clarification on the AAI-PKM-REQ/RSP message and ASN.1 coding thereof.

2. References

[1] IEEE 802.16-12-0132-00, GRIDMAN System Requirement Document including SARM annex, January 2012.
[2] IEEE P802.16n™/D1, Air Interface for Broadband Wireless Access Systems - Draft Amendment: Higher Reliability Networks, February 2012.
[3] IEEE P802.16.1a™/D1, WirelessMAN-Advanced Air Interface for Broadband Access Systems - Draft Amendment: Higher Reliability Networks, February 2012.
[4] EEE P802.16Rev3/D4, IEEE Draft Standard for Local and metropolitan area networks; Part 16: Air Interface for Fixed and Mobile Broadband Wireless Access Systems," February 2012.
[5] IEEE P802.16.1™/D4, IEEE Draft for WirelessMAN-Advanced Air Interface for Broadband Wireless Access Systems, February 2012.

3. Proposed Text on the IEEE 802.16.1a Amendment Draft Standard

[----------Start of Text Proposal----------]

[*Remedy1: Change 6.2.3.32 Privacy key MAC control message in page 26 on P802.16.1a/D1 as follows:*]

6.2.3.32 Privacy key MAC control message (AAI-PKM-REQ/AAI-PKM-RSP)

Change Table 69, AAI-PKM-REQ message field description, as indicated:

Table 69 - AAI-PKM-REQ message field description

Field	Size (bits)	Value/Description	Condition
PKM v3 message type code	4	- PKMv3 Reauth-Request; PKM v3 message code = 1 - PKMv3 EAP-Transfer; PKM v3 message code = 2 -PKMv3 Key_Agreement-MSG#2; PKM v3 message code = 4 - PKMv3 TEK-Request; PKM v3 message code = 6 - PKMv3 TEK-Invalid; PKM v3 message code =8 ~~9–16: *Reserved*~~ - Peer_KeyAgreement_MSG #2; PKM v3 message code = 10 - PKMv3 MulticastKey-Request; PKM v3 message code = 12 14~~9~~–16: *Reserved*	
PKM identifier	8	A value used to match an ABS response to the AMS requests or an AMS response to the ABS requests	
CMAC indicator	1	Indicates whether this message is protected by CMAC tuple 0: Not protected 1: Protected	Shall always be present
If(PKM v3 message code ==2) {			
EAP payload	variable (1..1400 x8)	Contains the EAP authentication data, not interpreted in the MAC	
}			
If(PKM v3 message code == 4) {			
…			
…			
If(PKM v3 message code == 8) {			
SAID	8	Security association identifier	

Table 69 - AAI-PKM-REQ message field description

Field	Size (bits)	Value/Description	Condition
}			
If(PKM v3 message code == 10) {			
Key Agreement Type	~~8~~1	Indicates whether this message is for which type of Direct communications key agreement 0: Pre-shared key 1: PKI ~~2-255: *Reserved*~~	
If(Key Agreement Type == 0) {			
NONCE_HR-MS1	64	A random number of 64 bits used for freshness	
NONCE_HR-MS2	64	A random number of 64 bits used for freshness	
DAKID	64	identifies the direct communications authorization key	
size of ICV	1	0: size of ICV = 32 bits (default; Max Invalid value is 4096) 1: size of ICV = 64 bits (Max Invalid value is not used)	
PN window Size	16	The receiver shall track PNs within this window to prevent replay attacks	
}			
If(Key Agreement Type == 1) {			
Timestamp_HR-MS2	32	Timestamp	
NONCE_HR-MS2	64	A random number of 64 bits used for freshness	
HR-MS1Addr	48	MAC Address	
HR-MS2Addr	48	MAC Address	
NONCE_HR-MS1	64	A random number of 64 bits used for freshness	
Encrypted DMK	1024	Public key encryption using HR-MS1's Public key	

Table 69 - AAI-PKM-REQ message field description

Field	Size (bits)	Value/Description	Condition
SigHR-MS2	1024	Signature of message generated by using its RSA private key	
HR-MS2_Certificate	1024	RSA Digital certificate	
}			
}			
If (PKM v3 message code == 12) {			
~~MulticastGrpID~~	~~16~~	~~The identifier of the multicast group 12bits of MSB is MGID and 4bit LSB is FID of the multicast group~~	
Multicast Group ID	12	Multicast Group ID	
FID	4	FID	
}			

Change Table 70, AAI-PKM-RSP message field description, as indicated:

Table 70 - AAI-PKM-RSP message field description

Field	Size (bits)	Value/Description	Condition
PKM v3 message type code	4	- PKMv3 EAP-Transfer; PKM v3 message code =2 - PKMv3 Key_Agreement-MSG#1; PKM v3 message code =3 - PKMv3 Key_Agreement-MSG#3; PKM v3 message code =5 - PKMv3 TEK-Reply; PKM v3 message code =7 - PKMv3 TEK-Invalid; PKM v3 message code =8 ~~9–16: *Reserved*~~ - Peer_KeyAgreement_MSG #1; PKM v3 message code = 9 - Peer_KeyAgreement_MSG #3; PKM v3 message code = 11 - PKMv3 MulticastKey-Reply; PKM v3 message code = 13 14~~9~~–16: *Reserved*	
PKM identifier	8	A value used to match an ABS response to the AMS requests or an AMS response to the ABS requests or an HR-MS response to another HR-MS request	
CMAC indicator	1	Indicates whether this message is protected by CMAC tuple 0: Not protected 1: Protected	Shall always be present
If(PKM v3 message code ==2) {			
EAP payload	variable (1..140 0 x8)	Contains the EAP authentication data, not interpreted in the MAC	
}			
If(PKM v3 message code == 3) {			
…			
…			
}			

Table 70 - AAI-PKM-RSP message field description

Field	Size (bits)	Value/Description	Condition
If(PKM v3 message code == 8) {			
SAID			
}			
If(PKM v3 message code == 9) {			
Key Agreement Type	~~8~~1	Indicates whether this message is for which type of Direct communications key agreement 0: Pre-shared key 1: PKI ~~2-255: *Reserved*~~	
If(Key Agreement Type == 0) {			
NONCE_HR-MS1	64	A random number of 64 bits used for freshness	
DAKID	64	identifies the direct communications authorization key	
Key_lifetime	32	DMK key lifetime	
}			
If(Key Agreement Type == 1) {			
Timestamp_HR-MS1	32	Timestamp	
NONCE_HR-MS1	64	A random number of 64 bits used for freshness	
HR-MS2Addr	48	MAC Address	
HR-MS1Addr	48	MAC Address	
SigHR-MS1	1024	Signature of message generated by using its RSA private key	
HR-MS1_Certificate	1024	RSA Digital certificate	
~~}~~			
}			
}			

Table 70 - AAI-PKM-RSP message field description

Field	Size (bits)	Value/Description	Condition
If(PKM v3 message code == 11) {			
Key Agreement Type	~~8~~1	Indicates whether this message is for which type of Direct communications key agreement 0: Pre-shared key 1: PKI ~~2: BS-to-BS security~~ ~~3-255: *Reserved*~~	
If(Key Agreement Type == 0) {			
NONCE_HR-MS1	64	A random number of 64 bits used for freshness	
NONCE_HR-MS2	64	A random number of 64 bits used for freshness	
size of ICV	1	0: size of ICV = 32 bits (default; Max Invalid value is 4096) 1: size of ICV = 64 bits (Max Invalid value is not used)	
PN window Size	16	The receiver shall track PNs within this window to prevent replay attacks	
}			
If(Key Agreement Type == 1) {			
NONCE_HR-MS2	64	A random number of 64 bits used for freshness	
HR-MS2Addr	48	MAC Address	
HR-MS1Addr	48	MAC Address	
~~}}~~			
}			
}			
If (PKM v3 message code == 13) {			

Table 70 - AAI-PKM-RSP message field description

Field	Size (bits)	Value/Description	Condition
~~MulticastGrpID~~	~~16~~	~~The identifier of the multicast group 12bits of MSB is MGID and 4bit LSB is FID of the multicast group~~	
Multicast Group ID	12	Multicast Group ID	
FID	4	FID	
MC_Nonce	128	The number used to derive the MCMAC-MTEK ~~Preky~~Prekey	
COUNTER_MTEK	16	The current COUNTER_MTEK in use	
MEKS	2	Multicast Encryption Key Sequence	
}			

[*Remedy2: Add the following text in Annex in page 212 on P802.16.1a/D1*]

Annex A

...

A.2 MAC control message definitions (normative)

Change Annex A.2 as indicated:

```
WirelessMAN-Advanced-Air-Interface DEFINITIONS AUTOMATIC TAGS ::=

BEGIN

-- MAC Control Messages

MAC-Control-Message ::=       SEQUENCE {
        message MAC-Control-Msg-Type,
...

}

MAC-Control-Msg-Type ::=      CHOICE {
        -- System information
        aaiSCD                          AAI-SCD,
        aaiSIIAdv                       AAI-SII-ADV,
        aaiULPCNi                       AAI-ULPC-NI,
        -- Network entry / re-entry
        aaiRngReq                       AAI-RNG-REQ,
        aaiRngRsp                       AAI-RNG-RSP,
        aaiRngAck                       AAI-RNG-ACK,
        aaiRngCfm                       AAI-RNG-CFM,
        aaiSbcReq                       AAI-SBC-REQ,
```

```
aaiSbcRsp                       AAI-SBC-RSP,
aaiRegReq                       AAI-REG-REQ,
aaiRegRsp                       AAI-REG-RSP,
-- Network exit
aaiDregReq                      AAI-DREG-REQ,
aaiDregRsp                      AAI-DREG-RSP,
-- Connection management
aaiDsaReq                       AAI-DSA-REQ,
aaiDsaRsp                       AAI-DSA-RSP,
aaiDsaAck                       AAI-DSA-ACK,
aaiDscReq                       AAI-DSC-REQ,
aaiDscRsp                       AAI-DSC-RSP,
aaiDscAck                       AAI-DSC-ACK,
aaiDsdReq                       AAI-DSD-REQ,
aaiDsdRsp                       AAI-DSD-RSP,
aaiGrpCfg                       AAI-GRP-CFG,
-- Security
aaiPkmReq                       AAI-PKM-REQ,
aaiPkmRsp                       AAI-PKM-RSP,
-- ARQ
aaiArqFbk                       AAI-ARQ-FBK,
aaiArqDsc                       AAI-ARQ-DSC,
aaiArqRst                       AAI-ARQ-RST,
-- Sleep mode
aaiSlpReq                       AAI-SLP-REQ,
aaiSlpRsp                       AAI-SLP-RSP,
aaiTrfInd                       AAI-TRF-IND,
aaiTrfIndReq                    AAI-TRF-IND-REQ,
aaiTrfIndRsp                    AAI-TRF-IND-RSP,
-- Handover
aaiHoInd                        AAI-HO-IND,
aaiHoReq                        AAI-HO-REQ,
aaiHoCmd                        AAI-HO-CMD,
aaiNbrAdv                       AAI-NBR-ADV,
aaiScnReq                       AAI-SCN-REQ,
aaiScnRsp                       AAI-SCN-RSP,
aaiScnRep                       AAI-SCN-REP,
-- Idle mode
aaiPagAdv                       AAI-PAG-ADV,
aaiPgidInfo                     AAI-PGID-INFO,
-- Multicarrier
aaiMcAdv                        AAI-MC-ADV,
aaiMcReq                        AAI-MC-REQ,
aaiMcRsp                        AAI-MC-RSP,
aaiCmCmd                        AAI-CM-CMD,
aaiCmInd                        AAI-CM-IND,
aaiGlobalConfig                 AAI-GLOBAL-CFG,
-- Power Control
aaiUlPowerAdj                   AAI-UL-POWER-ADJ,
aaiUlPsrConfig                  AAI-UL-PSR-CFG,
-- Collocated Coexistence
aaiClcReq                       AAI-CLC-REQ,
aaiClcRsp                       AAI-CLC-RSP,
-- MIMO
aaiSbsMimoFbk                   AAI-SBS-MIMO-FBK,
aaiMbsMimoFbk                   AAI-MBS-MIMO-FBK,
aaiMbsMimoReq                   AAI-MBS-MIMO-REQ,
aaiMbsMimoRsp                   AAI-MBS-MIMO-RSP,
aaiMbsMimoSbp                   AAI-MBS-MIMO-SBP,
```

```
        aaiMbsSoundingCal              AAI-MBS-SOUNDING-CAL,
        aaiDlIm                        AAI-DL-IM,
        -- FFR
        aaiFfrCmd                      AAI-FFR-CMD,
        aaiFfrRep                      AAI-FFR-REP,
        -- SON
        aaiSonAdv                      AAI-SON-ADV,
        -- Relay
        aaiARSCfgCmd                   AAI-ARS-CFG-CMD,
        -- EMBS
        aaiEmbsCfg                     AAI-EMBS-CFG,
        aaiEmbsRep                     AAI-EMBS-REP,
        aaiEmbsRsp                     AAI-EMBS-RSP,
        -- LBS
        aaiLbsAdv                      AAI-LBS-ADV,
        aaiLbsInd                      AAI-LBS-IND,
        -- Misc
        aaiL2Xfer                      AAI-L2-XFER,
        aaiMsgAck                      AAI-MSG-ACK,
        aaiResCmd                      AAI-RES-CMD,
        ...
}

-- *-*-*-*-*-*-*-*-*-*-*-*-*-*-*-*-*-*-*-*-*-*-*-*-*-*-*-*-*-
-- Common type definitions
-- *-*-*-*-*-*-*-*-*-*-*-*-*-*-*-*-*-*-*-*-*-*-*-*-*-*-*-*-*-

PhyCarrierIndex ::=            INTEGER (0..62)



..................


-- +-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-
-- Group Configuration
-- +-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-
-- Group Configuration
AAI-GRP-CFG ::=                SEQUENCE {
        deletionFlag                   ENUMERATED {
                                               flowAdded,
                                               flowDeleted
                                       },
        dlULIndicator                  ENUMERATED {
                                               dlAllocation,
                                               ulAllocation
                                       },
        flowID                         FID,
        burstSize                      INTEGER (0..31)                               OPTIONAL,
        graInfo                        CHOICE {
                graInfoForDeletededFlow        NULL,
                graInfoForAddedFlow            GroupResourceAllocInfo
        },
        ...

}



-- *-*-*-*-*-*-*-*-*-*-*-*-*-*-*-*-*-*-*-*-*-*-*-*-*-*-*-*-*-
```

```
-- Security Messages
-- *-*-*-*-*-*-*-*-*-*-*-*-*-*-*-*-*-*-*-*-*-*-*-*-*-*-*-*-*-*-
PKMID ::=                      INTEGER (0..255)
AKID ::=                       BIT STRING (SIZE (64))
SAID ::=                       INTEGER (0..255)
KeyLifetime ::=                INTEGER (0..4294967295)
CounterTEK ::=                 INTEGER (0..65535)
EKS ::=                        INTEGER (0..3)
Nonce ::=                      BIT STRING (SIZE (64))
MulticastNonce ::=             BIT STRING (SIZE (128))
TimeStamp ::=                  INTEGER (0..4294967295)
EncryptedDMK ::=               BIT STRING (SIZE (1024))
Signature ::=                  BIT STRING (SIZE (1024))
Certificate ::=                BIT STRING (SIZE (1024))

PKM-ReauthRequest ::=          SEQUENCE {
       cmacIndicator                  CMACI,
       ...
}
PKM-EAPTransfer ::=            SEQUENCE {
       eapPayload                     OCTET STRING (SIZE (1..1400)),
       ...
}
PKM-KeyAgreementMsg1 ::=       SEQUENCE {
       nonceABS                       Nonce,
       akID                           AKID,
       keyLifetime                    KeyLifetime,
       cmacIndicator                  CMACI,
       ...
}
PKM-KeyAgreementMsg2 ::=       SEQUENCE {
       nonceABS                       Nonce,
       nonceAMS                       Nonce,
       akID                           AKID,
       securityNegoParameters         SecurityNegotiationPara                      OPTIONAL,
       cmacIndicator  CMACI,
       ...
}
PKM-KeyAgreementMsg3 ::=       SEQUENCE {
       nonceABS                              Nonce,
       nonceAMS                              Nonce,
       supportingSAs                  SupportingSAs                                OPTIONAL,
       securityNegoParameters SecurityNegotiationPara OPTIONAL,
       cmacIndicator                  CMACI,
       ...
}
PKM-TEKRequest ::=             SEQUENCE {
       said                                  SAID,
       tekRefreshFlag          ENUMERATED {
                                      secondTEKUpdate,
                                      firstTEKUpdate
                               }                                                   OPTIONAL,
       cmacIndicator           CMACI,
       ...
}
PKM-TEKReply ::=               SEQUENCE {
       said                           SAID,
       counterTEK                     CounterTEK,
       eks                            EKS,
```

```
        cmacIndicator                   CMACI,
        ...
}
PKM-TEKInvalid ::=              SEQUENCE {
        said                            SAID,
        cmacIndicator                   CMACI,
        ...
}

-- for HR-Network
Peer-KeyAgreementMsg1 ::=       SEQUENCE {
        keyAgreementType                CHOICE {
                preSharedKey                    PreSharedKey1,
                pki                             PKI1,
                ...
        },
        ...
}
Peer-KeyAgreementMsg2 ::=       SEQUENCE {
        keyAgreementType                CHOICE {
                preSharedKey                    PreSharedKey2,
                pki                             PKI2,
                ...
        },
        ...
}
Peer-KeyAgreementMsg3 ::=       SEQUENCE {
        keyAgreementType                CHOICE {
                preSharedKey                    PreSharedKey2,
                pki                             PKI3,
                ...
        },
        ...
}
PKM-MulticastKeyRequest ::=     SEQUENCE {
        multicastGroupID                MulticastGroupID,
        fid                             FID,
        ...
}
PKM-MulticastKeyReply ::=       SEQUENCE {
        multicastGroupID                MulticastGroupID,
        fid                             FID,
        mcNonce                         MulticastNonce,
        counterMtek                     CounterTEK,
        meks                            EKS,
        ...
}
SecurityNegotiationPara ::=     SEQUENCE {
        sizeOfICV                       ENUMERATED {
                                                thirtyTwoBits,
                                                sixtyFourBits
                                        },
        windowSize                      INTEGER (0..65535)
}
SupportingSAs ::=               BIT STRING {
                                        nullSASupported         (0),
                                        said1Supported          (1),
                                        said2Supported          (2)
                                } (SIZE (3))
```

```
PreSharedKey1 ::=               SEQUENCE {
        nonceHRMS1                      Nonce,
        dakID                           AKID,
        keyLifetime                     KeyLifetime
}
PKI1 ::=                        SEQUENCE {
        timestampHRMS1                  TimeStamp,
        nonceHRMS1                      Nonce,
        macAddressHRMS2                 MACAddress,
        macAddressHRMS1                 MACAddress,
        sigHRMS1                        Signature,
        certificateHRMS1                Certificate
}

PreSharedKey2 ::=               SEQUENCE {
        nonceHRMS1                      Nonce,
        nonceHRMS2                      Nonce,
        dakID                           AKID,
        securityNegoParameters          SecurityNegotiationPara
}
PKI2 ::=                                SEQUENCE {
        timestampHRMS2                  TimeStamp,
        nonceHRMS2                      Nonce,
        macAddressHRMS1                 MACAddress,
        macAddressHRMS2                 MACAddress,
        nonceHRMS1                      Nonce,
        encryptedDMK                    EncryptedDMK,
        sigHRMS2                        Signature,
        certificateHRMS2                Certificate
}
PKI3 ::=                        SEQUENCE {
        nonceHRMS2                      Nonce,
        macAddressHRMS2                 MACAddress,
        macAddressHRMS1                 MACAddress
}

-- +-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-
-- Privacy Key Management Request
-- +-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-
AAI-PKM-REQ ::=                 SEQUENCE {
       pkmid                            PKMID,
       pkmMessage                       CHOICE {
               reauthRequest                    PKM-ReauthRequest,
               eapTransfer                      PKM-EAPTransfer,
               keyAgreementMsg2                 PKM-KeyAgreementMsg2,
               tekRequest                       PKM-TEKRequest,
               tekInvalid                       PKM-TEKInvalid,
               peerKeyAgreementMsg2             Peer-KeyAgreementMsg2,
               multicastKeyRequest              PKM-MulticastKeyRequest,
               ...
       },
       ...
}
-- +-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-
-- Privacy Key Management Response
-- +-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-
AAI-PKM-RSP ::=                 SEQUENCE {
       pkmid PKMID,
```

```
                pkmMessage              CHOICE {
                        eapTransfer             PKM-EAPTransfer,
                        keyAgreementMsg1        PKM-KeyAgreementMsg1,
                        keyAgreementMsg3        PKM-KeyAgreementMsg3,
                        tekReply                PKM-TEKReply,
                        tekInvalid              PKM-TEKInvalid,
                        peerKeyAgreementMsg1    Peer-KeyAgreementMsg1,
                        peerKeyAgreementMsg3    Peer-KeyAgreementMsg3,
                        multicastKeyReply       PKM-MulticastKeyReply,
                        ...
                },
        ...
}

...................

END
```

[----------End of Text Proposal----------]