Project	**IEEE 802.16 Broadband Wireless Access Working Group <http://ieee802.org/16>**
Title	**Proposed text and ASN.1 code to support PKMV1 and PKMV2**
Date Submitted	**2007-01-18**
Source(s)	Joey Chou Intel Corporation [mailto:joey.chou@intel.com]
Re:	
Abstract	This contribution proposes the text and ASN.1 code in wmanIf2Mib to support PKMV1 and PKMV2.
Purpose	Adoption
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 (Version 1.0) <http://ieee802.org/16/ipr/patents/policy.html>, including the statement "IEEE standards may include the known use of patent(s), including patent applications, if there is technical justification in the opinion of the standards-developing committee and provided the IEEE receives assurance from the patent holder that it will license applicants under reasonable terms and conditions for the purpose of implementing 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:r.b.marks@ieee.org> as early as possible, in written or electronic form, of any patents (granted or under application) that may cover technology that is under consideration by or has been approved by IEEE 802.16. The Chair will disclose this notification via the IEEE 802.16 web site <http://ieee802.org/16/ipr/patents/notices>.

Table of Content

1

1. Introduction

This contribution proposes the text and ASN.1 code in wmanIf2Mib to support PKMV1 and PKMV2.

2. NRM IRP SNMP Solution Set change Proposal

2.1 wmanIf2BsPkmObjects Changes

13.1.3.1 wmanIf2BsObjects

[Replace Subclause 13.1.3.1.3 as the following:]

13.1.3.1.3 wmanIf2BsPkmObjects

Figure 8 shows the structure of wmanIf2BsPkmObjects subtree that contains BS managed objects related to the MAC privacy management entity.

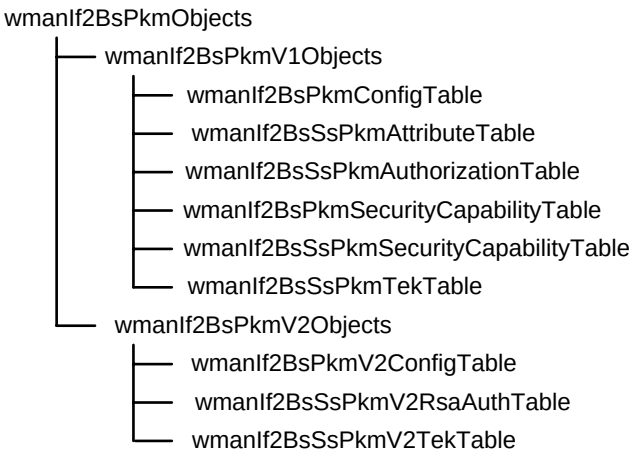

Figure 8— wmanIf2BsPkmObjects structure

13.1.3.1.3.1 wmanIf2BsPkmV1Objects

13.1.3.1.3.1.1 wmanIf2BsPkmConfigTable

wmanIf2BsPkmConfigTable contains the configuration of the PKM attributes that are to be used for BS and all SSs that are connected to such BS .

13.1.3.1.3.1.2 wmanIf2BsSsPkmAttributeTable

wmanIf2BsSsPkmAttributeTable contains the PKM attributes on per SS basis.

13.1.3.1.3.1.3 wmanIf2BsSsPkmAuthorizationTable

wmanIf2BsSsPkmAuthorizationTable contains information related to SS's authorization process.

13.1.3.1.3.1.4 wmanIf2BsPkmSecurityCapabilityTable

wmanIf2BsSsPkmSecurityCapabilityTable contains the list of the cryptographic suite(s) an BS supports.

13.1.3.1.3.1.5 wmanIf2BsSsPkmSecurityCapabilityTable

wmanIf2BsSsPkmSecurityCapabilityTable contains the SS's Security Capabilities that are conveyed by the Auth Request message. It contains the list of the cryptographic suite(s) an SS supports.

13.1.3.1.3.1.6 wmanIf2BsSsPkmTekTable

wmanIf2BsSsPkmTekTable contains the TEK attributes that are associated with each SAID.

13.1.3.1.3.2 wmanIf2BsPkmV2Objects

13.1.3.1.3.2.1 wmanIf2BsPkmV2ConfigTable

wmanIf2BsPkmV2ConfigTable contains the PKM attributes that are needed to PKM operation.

13.1.3.1.3.2.2 wmanIf2BsSsPkmV2RsaAuthTable

wmanIf2BsSsPkmV2RsaAuthTable contains information related to PKMV2 RSA based authorization process.

13.1.3.1.3.2.3 wmanIf2BsSsPkmV2TekTable

wmanIf2BsSsPkmV2TekTable contains the TEK attributes that are associated with each SAID.

2.2 wmanIf2SsPkmObjects Changes

13.1.3.1 wmanIf2BsObjects

[Replace Subclause 13.1.3.2.2 as the following:]

13.1.3.2.2 wmanIf2SsPkmObjects

Figure 12 shows the structure of wmanIf2SsPkmObjects subtree that contains subscriber station manageable objects related to the privacy management entity.

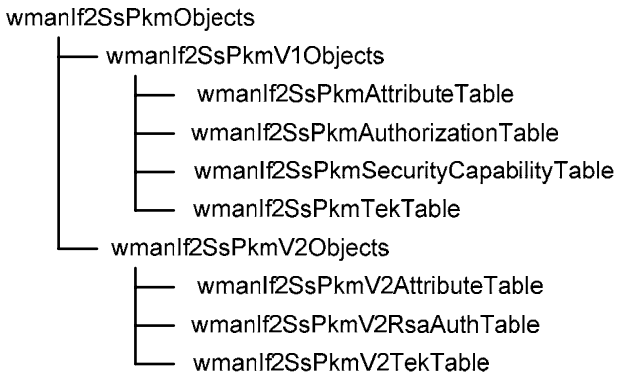

Figure 12— wmanIf2SsPkmObjects structure

13.1.3.2.2.1 wmanIf2BsPkmV1Objects

13.1.3.2.2.1.1 wmanIf2SsPkmAttributeTable

wmanIf2SsPkmAttributeTable provides the configuration of the PKM attributes that are needed to PKM operation.

13.1.3.2.2.1.2 wmanIf2SsPkmAuthorizationTable

wmanIf2SsPkmAuthorizationTable contains information that are related to SS's authorization proces.

13.1.3.2.2.1.3 wmanIf2SsPkmSecurityCapabilityTable

wmanIf2SsPkmSecurityCapabilityTable contains the SS's Security Capabilities that are conveyed by the Auth Request message. It contains the list of the cryptographic suite(s) an SS supports.

13.1.3.2.2.1.4 wmanIf2SsPkmTekTable

wmanIf2SsPkmTekTable contains the TEK attributes that are associated with each SAID.

13.1.3.2.2.2 wmanIf2BsPkmV2Objects

13.1.3.2.2.2.1 wmanIf2SsPkmV2AttributeTable

wmanIf2SsPkmV2AttributeTable contains the PKM attributes that are needed to PKM operation.

13.1.3.2.2.2.2 wmanIf2SsPkmV2RsaAuthTable

wmanIf2SsPkmV2RsaAuthTable contains information related to PKMV2 RSA based authorization process.

13.1.3.2.2.2.3 wmanIf2SsPkmV2TekTable

wmanIf2SsPkmV2TekTable contains the TEK attributes that are associated with each SAID.

2.3 wmanIf2BsPkmObjects ASN.1 Code Change

13.2 ASN.1 Definitions of MIB Modules

13.2.3 wmanIf2Mib

[Replace wmanIf2BsPkmObjects to the following in WMAN-IF2-MIB:]

```
WmanIf2PkmErrorCode ::= TEXTUAL-CONVENTION
        STATUS      current
        DESCRIPTION
            "This error code provides further information about an
             Authorization Reject, Key Reject, Authorization Invalid,
             or TEK Invalid.

               0 - no failure
               1 - unauthorized SS
               2 - unauthorized SAID
               3 - unsolicited
               4 - invalid key sequence
               5 - key request authentication failure

             The following are error code for permanent authorization
             failure that indicates any reattempts at authorization
             would continue to result in Authorization Rejects.

               6 - the BS does not have the CA certificate belonging
                   to the issuer of an SS certificate
               7 - SS certificate has an invalid signature
               8 - ASN.1 parsing failure during verification of SS
                   certificate
               9 - SS certificate is on the 'hot list'
               10 - inconsistencies between certificate data and data
                   in accompanying PKM attributes
               11 - SS and BS have incompatible security capabilities"
        REFERENCE
            "Subclause 11.9.10 in IEEE Std 802.16-2004"
        SYNTAX      INTEGER {noFailure(0),
                             unauthorizedSs(1),
                             unauthorizedSaid(2),
                             unsolicited(3),
                             invalidKeySequence(4),
                             keyReqAuthFailure(5),
                             umknownManufactur(6),
                             invalidSignature(7),
                             asn1ParsingFailure(8),
                             ssCaOnHotList(9),
                             dataInconsistency(10),
                             ssBsIncompatibleSc(11)}


WmanIf2SaType ::= TEXTUAL-CONVENTION
        STATUS      current
        DESCRIPTION
            "The type of Security Association (SA)."
        REFERENCE
            "Table 379 in IEEE Std 802.16-2004"
        SYNTAX      INTEGER {primarySa(0),
                             staticSa(1),
                             dynamicSa(2)}
```

```
WmanIf2TekState ::= TEXTUAL-CONVENTION
        STATUS      current
        DESCRIPTION
            "TEK State."
        REFERENCE
            "Subclause 7.2.5.1 in IEEE Std 802.16-2004"
        SYNTAX      INTEGER {start(1),
                             opWait(2),
                             opReauthWait(3),
                             operational(4),
                             rekeyWait(5),
                             rekeyReauthWait(6)}


WmanIf2CertificateStat ::= TEXTUAL-CONVENTION
        STATUS      current
        DESCRIPTION
            "The reason why a SS's certificate is deemed valid
             or invalid:

             0 - return unknown if the SS is running PKM mode
             1 - means the certificate is valid because it chains
                 to a valid certificate
             2 - means the certificate is valid because it has been
                 provisioned to be trusted
             3 - means the certificate is invalid because it has been
                 provisioned to be untrusted.
             4 - means the certificate is invalid because it chains
                 to an untrusted certificate.
             5 - refer to errors in parsing, validity periods, etc,
                 of SS certificate
             6 - refer to errors in parsing, validity periods, etc,
                 of CA certificate"
        REFERENCE
            "Subclause 7.2.5.1 in IEEE Std 802.16-2004"
        SYNTAX      INTEGER {unknown (0),
                             validSsChained (1),
                             validSsTrusted (2),
                             invalidSsUntrusted (3),
                             invalidCAUntrusted (4),
                             invalidSsOther (5),
                             invalidCAOther (6)}

--
-- Base station PKM group
-- wmanIf2BsPkmObjects contain the Base Station Privacy Sublayer objects
--
wmanIf2BsPkmObjects OBJECT IDENTIFIER ::= { wmanIf2BsObjects 3 }

wmanIf2BsPkmV1Objects OBJECT IDENTIFIER ::= { wmanIf2BsPkmObjects 1 }

-- Table wmanIf2BsPkmConfigTable
--
wmanIf2BsPkmConfigTable OBJECT-TYPE
        SYNTAX      SEQUENCE OF WmanIf2BsPkmConfigEntry
        MAX-ACCESS  not-accessible
        STATUS      current
        DESCRIPTION
            "This table contains the configuration of the PKM
             attributes that are to be used for BS and SS."
        REFERENCE
            "Table 343 in IEEE Std 802.16-2004 and 802.16e-2005"
        ::= { wmanIf2BsPkmV1Objects  1 }
```

```
wmanIf2BsPkmConfigEntry OBJECT-TYPE
        SYNTAX      WmanIf2BsPkmConfigEntry
        MAX-ACCESS  not-accessible
        STATUS      current
        DESCRIPTION
            "Each entry contains objects that define the PKM attributes
             of each BS wireless interface, and all SSs that are
             connected with such BS. The table is indexed by ifIndex
             that is associated with the BS sector."
        INDEX       { ifIndex }
        ::= { wmanIf2BsPkmConfigTable  1 }

WmanIf2BsPkmConfigEntry ::= SEQUENCE {
        wmanIf2BsPkmAkLifetime                  Integer32,
        wmanIf2BsPkmTekLifetime                 Integer32,
        wmanIf2BsPkmSelfSigManufCertTrust       INTEGER,
        wmanIf2BsPkmAuthWaitTimeout             Integer32,
        wmanIf2BsPkmReauthWaitTimeout           Integer32,
        wmanIf2BsPkmAuthGraceTime               Integer32,
        wmanIf2BsPkmOpWaitTimeout               Integer32,
        wmanIf2BsPkmRekeyWaitTimeout            Integer32,
        wmanIf2BsPkmTekGraceTime                Integer32,
        wmanIf2BsPkmAuthRejectWaitTimeout       Integer32,
        wmanIf2BsPkmCheckCertValidityPeriods    TruthValue}

wmanIf2BsPkmAkLifetime OBJECT-TYPE
        SYNTAX      Integer32 (86400 .. 6048000)
        UNITS       "seconds"
        MAX-ACCESS  read-write
        STATUS      current
        DESCRIPTION
            "This object defines the lifetime of a newly assigned
             authorization key."
        REFERENCE
             "Table 343 in IEEE Std 802.16-2004"
        DEFVAL         { 604800 }
        ::= { wmanIf2BsPkmConfigEntry 1 }

wmanIf2BsPkmTekLifetime OBJECT-TYPE
        SYNTAX      Integer32 (1800 .. 604800)
        UNITS       "seconds"
        MAX-ACCESS  read-write
        STATUS      current
        DESCRIPTION
            "This object defines the lifetime of a newly assigned
             Traffic Encryption Key(TEK)."
        REFERENCE
             "Table 343 in IEEE Std 802.16-2004"
        DEFVAL         { 43200 }
        ::= { wmanIf2BsPkmConfigEntry 2 }

wmanIf2BsPkmSelfSigManufCertTrust OBJECT-TYPE
        SYNTAX      INTEGER {trusted (1),
                             untrusted (2)}
        MAX-ACCESS  read-write
        STATUS      current
        DESCRIPTION
            "This object determines the default trust of all (new)
             self-signed manufacturer certificates obtained after
             setting the object."
        ::= { wmanIf2BsPkmConfigEntry 3 }

wmanIf2BsPkmAuthWaitTimeout OBJECT-TYPE
```

```
            SYNTAX      Integer32 (2 .. 30)
            UNITS       "seconds"
            MAX-ACCESS  read-write
            STATUS      current
            DESCRIPTION
                "This object defines the Auth Req retransmission interval
                 from Auth Wait state."
            REFERENCE
                "Table 343 and subclause 11.9.19 in IEEE Std 802.16-2004"
            DEFVAL      { 10 }
            ::= { wmanIf2BsPkmConfigEntry 4 }

    wmanIf2BsPkmReauthWaitTimeout OBJECT-TYPE
            SYNTAX      Integer32 (2 .. 30)
            UNITS       "seconds"
            MAX-ACCESS  read-write
            STATUS      current
            DESCRIPTION
                "This object defines the Auth Req retransmission interval
                 from Reauth Wait state."
            REFERENCE
                "Table 343 and subclause 11.9.19 in IEEE Std 802.16-2004"
            DEFVAL      { 10 }
            ::= { wmanIf2BsPkmConfigEntry 5 }

    wmanIf2BsPkmAuthGraceTime OBJECT-TYPE
            SYNTAX      Integer32 (300 .. 3024000)
            UNITS       "seconds"
            MAX-ACCESS  read-write
            STATUS      current
            DESCRIPTION
                "The value of this object is the grace time for an
                 authorization key. A SS is expected to start trying to get
                 a new authorization key beginning AuthGraceTime seconds
                 before the authorization key actually expires."
            REFERENCE
                "Table 343 and subclause 11.9.19 in IEEE Std 802.16-2004"
            DEFVAL      { 600 }
            ::= { wmanIf2BsPkmConfigEntry 6 }

    wmanIf2BsPkmOpWaitTimeout OBJECT-TYPE
            SYNTAX      Integer32 (1 .. 10)
            UNITS       "seconds"
            MAX-ACCESS  read-write
            STATUS      current
            DESCRIPTION
                "This object defines the Key Req retransmission interval
                 from Op Wait state."
            REFERENCE
                "Table 343 and subclause 11.9.19 in IEEE Std 802.16-2004"
            DEFVAL      { 1 }
            ::= { wmanIf2BsPkmConfigEntry 7 }

    wmanIf2BsPkmRekeyWaitTimeout OBJECT-TYPE
            SYNTAX      Integer32 (1 .. 10)
            UNITS       "seconds"
            MAX-ACCESS  read-write
            STATUS      current
            DESCRIPTION
                "This object defines the Key Req retransmission interval
                 from Rekey Wait state."
            REFERENCE
                "Table 343 and subclause 11.9.19 in IEEE Std 802.16-2004"
            DEFVAL      { 1 }
```

```
            ::= { wmanIf2BsPkmConfigEntry 8 }

    wmanIf2BsPkmTekGraceTime OBJECT-TYPE
            SYNTAX      Integer32 (300 .. 3024000)
            UNITS       "seconds"
            MAX-ACCESS  read-write
            STATUS      current
            DESCRIPTION
                "The value of this object is the grace time for the TEK in
                 seconds. The SS is expected to start trying to acquire a
                 new TEK beginning TEK GraceTime seconds before the
                 expiration of the most recent TEK."
            REFERENCE
                "Table 343 and subclause 11.9.19 in IEEE Std 802.16-2004"
            DEFVAL      { 3600 }
            ::= { wmanIf2BsPkmConfigEntry 9 }

    wmanIf2BsPkmAuthRejectWaitTimeout OBJECT-TYPE
            SYNTAX      Integer32 (10 .. 600)
            UNITS       "seconds"
            MAX-ACCESS  read-write
            STATUS      current
            DESCRIPTION
                "This object defines the Delay before resending Auth Request
                 after receiving Auth Reject."
            REFERENCE
                "Table 343 and subclause 11.9.19 in IEEE Std 802.16-2004"
            DEFVAL      { 60 }
            ::= { wmanIf2BsPkmConfigEntry 10 }

    wmanIf2BsPkmCheckCertValidityPeriods OBJECT-TYPE
            SYNTAX      TruthValue
            MAX-ACCESS  read-write
            STATUS      current
            DESCRIPTION
                "Setting this object to TRUE causes all certificates
                 received thereafter to have their validity periods (and
                 their chain's validity periods) checked against the current
                 time of day. A FALSE setting will cause all certificates
                 received Thereafter to not have their validity periods
                 (nor their chain's validity periods) checked against the
                 current time of day."
            ::= { wmanIf2BsPkmConfigEntry 11 }

    -- Table wmanIf2BsSsPkmConfigTable
    --
    wmanIf2BsSsPkmAttributeTable OBJECT-TYPE
            SYNTAX      SEQUENCE OF WmanIf2BsSsPkmAttributeEntry
            MAX-ACCESS  not-accessible
            STATUS      current
            DESCRIPTION
                "This table contains the the PKM attributes that are needed
                 to PKM operation."
            REFERENCE
                "Table 343 in IEEE Std 802.16-2004 and 802.16e-2005"
            ::= { wmanIf2BsPkmV1Objects 2 }

    wmanIf2BsSsPkmAttributeEntry OBJECT-TYPE
            SYNTAX      WmanIf2BsSsPkmAttributeEntry
            MAX-ACCESS  not-accessible
            STATUS      current
            DESCRIPTION
                "Each entry contains objects that show the PKM attributes
                 of each SS wireless interface. The table is indexed by
```

```
             ifIndex and wmanIf2BsSsMacAddress."
        INDEX       { ifIndex, wmanIf2BsSsMacAddress }
        ::= { wmanIf2BsSsPkmAttributeTable  1 }

WmanIf2BsSsPkmAttributeEntry ::= SEQUENCE {
        wmanIf2BsSsPkmAuthWaitTimeout           Integer32,
        wmanIf2BsSsPkmReauthWaitTimeout         Integer32,
        wmanIf2BsSsPkmAuthGraceTime             Integer32,
        wmanIf2BsSsPkmOpWaitTimeout             Integer32,
        wmanIf2BsSsPkmRekeyWaitTimeout          Integer32,
        wmanIf2BsSsPkmTekGraceTime              Integer32,
        wmanIf2BsSsPkmAuthRejectWaitTimeout     Integer32}

wmanIf2BsSsPkmAuthWaitTimeout OBJECT-TYPE
        SYNTAX      Integer32 (2 .. 30)
        UNITS       "seconds"
        MAX-ACCESS  read-only
        STATUS      current
        DESCRIPTION
            "This object defines the Auth Req retransmission interval
             from Auth Wait state."
        REFERENCE
            "Table 343 and subclause 11.9.19 in IEEE Std 802.16-2004"
        DEFVAL      { 10 }
        ::= { wmanIf2BsSsPkmAttributeEntry 1 }

wmanIf2BsSsPkmReauthWaitTimeout OBJECT-TYPE
        SYNTAX      Integer32 (2 .. 30)
        UNITS       "seconds"
        MAX-ACCESS  read-only
        STATUS      current
        DESCRIPTION
            "This object defines the Auth Req retransmission interval
             from Reauth Wait state."
        REFERENCE
            "Table 343 and subclause 11.9.19 in IEEE Std 802.16-2004"
        DEFVAL      { 10 }
        ::= { wmanIf2BsSsPkmAttributeEntry 2 }

wmanIf2BsSsPkmAuthGraceTime OBJECT-TYPE
        SYNTAX      Integer32 (300 .. 3024000)
        UNITS       "seconds"
        MAX-ACCESS  read-only
        STATUS      current
        DESCRIPTION
            "The value of this object is the grace time for an
             authorization key. A SS is expected to start trying to get
             a new authorization key beginning AuthGraceTime seconds
             before the authorization key actually expires."
        REFERENCE
            "Table 343 and subclause 11.9.19 in IEEE Std 802.16-2004"
        DEFVAL      { 600 }
        ::= { wmanIf2BsSsPkmAttributeEntry 3 }

wmanIf2BsSsPkmOpWaitTimeout OBJECT-TYPE
        SYNTAX      Integer32 (1 .. 10)
        UNITS       "seconds"
        MAX-ACCESS  read-only
        STATUS      current
        DESCRIPTION
            "This object defines the Key Req retransmission interval
             from Op Wait state."
        REFERENCE
            "Table 343 and subclause 11.9.19 in IEEE Std 802.16-2004"
```

```
            DEFVAL      { 1 }
            ::= { wmanIf2BsSsPkmAttributeEntry 4 }

    wmanIf2BsSsPkmRekeyWaitTimeout OBJECT-TYPE
            SYNTAX      Integer32 (1 .. 10)
            UNITS       "seconds"
            MAX-ACCESS  read-only
            STATUS      current
            DESCRIPTION
                "This object defines the Key Req retransmission interval
                 from Rekey Wait state."
            REFERENCE
                "Table 343 and subclause 11.9.19 in IEEE Std 802.16-2004"
            DEFVAL      { 1 }
            ::= { wmanIf2BsSsPkmAttributeEntry 5 }

    wmanIf2BsSsPkmTekGraceTime OBJECT-TYPE
            SYNTAX      Integer32 (300 .. 3024000)
            UNITS       "seconds"
            MAX-ACCESS  read-only
            STATUS      current
            DESCRIPTION
                "The value of this object is the grace time for the TEK in
                 seconds. The SS is expected to start trying to acquire a
                 new TEK beginning TEK GraceTime seconds before the
                 expiration of the most recent TEK."
            REFERENCE
                "Table 343 and subclause 11.9.19 in IEEE Std 802.16-2004"
            DEFVAL      { 3600 }
            ::= { wmanIf2BsSsPkmAttributeEntry 6 }

    wmanIf2BsSsPkmAuthRejectWaitTimeout OBJECT-TYPE
            SYNTAX      Integer32 (10 .. 600)
            UNITS       "seconds"
            MAX-ACCESS  read-only
            STATUS      current
            DESCRIPTION
                "This object defines the Delay before resending Auth Request
                 after receiving Auth Reject."
            REFERENCE
                "Table 343 and subclause 11.9.19 in IEEE Std 802.16-2004"
            DEFVAL      { 60 }
            ::= { wmanIf2BsSsPkmAttributeEntry 7 }

    -- Table wmanIf2BsSsPkmAuthorizationTable
    --
    wmanIf2BsSsPkmAuthorizationTable OBJECT-TYPE
            SYNTAX      SEQUENCE OF WmanIf2BsSsPkmAuthorizationEntry
            MAX-ACCESS  not-accessible
            STATUS      current
            DESCRIPTION
                "This table contains information related to SS's
                 authorization process."
            REFERENCE
                "Table 28 and 37 in IEEE Std 802.16-2004"
            ::= { wmanIf2BsPkmV1Objects 3 }

    wmanIf2BsSsPkmAuthorizationEntry OBJECT-TYPE
            SYNTAX      WmanIf2BsSsPkmAuthorizationEntry
            MAX-ACCESS  not-accessible
            STATUS      current
            DESCRIPTION
                "Each entry contains objects that define the SS
                 authorization attributes for each SS associated with each
```

```
                BS sector. The table is indexed by ifIndex and
                wmanIf2BsSsMacAddress."
            INDEX       { ifIndex, wmanIf2BsSsPkmAuthMacAddress }
            ::= { wmanIf2BsSsPkmAuthorizationTable  1 }

    WmanIf2BsSsPkmAuthorizationEntry ::= SEQUENCE {
            wmanIf2BsSsPkmAuthMacAddress            MacAddress,
            wmanIf2BsSsPkmCaCertificate             OCTET STRING,
            wmanIf2BsSsPkmSsCertificate             OCTET STRING,
            wmanIf2BsSsPkmSaId                      INTEGER,
            wmanIf2BsSsPkmAuthKeySequenceNumber     Integer32,
            wmanIf2BsSsPkmAuthKeyLifetime           Integer32,
            wmanIf2BsSsPkmAuthRejectError           WmanIf2PkmErrorCode,
            wmanIf2BsSsPkmAuthInvalidError          WmanIf2PkmErrorCode,
            wmanIf2BsSsPkmLastAkExpireTime          DateAndTime,
            wmanIf2BsSsPkmLatestAkExpireTime        DateAndTime,
            wmanIf2BsSsPkmCertificateStatus         WmanIf2CertificateStat,
            wmanIf2BsSsPkmAuthReset                 INTEGER}

    wmanIf2BsSsPkmAuthMacAddress OBJECT-TYPE
            SYNTAX      MacAddress
            MAX-ACCESS  not-accessible
            STATUS      current
            DESCRIPTION
                "The value of this object is the physical address of the SS
                 to which the authorization association applies."
            ::= { wmanIf2BsSsPkmAuthorizationEntry 1 }

    wmanIf2BsSsPkmCaCertificate OBJECT-TYPE
            SYNTAX      OCTET STRING (SIZE(0..65535))
            MAX-ACCESS  read-only
            STATUS      current
            DESCRIPTION
                "SS sends the CA-Certificate in the Auth Info message. It
                 contains an X.509 CA certificate for the manufacturer of
                 the SS. The SS's X.509 user certificate shall have been
                 issued by the CA identified by the X.509 CA certificate."
            REFERENCE
                "Table 37 in IEEE Std 802.16-2004"
            ::= { wmanIf2BsSsPkmAuthorizationEntry 2 }

    wmanIf2BsSsPkmSsCertificate OBJECT-TYPE
            SYNTAX      OCTET STRING (SIZE(0..65535))
            MAX-ACCESS  read-only
            STATUS      current
            DESCRIPTION
                "SS sends the SS-Certificate in the Auth Request message.
                 It contains an X.509 SS certificate issued by the SS's
                 manufacturer. The SS's X.509 certificate is a public-key
                 certificate which binds the SS's identifying information
                 to its RSA public key in a verifiable manner. The X.509
                 certificate is digitally signed by the SS's manufacturer,
                 and that signature can be verified by a BS that knows
                 the manufacturer's public key. The manufacturer's public
                 key is placed in an X.509 certification authority (CA)
                 certificate, which in turn is signed by a higher level CA."
            REFERENCE
                "Table 28 in IEEE Std 802.16-2004"
            ::= { wmanIf2BsSsPkmAuthorizationEntry 3 }

    wmanIf2BsSsPkmSaId OBJECT-TYPE
            SYNTAX      INTEGER (0..65535)
            MAX-ACCESS  read-only
            STATUS      current
```

```
            DESCRIPTION
                "SS's primary SAID equal to the Basic CID."
            REFERENCE
                 "Subclause 6.3.2.3.9.2 in IEEE Std 802.16-2004"
            ::= { wmanIf2BsSsPkmAuthorizationEntry 4 }

    wmanIf2BsSsPkmAuthKeySequenceNumber OBJECT-TYPE
            SYNTAX      Integer32 (0 .. 15)
            MAX-ACCESS  read-only
            STATUS      current
            DESCRIPTION
                "This object provides the most recent authorization key
                 sequence number in the Auth Reply message for an SS."
            REFERENCE
                 "Table 29 in IEEE Std 802.16-2004"
            ::= { wmanIf2BsSsPkmAuthorizationEntry 5 }

    wmanIf2BsSsPkmAuthKeyLifetime OBJECT-TYPE
            SYNTAX      Integer32 (86400..6048000)
            UNITS       "seconds"
            MAX-ACCESS  read-only
            STATUS      current
            DESCRIPTION
                "This object defines the lifetime of an authorization
                 key (AK) the BS assigns to a SS."
            REFERENCE
                 "Table 343 in IEEE Std 802.16-2004"
            ::= { wmanIf2BsSsPkmAuthorizationEntry 6 }

    wmanIf2BsSsPkmAuthRejectError OBJECT-TYPE
            SYNTAX      WmanIf2PkmErrorCode
            MAX-ACCESS  read-only
            STATUS      current
            DESCRIPTION
                "The Error Code in most recent Authorization Reject message
                 transmitted to the SS.

                 The valid codes are:
                   0 - no failure
                   1 - unauthorized SS
                   2 - unauthorized SAID
                   6..11 - permanent authorization failure"
            REFERENCE
                 "Table 371, Subclause 11.9.10, in IEEE Std 802.16-2004"
            ::= { wmanIf2BsSsPkmAuthorizationEntry 7 }

    wmanIf2BsSsPkmAuthInvalidError OBJECT-TYPE
            SYNTAX      WmanIf2PkmErrorCode
            MAX-ACCESS  read-only
            STATUS      current
            DESCRIPTION
                "The Error Code in most recent Authorization Invalid message
                 transmitted to the SS.

                 The valid codes are:
                   0 - no failure
                   1 - unauthorized SS
                   3 - unsolicited
                   4 - invalid key sequence
                   5 - key request authentication failure"

            REFERENCE
                 "Table 371, Subclause 11.9.10, in IEEE Std 802.16-2004"
            ::= { wmanIf2BsSsPkmAuthorizationEntry 8 }
```

```
wmanIf2BsSsPkmLastAkExpireTime OBJECT-TYPE
        SYNTAX      DateAndTime
        MAX-ACCESS  read-only
        STATUS      current
        DESCRIPTION
            "This object is the time when the last AK expires.
             wmanIf2BsSsPkmLastAkExpireTime = Time(last AK[Auth Reply])
                                              + AK lifetime
             If this FSM has only one authorization key, then
             wmanIf2BsSsPkmLastAkExpireTime = the activation of FSM."
        ::= { wmanIf2BsSsPkmAuthorizationEntry 9 }

wmanIf2BsSsPkmLatestAkExpireTime OBJECT-TYPE
        SYNTAX      DateAndTime
        MAX-ACCESS  read-only
        STATUS      current
        DESCRIPTION
            "This object is the time when the latest AK expires."
        ::= { wmanIf2BsSsPkmAuthorizationEntry 10 }

wmanIf2BsSsPkmCertificateStatus OBJECT-TYPE
        SYNTAX      WmanIf2CertificateStat
        MAX-ACCESS  read-only
        STATUS      current
        DESCRIPTION
            "Indicate the reason why a SS's certificate is deemed valid
             or invalid."
        ::= { wmanIf2BsSsPkmAuthorizationEntry 11 }

wmanIf2BsSsPkmAuthReset OBJECT-TYPE
        SYNTAX      INTEGER {noResetRequested(1),
                             invalidateAuth(2),
                             sendAuthInvalid(3),
                             invalidateTeks(4)}
        MAX-ACCESS  read-write
        STATUS      current
        DESCRIPTION
            "Setting this object to:
               1 - no reset
               2 - causes the BS to invalidate the current SS
                   authorization key(s), but not to transmit an
                   Authorization Invalid message nor to invalidate
                   unicast TEKs.
               3 - causes the BS to invalidate the current SS
                   authorization key(s), and to transmit an
                   Authorization Invalid message to the SS, but not
                   to invalidate unicast TEKs.
               4 - causes the BS to invalidate the current SS
                   authorization key(s), to transmit an Authorization
                   Invalid message to the SS, and to invalidate all
                   unicast TEKs associated with this SS authorization.
             Reading this object returns the most-recently-set value
             of this object, or returns noResetRequested(1) if the
             object has not been set since the last BS reboot."
        ::= { wmanIf2BsSsPkmAuthorizationEntry 12 }

---- Table wmanIf2BsPkmSecurityCapabilityTable
--
wmanIf2BsPkmSecurityCapabilityTable OBJECT-TYPE
        SYNTAX      SEQUENCE OF WmanIf2BsPkmSecurityCapabilityEntry
        MAX-ACCESS  not-accessible
        STATUS      current
        DESCRIPTION
```

```
            "This table contains the the list of the cryptographic
             suite(s) an SS supports."
        REFERENCE
            "Subclause 11.9.13 in IEEE Std 802.16-2004"
        ::= { wmanIf2BsPkmV1Objects 4 }

wmanIf2BsPkmSecurityCapabilityEntry OBJECT-TYPE
        SYNTAX      WmanIf2BsPkmSecurityCapabilityEntry
        MAX-ACCESS  not-accessible
        STATUS      current
        DESCRIPTION
            "This table is triple indexed by ifIndex and
             wmanIf2BsSsSecurityCapIndex."
        INDEX       { ifIndex,
                      wmanIf2BsPkmSecurityCapIndex }
        ::= { wmanIf2BsPkmSecurityCapabilityTable  1 }

WmanIf2BsPkmSecurityCapabilityEntry ::= SEQUENCE {
        wmanIf2BsPkmSecurityCapIndex            INTEGER,
        wmanIf2BsPkmScDataEncryptAlgorithm      WmanIf2DataEncryptAlgId,
        wmanIf2BsPkmScDataAuthentAlgorithm      WmanIf2DataAuthAlgId,
        wmanIf2BsPkmScEncryptAlgorithm          WmanIf2TekEncryptAlgId}

wmanIf2BsPkmSecurityCapIndex OBJECT-TYPE
        SYNTAX      INTEGER (1 .. 65535)
        MAX-ACCESS  not-accessible
        STATUS      current
        DESCRIPTION
            "The index value which uniquely identifies an entry
             in the wmanIf2BsPkmSecurityCapabilityTable"
        ::= { wmanIf2BsPkmSecurityCapabilityEntry 1 }

wmanIf2BsPkmScDataEncryptAlgorithm OBJECT-TYPE
        SYNTAX      WmanIf2DataEncryptAlgId
        MAX-ACCESS  read-only
        STATUS      current
        DESCRIPTION
            "The value of this object is the data encryption algorithm
             being utilized."
        REFERENCE
             "Table 375, IEEE Std 802.16-2004"
        ::= { wmanIf2BsPkmSecurityCapabilityEntry 2 }

wmanIf2BsPkmScDataAuthentAlgorithm OBJECT-TYPE
        SYNTAX      WmanIf2DataAuthAlgId
        MAX-ACCESS  read-only
        STATUS      current
        DESCRIPTION
            "The value of this object is the data authentication
             algorithm being utilized."
        REFERENCE
             "Table 376, IEEE Std 802.16-2004"
        ::= { wmanIf2BsPkmSecurityCapabilityEntry 3 }

wmanIf2BsPkmScEncryptAlgorithm OBJECT-TYPE
        SYNTAX      WmanIf2TekEncryptAlgId
        MAX-ACCESS  read-only
        STATUS      current
        DESCRIPTION
            "The value of this object is the TEK key encryption
             algorithm being utilized."
        REFERENCE
             "Table 377, IEEE Std 802.16-2004"
        ::= { wmanIf2BsPkmSecurityCapabilityEntry 4 }
```

```
1
2   -- Table wmanIf2BsSsPkmSecurityCapabilityTable
3   --
4   wmanIf2BsSsPkmSecurityCapabilityTable OBJECT-TYPE
5           SYNTAX      SEQUENCE OF WmanIf2BsSsPkmSecurityCapabilityEntry
6           MAX-ACCESS  not-accessible
7           STATUS      current
8           DESCRIPTION
9               "This table contains the SS's Security Capabilities that are
10               conveyed by the Auth Request message. It contains the list
11               of the cryptographic suite(s) an SS supports."
12          REFERENCE
13              "Subclause 11.9.13 in IEEE Std 802.16-2004"
14          ::= { wmanIf2BsPkmV1Objects 5 }
15
16  wmanIf2BsSsPkmSecurityCapabilityEntry OBJECT-TYPE
17          SYNTAX      WmanIf2BsSsPkmSecurityCapabilityEntry
18          MAX-ACCESS  not-accessible
19          STATUS      current
20          DESCRIPTION
21              "This table is triple indexed by ifIndex,
22               wmanIf2BsSsSecurityCapIndex and wmanIf2BsSsMacAddress."
23          INDEX       { ifIndex,
24                        wmanIf2BsSsMacAddress,
25                        wmanIf2BsSsPkmSecurityCapIndex }
26          ::= { wmanIf2BsSsPkmSecurityCapabilityTable  1 }
27
28  WmanIf2BsSsPkmSecurityCapabilityEntry ::= SEQUENCE {
29          wmanIf2BsSsPkmSecurityCapIndex          INTEGER,
30          wmanIf2BsSsPkmScDataEncryptAlgorithm    WmanIf2DataEncryptAlgId,
31          wmanIf2BsSsPkmScDataAuthentAlgorithm    WmanIf2DataAuthAlgId,
32          wmanIf2BsSsPkmScEncryptAlgorithm        WmanIf2TekEncryptAlgId}
33
34  wmanIf2BsSsPkmSecurityCapIndex OBJECT-TYPE
35          SYNTAX      INTEGER (1 .. 65535)
36          MAX-ACCESS  not-accessible
37          STATUS      current
38          DESCRIPTION
39              "The index value which uniquely identifies an entry
40               in the wmanIf2BsSsPkmSecurityCapabilityTable"
41          ::= { wmanIf2BsSsPkmSecurityCapabilityEntry 1 }
42
43  wmanIf2BsSsPkmScDataEncryptAlgorithm OBJECT-TYPE
44          SYNTAX      WmanIf2DataEncryptAlgId
45          MAX-ACCESS  read-only
46          STATUS      current
47          DESCRIPTION
48              "The value of this object is the data encryption algorithm
49               being utilized."
50          REFERENCE
51               "Table 375, IEEE Std 802.16-2004"
52          ::= { wmanIf2BsSsPkmSecurityCapabilityEntry 2 }
53
54  wmanIf2BsSsPkmScDataAuthentAlgorithm OBJECT-TYPE
55          SYNTAX      WmanIf2DataAuthAlgId
56          MAX-ACCESS  read-only
57          STATUS      current
58          DESCRIPTION
59              "The value of this object is the data authentication
60               algorithm being utilized."
61          REFERENCE
62               "Table 376, IEEE Std 802.16-2004"
63          ::= { wmanIf2BsSsPkmSecurityCapabilityEntry 3 }
64
```

```
wmanIf2BsSsPkmScEncryptAlgorithm OBJECT-TYPE
        SYNTAX      WmanIf2TekEncryptAlgId
        MAX-ACCESS  read-only
        STATUS      current
        DESCRIPTION
            "The value of this object is the TEK key encryption
             algorithm being utilized."
        REFERENCE
             "Table 377, IEEE Std 802.16-2004"
        ::= { wmanIf2BsSsPkmSecurityCapabilityEntry 4 }

-- Table wmanIf2BsSsPkmTekTable
--
wmanIf2BsSsPkmTekTable OBJECT-TYPE
        SYNTAX      SEQUENCE OF WmanIf2BsSsPkmTekEntry
        MAX-ACCESS  not-accessible
        STATUS      current
        DESCRIPTION
            "This table contains the TEK attributes that are associated
             with each SAID."
        ::= { wmanIf2BsPkmV1Objects 6 }

wmanIf2BsSsPkmTekEntry OBJECT-TYPE
        SYNTAX      WmanIf2BsSsPkmTekEntry
        MAX-ACCESS  not-accessible
        STATUS      current
        DESCRIPTION
            "This table is triple indexed by ifIndex,
             wmanIf2BsSsMacAddress, and wmanIf2BsSsPkmSaidIndex."
        INDEX       { ifIndex,
                      wmanIf2BsSsMacAddress,
                      wmanIf2BsSsPkmSaidIndex }
        ::= { wmanIf2BsSsPkmTekTable  1 }

WmanIf2BsSsPkmTekEntry ::= SEQUENCE {
        wmanIf2BsSsPkmSaidIndex                 INTEGER,
        wmanIf2BsSsPkmSaType                    WmanIf2SaType,
        wmanIf2BsSsPkmTekDataEncryptAlgorithm   WmanIf2DataEncryptAlgId,
        wmanIf2BsSsPkmTekDataAuthentAlgorithm   WmanIf2DataAuthAlgId,
        wmanIf2BsSsPkmTekEncryptAlgorithm       WmanIf2TekEncryptAlgId,
        wmanIf2BsSsPkmOlderTekSequenceNumber    Integer32,
        wmanIf2BsSsPkmOlderTekLifetime          Integer32,
        wmanIf2BsSsPkmNewerTekSequenceNumber    Integer32,
        wmanIf2BsSsPkmNewerTekLifetime          Integer32,
        wmanIf2BsSsPkmKeyRejectError            WmanIf2PkmErrorCode,
        wmanIf2BsSsPkmTekInvalidError           WmanIf2PkmErrorCode,
        wmanIf2BsSsPkmLastTekExpireTime         DateAndTime,
        wmanIf2BsSsPkmLatestTekExpireTime       DateAndTime,
        wmanIf2BsSsPkmTekReset                  TruthValue}

wmanIf2BsSsPkmSaidIndex OBJECT-TYPE
        SYNTAX      INTEGER (0 .. 65535)
        MAX-ACCESS  not-accessible
        STATUS      current
        DESCRIPTION
            "SAID index to the wmanIf2BsSsPkmTekTable."
        ::= { wmanIf2BsSsPkmTekEntry 1 }

wmanIf2BsSsPkmSaType OBJECT-TYPE
        SYNTAX      WmanIf2SaType
        MAX-ACCESS  read-only
        STATUS      current
        DESCRIPTION
            "SA Type attribute that is included in the Auth Reply
```

```
                message."
            ::= { wmanIf2BsSsPkmTekEntry 2 }

    wmanIf2BsSsPkmTekDataEncryptAlgorithm OBJECT-TYPE
            SYNTAX      WmanIf2DataEncryptAlgId
            MAX-ACCESS  read-only
            STATUS      current
            DESCRIPTION
                "The data encryption algorithm attribute that is included
                 in the Auth Reply message."
            REFERENCE
                 "Table 375, IEEE Std 802.16-2004"
            ::= { wmanIf2BsSsPkmTekEntry 3 }

    wmanIf2BsSsPkmTekDataAuthentAlgorithm OBJECT-TYPE
            SYNTAX      WmanIf2DataAuthAlgId
            MAX-ACCESS  read-only
            STATUS      current
            DESCRIPTION
                "The data authentication algorithm attribute that is
                 included in the Auth Reply message."
            REFERENCE
                 "Table 376, IEEE Std 802.16-2004"
            ::= { wmanIf2BsSsPkmTekEntry 4 }

    wmanIf2BsSsPkmTekEncryptAlgorithm OBJECT-TYPE
            SYNTAX      WmanIf2TekEncryptAlgId
            MAX-ACCESS  read-only
            STATUS      current
            DESCRIPTION
                "The TEK key encryption algorithm attribute that is
                 included in the Auth Reply message."
            REFERENCE
                 "Table 377, IEEE Std 802.16-2004"
            ::= { wmanIf2BsSsPkmTekEntry 5 }

    wmanIf2BsSsPkmOlderTekSequenceNumber OBJECT-TYPE
            SYNTAX      Integer32 (0 .. 3)
            MAX-ACCESS  read-only
            STATUS      current
            DESCRIPTION
                "At all times the BS maintains two sets of active
                 generations of keying material per SAID. One set
                 corresponds to the 'older' generation of keying material,
                 the second set corresponds to the 'newer' generation of
                 keying material. The newer generation has a key sequence
                 number one greater than (modulo 4) that of the older
                 generation. This object provides the older TEK sequence
                 number in the Key Reply message for an SS."
            REFERENCE
                 "Subclause 11.9.8 in IEEE Std 802.16-2004"
            ::= { wmanIf2BsSsPkmTekEntry 6 }

    wmanIf2BsSsPkmOlderTekLifetime OBJECT-TYPE
            SYNTAX      Integer32 (1800 .. 604800)
            UNITS       "seconds"
            MAX-ACCESS  read-only
            STATUS      current
            DESCRIPTION
                "This object provides the older TEK Remaining Lifetime."
            REFERENCE
                 "Subclause 11.9.8 in IEEE Std 802.16-2004"
            ::= { wmanIf2BsSsPkmTekEntry 7 }
```

```
wmanIf2BsSsPkmNewerTekSequenceNumber OBJECT-TYPE
        SYNTAX      Integer32 (0 .. 3)
        MAX-ACCESS  read-only
        STATUS      current
        DESCRIPTION
            "This object provides the newer TEK sequence
             number in the Key Reply message for an SS."
        REFERENCE
             "Subclause 11.9.8 in IEEE Std 802.16-2004"
        ::= { wmanIf2BsSsPkmTekEntry 8 }

wmanIf2BsSsPkmNewerTekLifetime OBJECT-TYPE
        SYNTAX      Integer32 (1800 .. 604800)
        UNITS       "seconds"
        MAX-ACCESS  read-only
        STATUS      current
        DESCRIPTION
            "This object provides the newer TEK Remaining Lifetime."
        REFERENCE
             "Subclause 11.9.8 in IEEE Std 802.16-2004"
        ::= { wmanIf2BsSsPkmTekEntry 9 }

wmanIf2BsSsPkmKeyRejectError OBJECT-TYPE
        SYNTAX      WmanIf2PkmErrorCode
        MAX-ACCESS  read-only
        STATUS      current
        DESCRIPTION
            "The Error Code in the most recent Key Reject message sent
             in response to a Key Request for this SAID.

             The valid error codes are:
               0 - no failure
               2 - unauthorized SAID"
        REFERENCE
             "IEEE Std 802.16-2004; Table 371"
        ::= { wmanIf2BsSsPkmTekEntry 10 }

wmanIf2BsSsPkmTekInvalidError OBJECT-TYPE
        SYNTAX      WmanIf2PkmErrorCode
        MAX-ACCESS  read-only
        STATUS      current
        DESCRIPTION
            "The Error Code in the most recent TEK Invalid message sent
             in association with this SAID.

             The valid error codes are:
               0 - no failure
               4 - invalid key sequence"
        REFERENCE
             "IEEE Std 802.16-2004; Table 371"
        ::= { wmanIf2BsSsPkmTekEntry 11 }

wmanIf2BsSsPkmLastTekExpireTime OBJECT-TYPE
        SYNTAX      DateAndTime
        MAX-ACCESS  read-only
        STATUS      current
        DESCRIPTION
            "This object is the time when the last TEK expires.
             wmanIf2BsSsPkmLastTekExpireTime = Time(last TEK[Key Reply])
                                               + TEK lifetime
             If this FSM has only one authorization key, then
             wmanIf2BsSsPkmLastTekExpireTime = the activation of FSM."
        ::= { wmanIf2BsSsPkmTekEntry 12 }
```

```
wmanIf2BsSsPkmLatestTekExpireTime OBJECT-TYPE
        SYNTAX      DateAndTime
        MAX-ACCESS  read-only
        STATUS      current
        DESCRIPTION
            "This object is the time when the latest TEK expires."
        ::= { wmanIf2BsSsPkmTekEntry 13 }

wmanIf2BsSsPkmTekReset OBJECT-TYPE
        SYNTAX      TruthValue
        MAX-ACCESS  read-write
        STATUS      current
        DESCRIPTION
            "Setting this object to TRUE causes the BS to invalidate
             the current active TEK(s) (plural due to key transition
             periods), and to generate a new TEK for the associated
             SAID; the BS MAY also generate an unsolicited TEK Invalid
             message, to optimize the TEK synchronization between the BS
             and the SS. Reading this object always returns FALSE."
        ::= { wmanIf2BsSsPkmTekEntry 14 }
```

2.4 wmanIf2BsPkmV2Objects ASN.1 Code Change

13.2 ASN.1 Definitions of MIB Modules

13.2.3 wmanIf2Mib

[Add wmanIf2BsPkmV2Objects as the following in WMAN-IF2-MIB:]

```
wmanIf2BsPkmV2Objects OBJECT IDENTIFIER ::= { wmanIf2BsPkmObjects 2 }

--
-- Table wmanIf2BsPkmV2ConfigTable
--
wmanIf2BsPkmV2ConfigTable OBJECT-TYPE
        SYNTAX      SEQUENCE OF WmanIf2BsPkmV2ConfigEntry
        MAX-ACCESS  not-accessible
        STATUS      current
        DESCRIPTION
            "This table contains the configuration of the PKM
             attributes that are needed to PKM operation."
        REFERENCE
            "Table 343 in IEEE Std 802.16-2004 and 802.16e-2005"
        ::= { wmanIf2BsPkmV2Objects  1 }

wmanIf2BsPkmV2ConfigEntry OBJECT-TYPE
        SYNTAX      WmanIf2BsPkmV2ConfigEntry
        MAX-ACCESS  not-accessible
        STATUS      current
        DESCRIPTION
            "Each entry contains objects that define the PKM attributes
             of each BS. The table is indexed by ifIndex that is
             associated with the BS sector."
        INDEX       { ifIndex }
        ::= { wmanIf2BsPkmV2ConfigTable  1 }

WmanIf2BsPkmV2ConfigEntry ::= SEQUENCE {
        wmanIf2BsPkmPmkPrehandshakeLifetime     Integer32,
        wmanIf2BsPkmPmkLifetime                 Integer32,
        wmanIf2BsSaChallengeTimeout             Integer32,
        wmanIf2BsMaxSaTekChallenge              Integer32,
        wmanIf2BsSaTekTimeout                   Integer32,
        wmanIf2BsMaxSaTekRequest                Integer32}

wmanIf2BsPkmPmkPrehandshakeLifetime OBJECT-TYPE
        SYNTAX      Integer32 (5 .. 900)
        UNITS       "seconds"
        MAX-ACCESS  read-write
        STATUS      current
        DESCRIPTION
            "This object defines the PMK or PAK prehandshake lifetime."
        REFERENCE
             "Table 343 in IEEE Std 802.16e-2005"
        DEFVAL          { 10 }
        ::= { wmanIf2BsPkmV2ConfigEntry 1 }

wmanIf2BsPkmPmkLifetime OBJECT-TYPE
        SYNTAX      Integer32 (60 .. 86400)
        UNITS       "seconds"
        MAX-ACCESS  read-write
        STATUS      current
        DESCRIPTION
```

```
                "This object defines PMK lifetime, if MSK lifetime is
                 unspecified (i.e., by AAA server)."
            REFERENCE
                 "Table 343 in IEEE Std 802.16e-2005"
            DEFVAL          { 3600 }
            ::= { wmanIf2BsPkmV2ConfigEntry 2 }

    wmanIf2BsSaChallengeTimeout OBJECT-TYPE
            SYNTAX      Integer32 (500 .. 2000)
            UNITS       "milliseconds"
            MAX-ACCESS  read-write
            STATUS      current
            DESCRIPTION
                "This object defines the timeout value for SA-TEKChallenge
                 retransmission."
            REFERENCE
                 "Table 343 in IEEE Std 802.16e-2005"
            DEFVAL          { 1000 }
            ::= { wmanIf2BsPkmV2ConfigEntry 3 }

    wmanIf2BsMaxSaTekChallenge OBJECT-TYPE
            SYNTAX      Integer32 (1 .. 3)
            MAX-ACCESS  read-write
            STATUS      current
            DESCRIPTION
                "This object defines the maximum number of SA-TEK-Challenge
                 transmissions."
            REFERENCE
                 "Table 343 in IEEE Std 802.16e-2005"
            DEFVAL          { 3 }
            ::= { wmanIf2BsPkmV2ConfigEntry 4 }

    wmanIf2BsSaTekTimeout OBJECT-TYPE
            SYNTAX      Integer32 (100 .. 1000)
            UNITS       "milliseconds"
            MAX-ACCESS  read-write
            STATUS      current
            DESCRIPTION
                "This object defines the timeout value for SA-TEKRequest
                 retransmission."
            REFERENCE
                 "Table 343 in IEEE Std 802.16e-2005"
            DEFVAL          { 300 }
            ::= { wmanIf2BsPkmV2ConfigEntry 5 }

    wmanIf2BsMaxSaTekRequest OBJECT-TYPE
            SYNTAX      Integer32 (1 .. 3)
            MAX-ACCESS  read-write
            STATUS      current
            DESCRIPTION
                "This object defines the maximum number of SA-TEK-Request
                 retransmission."
            REFERENCE
                 "Table 343 in IEEE Std 802.16e-2005"
            DEFVAL          { 3 }
            ::= { wmanIf2BsPkmV2ConfigEntry 6 }

    --
    -- Table wmanIf2BsSsPkmV2RsaAuthTable
    --
    wmanIf2BsSsPkmV2RsaAuthTable OBJECT-TYPE
            SYNTAX      SEQUENCE OF WmanIf2BsSsPkmV2RsaAuthEntry
            MAX-ACCESS  not-accessible
            STATUS      current
```

```
            DESCRIPTION
                "This table contains information related to PKMV2
                 RSA based authorization process."
            REFERENCE
                "Subclause 6.3.2.3.9.11 in IEEE Std 802.16e-2005"
            ::= { wmanIf2BsPkmV2Objects 2 }

    wmanIf2BsSsPkmV2RsaAuthEntry OBJECT-TYPE
            SYNTAX      WmanIf2BsSsPkmV2RsaAuthEntry
            MAX-ACCESS  not-accessible
            STATUS      current
            DESCRIPTION
                "Each entry contains objects that define the SS
                 authorization attributes for each SS associated with each
                 BS sector. The table is indexed by ifIndex and
                 wmanIf2BsSsMacAddress."
            INDEX       { ifIndex, wmanIf2BsSsMacAddress }
            ::= { wmanIf2BsSsPkmV2RsaAuthTable  1 }

    WmanIf2BsSsPkmV2RsaAuthEntry ::= SEQUENCE {
            wmanIf2BsSsPkmV2BsCertificate           OCTET STRING,
            wmanIf2BsSsPkmV2SsCertificate           OCTET STRING,
            wmanIf2BsSsPkmV2SaId                    INTEGER,
            wmanIf2BsSsPkmV2SsRandom                OCTET STRING,
            wmanIf2BsSsPkmV2BsRandom                OCTET STRING,
            wmanIf2BsSsPkmV2AuthKeySequenceNumber   Integer32,
            wmanIf2BsSsPkmV2AuthKeyLifetime         Integer32,
            wmanIf2BsSsPkmV2AuthResult              INTEGER,
            wmanIf2BsSsPkmV2AuthFailure             WmanIf2PkmErrorCode,
            wmanIf2BsSsPkmV2LastAkExpireTime        DateAndTime,
            wmanIf2BsSsPkmV2LatestAkExpireTime      DateAndTime,
            wmanIf2BsSsPkmV2CertificateStatus       WmanIf2CertificateStat}

    wmanIf2BsSsPkmV2BsCertificate OBJECT-TYPE
            SYNTAX      OCTET STRING (SIZE(0..65535))
            MAX-ACCESS  read-only
            STATUS      current
            DESCRIPTION
                "BS sends the BS-Certificate in the PKMV2 RSA-Reply message
                 for BS-SS mutual authentication. It is the DER-encoded
                 ASN.1 X.509 BS Certificate."
            REFERENCE
                "Subclause 11.9.24 in IEEE Std 802.16e-2005"
            ::= { wmanIf2BsSsPkmV2RsaAuthEntry 1 }

    wmanIf2BsSsPkmV2SsCertificate OBJECT-TYPE
            SYNTAX      OCTET STRING (SIZE(0..65535))
            MAX-ACCESS  read-only
            STATUS      current
            DESCRIPTION
                "SS sends the SS-Certificate in the PKMV2 RSA-Request
                 message. It contains an X.509 SS certificate issued by the
                 SS's manufacturer. The SS's X.509 certificate is a
                 public-key certificate which binds the SS's identifying
                 information to its RSA public key in a verifiable manner.
                 The X.509 certificate is digitally signed by the SS's
                 manufacturer, and that signature can be verified by a BS
                 that knows the manufacturer's public key.
                 The manufacturer's public key is placed in an X.509
                 certification authority (CA) certificate, which in turn
                 is signed by a higher level CA."
            REFERENCE
                "Subclause 11.9.12 in IEEE Std 802.16-2004"
            ::= { wmanIf2BsSsPkmV2RsaAuthEntry 2 }
```

```
wmanIf2BsSsPkmV2SaId OBJECT-TYPE
        SYNTAX      INTEGER (0..65535)
        MAX-ACCESS  read-only
        STATUS      current
        DESCRIPTION
            "SS's primary SAID equal to the Basic CID. SS sends the SAID
             in the PKMV2 RSA-Request message."
        REFERENCE
             "Subclause 6.3.2.3.9.2 in IEEE Std 802.16-2004"
        ::= { wmanIf2BsSsPkmV2RsaAuthEntry 3 }

wmanIf2BsSsPkmV2SsRandom OBJECT-TYPE
        SYNTAX      OCTET STRING (SIZE(8))
        MAX-ACCESS  read-only
        STATUS      current
        DESCRIPTION
            "This attribute contains a quantity that is pseudo random
             number generated from the MS and used as fresh number for
             mutual authorization message handshake. SS sends the SS-Random
             in the PKMV2 RSA-Request message."
        REFERENCE
            "Subclause 11.9.21 in IEEE Std 802.16e-2005"
        ::= { wmanIf2BsSsPkmV2RsaAuthEntry 4 }

wmanIf2BsSsPkmV2BsRandom OBJECT-TYPE
        SYNTAX      OCTET STRING (SIZE(8))
        MAX-ACCESS  read-only
        STATUS      current
        DESCRIPTION
            "This attribute contains a quantity that is pseudo random
             number generated from the BS and used as fresh number for
             mutual authorization message handshake.BS sends the BS-Random
             in the PKMV2 RSA-Reply message."
        REFERENCE
            "Subclause 11.9.22 in IEEE Std 802.16e-2005"
        ::= { wmanIf2BsSsPkmV2RsaAuthEntry 5 }

wmanIf2BsSsPkmV2AuthKeySequenceNumber OBJECT-TYPE
        SYNTAX      Integer32 (0 .. 15)
        MAX-ACCESS  read-only
        STATUS      current
        DESCRIPTION
            "This object provides the most recent authorization key
             sequence number in the PKMV2 RSA-Reply message for an SS."
        REFERENCE
             "Subclause 11.9.5 in IEEE Std 802.16e-2005"
        ::= { wmanIf2BsSsPkmV2RsaAuthEntry 6 }

wmanIf2BsSsPkmV2AuthKeyLifetime OBJECT-TYPE
        SYNTAX      Integer32 (86400..6048000)
        UNITS       "seconds"
        MAX-ACCESS  read-only
        STATUS      current
        DESCRIPTION
            "This object defines the lifetime of an authorization
             key (AK) the BS assigns to a SS. BS sends the key lifetime
             in the PKMV2 RSA-Reply message."
        REFERENCE
             "Subclause 11.9.4 in IEEE Std 802.16e-2005"
        ::= { wmanIf2BsSsPkmV2RsaAuthEntry 7 }

wmanIf2BsSsPkmV2AuthResult OBJECT-TYPE
        SYNTAX      INTEGER {success(0),
```

```
                                reject(1)}
        MAX-ACCESS  read-only
        STATUS      current
        DESCRIPTION
            "This attribute contains the result code of the RSA-based
             authorization. SS sends the result code in PKMV2
             RSA-Acknowledgement message."
        REFERENCE
             "Subclause 11.9.4 in IEEE Std 802.16e-2005"
        ::= { wmanIf2BsSsPkmV2RsaAuthEntry 8 }

wmanIf2BsSsPkmV2AuthFailure OBJECT-TYPE
        SYNTAX      WmanIf2PkmErrorCode
        MAX-ACCESS  read-only
        STATUS      current
        DESCRIPTION
            "BS returs PKMV2 RSA-Rejects message if an authorization
             failure is detected.

             Failure type umknownManufactur(4)- ssBsIncompatibleSc(9)are
             considered permanent authorization failure, since any
             attempts of reauthorization would continue to result in
             Authorization Rejects. Details about the cause of a
             Permanent Authorization Failure may be reported to the SS
             in an optional Display-String attribute that may accompany
             the Error-Code attribute in Authorization Reject messages.

             Note that the BS may log the Display-String attribute and
             Authorization failures in wmanIfDevMib, and generate a trap
              to an SNMP manager."
        REFERENCE
             "Subclause 11.9.10 in IEEE Std 802.16-2004"
        ::= { wmanIf2BsSsPkmV2RsaAuthEntry 9 }

wmanIf2BsSsPkmV2LastAkExpireTime OBJECT-TYPE
        SYNTAX      DateAndTime
        MAX-ACCESS  read-only
        STATUS      current
        DESCRIPTION
            "This object is the time when the last AK expires.
             wmanIf2BsSsPkmV2LastAkExpireTime = Time(last AK[RSA-Reply])
                                                + AK lifetime
             If this FSM has only one authorization key, then
             wmanIf2BsSsPkmV2LastAkExpireTime = the activation of FSM."
        ::= { wmanIf2BsSsPkmV2RsaAuthEntry 10 }

wmanIf2BsSsPkmV2LatestAkExpireTime OBJECT-TYPE
        SYNTAX      DateAndTime
        MAX-ACCESS  read-only
        STATUS      current
        DESCRIPTION
            "This object is the time when the latest AK expires."
        ::= { wmanIf2BsSsPkmV2RsaAuthEntry 11 }

wmanIf2BsSsPkmV2CertificateStatus OBJECT-TYPE
        SYNTAX      WmanIf2CertificateStat
        MAX-ACCESS  read-only
        STATUS      current
        DESCRIPTION
            "Indicate the reason why a SS's certificate is deemed valid
             or invalid."
        ::= { wmanIf2BsSsPkmV2RsaAuthEntry 12 }

--
```

```
-- Table wmanIf2BsSsPkmV2TekTable
--
wmanIf2BsSsPkmV2TekTable OBJECT-TYPE
        SYNTAX      SEQUENCE OF WmanIf2BsSsPkmV2TekEntry
        MAX-ACCESS  not-accessible
        STATUS      current
        DESCRIPTION
            "This table contains the TEK attributes that are associated
             with each SAID."
        ::= { wmanIf2BsPkmV2Objects 3 }

wmanIf2BsSsPkmV2TekEntry OBJECT-TYPE
        SYNTAX      WmanIf2BsSsPkmV2TekEntry
        MAX-ACCESS  not-accessible
        STATUS      current
        DESCRIPTION
            "This table is triple indexed by ifIndex,
             wmanIf2BsSsMacAddress, and wmanIf2BsSsPkmSaidIndex."
        INDEX       { ifIndex,
                      wmanIf2BsSsMacAddress,
                      wmanIf2BsSsPkmV2SaidIndex }
        ::= { wmanIf2BsSsPkmV2TekTable  1 }

WmanIf2BsSsPkmV2TekEntry ::= SEQUENCE {
        wmanIf2BsSsPkmV2SaidIndex               INTEGER,
        wmanIf2BsSsPkmV2SaType                  WmanIf2SaType,
        wmanIf2BsSsPkmV2OlderTekSequenceNumber  Integer32,
        wmanIf2BsSsPkmV2OlderTekLifetime        Integer32,
        wmanIf2BsSsPkmV2NewerTekSequenceNumber  Integer32,
        wmanIf2BsSsPkmV2NewerTekLifetime        Integer32,
        wmanIf2BsSsPkmV2AuthInvalidError        WmanIf2PkmErrorCode,
        wmanIf2BsSsPkmV2LastTekExpireTime       DateAndTime,
        wmanIf2BsSsPkmV2LatestTekExpireTime     DateAndTime}

wmanIf2BsSsPkmV2SaidIndex OBJECT-TYPE
        SYNTAX      INTEGER (0 .. 65535)
        MAX-ACCESS  not-accessible
        STATUS      current
        DESCRIPTION
            "SAID index to the wmanIf2BsSsPkmV2TekTable."
        ::= { wmanIf2BsSsPkmV2TekEntry 1 }

wmanIf2BsSsPkmV2SaType OBJECT-TYPE
        SYNTAX      WmanIf2SaType
        MAX-ACCESS  read-only
        STATUS      current
        DESCRIPTION
            "SA Type attribute that is included in the Auth Reply
             message."
        ::= { wmanIf2BsSsPkmV2TekEntry 2 }

wmanIf2BsSsPkmV2OlderTekSequenceNumber OBJECT-TYPE
        SYNTAX      Integer32 (0 .. 3)
        MAX-ACCESS  read-only
        STATUS      current
        DESCRIPTION
            "At all times the BS maintains two sets of active
             generations of keying material per SAID. One set
             corresponds to the 'older' generation of keying material,
             the second set corresponds to the 'newer' generation of
             keying material. The newer generation has a key sequence
             number one greater than (modulo 4) that of the older
             generation. This object provides the older TEK sequence
             number in the Key Reply message for an SS."
```

```
            REFERENCE
                 "Subclause 11.9.8 in IEEE Std 802.16-2004"
            ::= { wmanIf2BsSsPkmV2TekEntry 3 }

    wmanIf2BsSsPkmV2OlderTekLifetime OBJECT-TYPE
            SYNTAX      Integer32 (1800 .. 604800)
            UNITS       "seconds"
            MAX-ACCESS  read-only
            STATUS      current
            DESCRIPTION
                "This object provides the older TEK Remaining Lifetime."
            REFERENCE
                 "Subclause 11.9.8 in IEEE Std 802.16-2004"
            ::= { wmanIf2BsSsPkmV2TekEntry 4 }

    wmanIf2BsSsPkmV2NewerTekSequenceNumber OBJECT-TYPE
            SYNTAX      Integer32 (0 .. 3)
            MAX-ACCESS  read-only
            STATUS      current
            DESCRIPTION
                "This object provides the newer TEK sequence
                 number in the Key Reply message for an SS."
            REFERENCE
                 "Subclause 11.9.8 in IEEE Std 802.16-2004"
            ::= { wmanIf2BsSsPkmV2TekEntry 5 }

    wmanIf2BsSsPkmV2NewerTekLifetime OBJECT-TYPE
            SYNTAX      Integer32 (1800 .. 604800)
            UNITS       "seconds"
            MAX-ACCESS  read-only
            STATUS      current
            DESCRIPTION
                "This object provides the newer TEK Remaining Lifetime."
            REFERENCE
                 "Subclause 11.9.8 in IEEE Std 802.16-2004"
            ::= { wmanIf2BsSsPkmV2TekEntry 6 }

    wmanIf2BsSsPkmV2AuthInvalidError OBJECT-TYPE
            SYNTAX      WmanIf2PkmErrorCode
            MAX-ACCESS  read-only
            STATUS      current
            DESCRIPTION
                "BS returs Authorization Invalid message if an authorization
                 invlaid error is detected.

                 Note that the BS may log the Display-String attribute and
                 Authorization invalid error in wmanIfDevMib."
            REFERENCE
                 "Subclause 11.9.10 in IEEE Std 802.16-2004"
            ::= { wmanIf2BsSsPkmV2TekEntry 7 }

    wmanIf2BsSsPkmV2LastTekExpireTime OBJECT-TYPE
            SYNTAX      DateAndTime
            MAX-ACCESS  read-only
            STATUS      current
            DESCRIPTION
                "This object is the time when the last TEK expires.
                 wmanIf2BsSsPkmV2LastTekExpireTime = Time(last TEK[Key Reply])
                                                     + TEK lifetime
                 If this FSM has only one authorization key, then
                 wmanIf2BsSsPkmV2LastTekExpireTime = the activation of FSM."
            ::= { wmanIf2BsSsPkmV2TekEntry 8 }

    wmanIf2BsSsPkmV2LatestTekExpireTime OBJECT-TYPE
```

```
            SYNTAX      DateAndTime
            MAX-ACCESS  read-only
            STATUS      current
            DESCRIPTION
                "This object is the time when the latest TEK expires."
            ::= { wmanIf2BsSsPkmV2TekEntry 9 }
```

2.5 wmanIf2SsPkmObjects ASN.1 Code Change

13.2 ASN.1 Definitions of MIB Modules

13.2.3 wmanIf2Mib

[Replace wmanIf2SsPkmObjects to the following in WMAN-IF2-MIB:]

```
--
-- Subscriber station PKM group
-- wmanIf2SsPkmObjects contain the Subscriber Station Privacy Sublayer
-- objects
--
wmanIf2SsPkmObjects OBJECT IDENTIFIER ::= { wmanIf2SsObjects 2 }

wmanIf2SsPkmV1Objects OBJECT IDENTIFIER ::= { wmanIf2SsPkmObjects 1 }

--
-- Table wmanIf2SsPkmAttributeTable
--
wmanIf2SsPkmAttributeTable OBJECT-TYPE
        SYNTAX      SEQUENCE OF WmanIf2SsPkmAttributeEntry
        MAX-ACCESS  not-accessible
        STATUS      current
        DESCRIPTION
            "This table provides the configuration of the PKM
             attributes that are needed to PKM operation."
        REFERENCE
            "Table 343 in IEEE Std 802.16-2004 and 802.16e-2005"
        ::= { wmanIf2SsPkmV1Objects  1 }

wmanIf2SsPkmAttributeEntry OBJECT-TYPE
        SYNTAX      WmanIf2SsPkmAttributeEntry
        MAX-ACCESS  not-accessible
        STATUS      current
        DESCRIPTION
            "The table is indexed by ifIndex."
        INDEX       { ifIndex }
        ::= { wmanIf2SsPkmAttributeTable  1 }

WmanIf2SsPkmAttributeEntry ::= SEQUENCE {
        wmanIf2SsPkmAuthWaitTimeout             Integer32,
        wmanIf2SsPkmReauthWaitTimeout           Integer32,
        wmanIf2SsPkmAuthGraceTime               Integer32,
        wmanIf2SsPkmOpWaitTimeout               Integer32,
        wmanIf2SsPkmRekeyWaitTimeout            Integer32,
        wmanIf2SsPkmTekGraceTime                Integer32,
        wmanIf2SsPkmAuthRejectWaitTimeout       Integer32}

wmanIf2SsPkmAuthWaitTimeout OBJECT-TYPE
        SYNTAX      Integer32 (2 .. 30)
        UNITS       "seconds"
        MAX-ACCESS  read-only
        STATUS      current
        DESCRIPTION
            "This object defines the Auth Req retransmission interval
             from Auth Wait state."
        REFERENCE
            "Table 343 and subclause 11.9.19 in IEEE Std 802.16-2004"
        DEFVAL      { 10 }
        ::= { wmanIf2SsPkmAttributeEntry 1 }
```

```
wmanIf2SsPkmReauthWaitTimeout OBJECT-TYPE
        SYNTAX      Integer32 (2 .. 30)
        UNITS       "seconds"
        MAX-ACCESS  read-only
        STATUS      current
        DESCRIPTION
            "This object defines the Auth Req retransmission interval
             from Reauth Wait state."
        REFERENCE
            "Table 343 and subclause 11.9.19 in IEEE Std 802.16-2004"
        DEFVAL      { 10 }
        ::= { wmanIf2SsPkmAttributeEntry 2 }

wmanIf2SsPkmAuthGraceTime OBJECT-TYPE
        SYNTAX      Integer32 (300 .. 3024000)
        UNITS       "seconds"
        MAX-ACCESS  read-only
        STATUS      current
        DESCRIPTION
            "The value of this object is the grace time for an
             authorization key. A SS is expected to start trying to get
             a new authorization key beginning AuthGraceTime seconds
             before the authorization key actually expires."
        REFERENCE
            "Table 343 and subclause 11.9.19 in IEEE Std 802.16-2004"
        DEFVAL      { 600 }
        ::= { wmanIf2SsPkmAttributeEntry 3 }

wmanIf2SsPkmOpWaitTimeout OBJECT-TYPE
        SYNTAX      Integer32 (1 .. 10)
        UNITS       "seconds"
        MAX-ACCESS  read-only
        STATUS      current
        DESCRIPTION
            "This object defines the Key Req retransmission interval
             from Op Wait state."
        REFERENCE
            "Table 343 and subclause 11.9.19 in IEEE Std 802.16-2004"
        DEFVAL      { 1 }
        ::= { wmanIf2SsPkmAttributeEntry 4 }

wmanIf2SsPkmRekeyWaitTimeout OBJECT-TYPE
        SYNTAX      Integer32 (1 .. 10)
        UNITS       "seconds"
        MAX-ACCESS  read-only
        STATUS      current
        DESCRIPTION
            "This object defines the Key Req retransmission interval
             from Rekey Wait state."
        REFERENCE
            "Table 343 and subclause 11.9.19 in IEEE Std 802.16-2004"
        DEFVAL      { 1 }
        ::= { wmanIf2SsPkmAttributeEntry 5 }

wmanIf2SsPkmTekGraceTime OBJECT-TYPE
        SYNTAX      Integer32 (300 .. 3024000)
        UNITS       "seconds"
        MAX-ACCESS  read-only
        STATUS      current
        DESCRIPTION
            "The value of this object is the grace time for the TEK in
             seconds. The SS is expected to start trying to acquire a
             new TEK beginning TEK GraceTime seconds before the
             expiration of the most recent TEK."
```

```
            REFERENCE
                "Table 343 and subclause 11.9.19 in IEEE Std 802.16-2004"
            DEFVAL      { 3600 }
            ::= { wmanIf2SsPkmAttributeEntry 6 }

    wmanIf2SsPkmAuthRejectWaitTimeout OBJECT-TYPE
            SYNTAX      Integer32 (10 .. 600)
            UNITS       "seconds"
            MAX-ACCESS  read-only
            STATUS      current
            DESCRIPTION
                "This object defines the Delay before resending Auth Request
                 after receiving Auth Reject."
            REFERENCE
                "Table 343 and subclause 11.9.19 in IEEE Std 802.16-2004"
            DEFVAL      { 60 }
            ::= { wmanIf2SsPkmAttributeEntry 7 }

    --
    -- Table wmanIf2SsPkmAuthorizationTable
    --
    wmanIf2SsPkmAuthorizationTable OBJECT-TYPE
            SYNTAX      SEQUENCE OF WmanIf2SsPkmAuthorizationEntry
            MAX-ACCESS  not-accessible
            STATUS      current
            DESCRIPTION
                "This table contains information that are related to SS's
                 authorization process."
            REFERENCE
                "Table 28 and 37 in IEEE Std 802.16-2004"
            ::= { wmanIf2SsPkmV1Objects 2 }

    wmanIf2SsPkmAuthorizationEntry OBJECT-TYPE
            SYNTAX      WmanIf2SsPkmAuthorizationEntry
            MAX-ACCESS  not-accessible
            STATUS      current
            DESCRIPTION
                "This table is indexed by ifIndex"
            INDEX       { ifIndex }
            ::= { wmanIf2SsPkmAuthorizationTable  1 }

    WmanIf2SsPkmAuthorizationEntry ::= SEQUENCE {
            wmanIf2SsPkmCaCertificate               OCTET STRING,
            wmanIf2SsPkmSsCertificate               OCTET STRING,
            wmanIf2SsPkmSaId                        INTEGER,
            wmanIf2SsPkmAuthKeySequenceNumber       Integer32,
            wmanIf2SsPkmAuthKeyLifetime             Integer32,
            wmanIf2SsPkmAuthRejectError             WmanIf2PkmErrorCode,
            wmanIf2SsPkmAuthInvalidError            WmanIf2PkmErrorCode,
            wmanIf2SsPkmLastAkExpireTime            DateAndTime,
            wmanIf2SsPkmLatestAkExpireTime          DateAndTime,
            wmanIf2SsPkmAuthReset                   TruthValue}

    wmanIf2SsPkmCaCertificate OBJECT-TYPE
            SYNTAX      OCTET STRING (SIZE(0..65535))
            MAX-ACCESS  read-only
            STATUS      current
            DESCRIPTION
                "SS sends the CA-Certificate in the Auth Info message. It
                 contains an X.509 CA certificate for the manufacturer of
                 the SS. The SS's X.509 user certificate shall have been
                 issued by the CA identified by the X.509 CA certificate."
            REFERENCE
                "Table 37 in IEEE Std 802.16-2004"
```

```
        ::= { wmanIf2SsPkmAuthorizationEntry 1 }

wmanIf2SsPkmSsCertificate OBJECT-TYPE
        SYNTAX      OCTET STRING (SIZE(0..65535))
        MAX-ACCESS  read-only
        STATUS      current
        DESCRIPTION
            "SS sends the SS-Certificate in the Auth Request message.
             It contains an X.509 SS certificate issued by the SS's
             manufacturer. The SS's X.509 certificate is a public-key
             certificate which binds the SS's identifying information
             to its RSA public key in a verifiable manner. The X.509
             certificate is digitally signed by the SS's manufacturer,
             and that signature can be verified by a BS that knows
             the manufacturer's public key. The manufacturer's public
             key is placed in an X.509 certification authority (CA)
             certificate, which in turn is signed by a higher level CA."
        REFERENCE
            "Table 28 in IEEE Std 802.16-2004"
        ::= { wmanIf2SsPkmAuthorizationEntry 2 }

wmanIf2SsPkmSaId OBJECT-TYPE
        SYNTAX      INTEGER (0..65535)
        MAX-ACCESS  read-only
        STATUS      current
        DESCRIPTION
            "SS's primary SAID equal to the Basic CID."
        REFERENCE
             "Subclause 6.3.2.3.9.2 in IEEE Std 802.16-2004"
        ::= { wmanIf2SsPkmAuthorizationEntry 3 }

wmanIf2SsPkmAuthKeySequenceNumber OBJECT-TYPE
        SYNTAX      Integer32 (0 .. 15)
        MAX-ACCESS  read-only
        STATUS      current
        DESCRIPTION
            "This object provides the most recent authorization key
             sequence number in the Auth Reply message for an SS."
        REFERENCE
             "Table 29 in IEEE Std 802.16-2004"
        ::= { wmanIf2SsPkmAuthorizationEntry 4 }

wmanIf2SsPkmAuthKeyLifetime OBJECT-TYPE
        SYNTAX      Integer32 (86400..6048000)
        UNITS       "seconds"
        MAX-ACCESS  read-only
        STATUS      current
        DESCRIPTION
            "This object defines the lifetime of an authorization
             key (AK) the BS assigns to a SS."
        REFERENCE
             "Table 343 in IEEE Std 802.16-2004"
        ::= { wmanIf2SsPkmAuthorizationEntry 5 }

wmanIf2SsPkmAuthRejectError OBJECT-TYPE
        SYNTAX      WmanIf2PkmErrorCode
        MAX-ACCESS  read-only
        STATUS      current
        DESCRIPTION
            "The Error Code in most recent Authorization Reject message
             received from the BS.

             The valid codes are:
               0 - no failure
```

```
                1 - unauthorized SS
                2 - unauthorized SAID
                6..11 - permanent authorization failure"
        REFERENCE
             "Table 371, Subclause 11.9.10, in IEEE Std 802.16-2004"
        ::= { wmanIf2SsPkmAuthorizationEntry 6 }

wmanIf2SsPkmAuthInvalidError OBJECT-TYPE
        SYNTAX      WmanIf2PkmErrorCode
        MAX-ACCESS  read-only
        STATUS      current
        DESCRIPTION
            "The Error Code in most recent Authorization Invalid message
             received from the BS.

             The valid codes are:
               0 - no failure
               1 - unauthorized SS
               3 - unsolicited
               4 - invalid key sequence
               5 - key request authentication failure"

        REFERENCE
             "Table 371, Subclause 11.9.10, in IEEE Std 802.16-2004"
        ::= { wmanIf2SsPkmAuthorizationEntry 7 }

wmanIf2SsPkmLastAkExpireTime OBJECT-TYPE
        SYNTAX      DateAndTime
        MAX-ACCESS  read-only
        STATUS      current
        DESCRIPTION
            "This object is the time when the last AK expires.
             wmanIf2SsPkmLastAkExpireTime = Time(last AK[Auth Reply])
                                            + AK lifetime
             If this FSM has only one authorization key, then
             wmanIf2SsPkmLastAkExpireTime = the activation of FSM."
        ::= { wmanIf2SsPkmAuthorizationEntry 8 }

wmanIf2SsPkmLatestAkExpireTime OBJECT-TYPE
        SYNTAX      DateAndTime
        MAX-ACCESS  read-only
        STATUS      current
        DESCRIPTION
            "This object is the time when the latest AK expires."
        ::= { wmanIf2SsPkmAuthorizationEntry 9 }

wmanIf2SsPkmAuthReset OBJECT-TYPE
        SYNTAX      TruthValue
        MAX-ACCESS  read-write
        STATUS      current
        DESCRIPTION
            "Setting this object to TRUE generates a Reauthorize event
             in the authorization FSM. Reading this object always
             returns FALSE."
        ::= { wmanIf2SsPkmAuthorizationEntry 10 }

--
-- Table wmanIf2SsPkmSecurityCapabilityTable
--
wmanIf2SsPkmSecurityCapabilityTable OBJECT-TYPE
        SYNTAX      SEQUENCE OF WmanIf2SsPkmSecurityCapabilityEntry
        MAX-ACCESS  not-accessible
        STATUS      current
        DESCRIPTION
```

```
            "This table contains the SS's Security Capabilities that are
             conveyed by the Auth Request message. It contains the list
             of the cryptographic suite(s) an SS supports."
        REFERENCE
            "Subclause 11.9.13 in IEEE Std 802.16-2004"
        ::= { wmanIf2SsPkmV1Objects 3 }

wmanIf2SsPkmSecurityCapabilityEntry OBJECT-TYPE
        SYNTAX      WmanIf2SsPkmSecurityCapabilityEntry
        MAX-ACCESS  not-accessible
        STATUS      current
        DESCRIPTION
            "This table is indexed by wmanIf2SsSecurityCapIndex."
        INDEX       { wmanIf2SsPkmSecurityCapIndex }
        ::= { wmanIf2SsPkmSecurityCapabilityTable  1 }

WmanIf2SsPkmSecurityCapabilityEntry ::= SEQUENCE {
        wmanIf2SsPkmSecurityCapIndex            INTEGER,
        wmanIf2SsPkmScDataEncryptAlgorithm      WmanIf2DataEncryptAlgId,
        wmanIf2SsPkmScDataAuthentAlgorithm      WmanIf2DataAuthAlgId,
        wmanIf2SsPkmScEncryptAlgorithm          WmanIf2TekEncryptAlgId}

wmanIf2SsPkmSecurityCapIndex OBJECT-TYPE
        SYNTAX      INTEGER (1 .. 65535)
        MAX-ACCESS  not-accessible
        STATUS      current
        DESCRIPTION
            "The index value which uniquely identifies an entry
             in the wmanIf2SsPkmSecurityCapabilityTable"
        ::= { wmanIf2SsPkmSecurityCapabilityEntry 1 }

wmanIf2SsPkmScDataEncryptAlgorithm OBJECT-TYPE
        SYNTAX      WmanIf2DataEncryptAlgId
        MAX-ACCESS  read-only
        STATUS      current
        DESCRIPTION
            "The value of this object is the data encryption algorithm
             being utilized."
        REFERENCE
             "Table 375, IEEE Std 802.16-2004"
        ::= { wmanIf2SsPkmSecurityCapabilityEntry 2 }

wmanIf2SsPkmScDataAuthentAlgorithm OBJECT-TYPE
        SYNTAX      WmanIf2DataAuthAlgId
        MAX-ACCESS  read-only
        STATUS      current
        DESCRIPTION
            "The value of this object is the data authentication
             algorithm being utilized."
        REFERENCE
             "Table 376, IEEE Std 802.16-2004"
        ::= { wmanIf2SsPkmSecurityCapabilityEntry 3 }

wmanIf2SsPkmScEncryptAlgorithm OBJECT-TYPE
        SYNTAX      WmanIf2TekEncryptAlgId
        MAX-ACCESS  read-only
        STATUS      current
        DESCRIPTION
            "The value of this object is the TEK key encryption
             algorithm being utilized."
        REFERENCE
             "Table 377, IEEE Std 802.16-2004"
        ::= { wmanIf2SsPkmSecurityCapabilityEntry 4 }
```

```
--
-- Table wmanIf2SsPkmTekTable
--
wmanIf2SsPkmTekTable OBJECT-TYPE
        SYNTAX      SEQUENCE OF WmanIf2SsPkmTekEntry
        MAX-ACCESS  not-accessible
        STATUS      current
        DESCRIPTION
            "This table contains the TEK attributes that are associated
             with each SAID."
        ::= { wmanIf2SsPkmV1Objects 4 }

wmanIf2SsPkmTekEntry OBJECT-TYPE
        SYNTAX      WmanIf2SsPkmTekEntry
        MAX-ACCESS  not-accessible
        STATUS      current
        DESCRIPTION
            "This table is double indexed by ifIndex and
             wmanIf2SsSaidIndex."
        INDEX       { ifIndex, wmanIf2SsPkmSaidIndex }
        ::= { wmanIf2SsPkmTekTable  1 }

WmanIf2SsPkmTekEntry ::= SEQUENCE {
        wmanIf2SsPkmSaidIndex                   INTEGER,
        wmanIf2SsPkmSaType                      WmanIf2SaType,
        wmanIf2SsPkmTekDataEncryptAlgorithm     WmanIf2DataEncryptAlgId,
        wmanIf2SsPkmTekDataAuthentAlgorithm     WmanIf2DataAuthAlgId,
        wmanIf2SsPkmTekEncryptAlgorithm         WmanIf2TekEncryptAlgId,
        wmanIf2SsPkmOlderTekSequenceNumber      Integer32,
        wmanIf2SsPkmOlderTekLifetime            Integer32,
        wmanIf2SsPkmNewerTekSequenceNumber      Integer32,
        wmanIf2SsPkmNewerTekLifetime            Integer32,
        wmanIf2SsPkmKeyRejectError              WmanIf2PkmErrorCode,
        wmanIf2SsPkmTekInvalidError             WmanIf2PkmErrorCode,
        wmanIf2SsPkmLastTekExpireTime           DateAndTime,
        wmanIf2SsPkmLatestTekExpireTime         DateAndTime,
        wmanIf2SsPkmTekState                    WmanIf2TekState}

wmanIf2SsPkmSaidIndex OBJECT-TYPE
        SYNTAX      INTEGER (0 .. 65535)
        MAX-ACCESS  not-accessible
        STATUS      current
        DESCRIPTION
            "SAID index to the wmanIf2SsPkmSaDescriptorTable."
        ::= { wmanIf2SsPkmTekEntry 1 }

wmanIf2SsPkmSaType OBJECT-TYPE
        SYNTAX      WmanIf2SaType
        MAX-ACCESS  read-only
        STATUS      current
        DESCRIPTION
            "SA Type attribute that is included in the Auth Reply
             message."
        ::= { wmanIf2SsPkmTekEntry 2 }

wmanIf2SsPkmTekDataEncryptAlgorithm OBJECT-TYPE
        SYNTAX      WmanIf2DataEncryptAlgId
        MAX-ACCESS  read-only
        STATUS      current
        DESCRIPTION
            "The data encryption algorithm attribute that is included
             in the Auth Reply message."
        REFERENCE
             "Table 375, IEEE Std 802.16-2004"
```

```
            ::= { wmanIf2SsPkmTekEntry 3 }

    wmanIf2SsPkmTekDataAuthentAlgorithm OBJECT-TYPE
            SYNTAX      WmanIf2DataAuthAlgId
            MAX-ACCESS  read-only
            STATUS      current
            DESCRIPTION
                "The data authentication algorithm attribute that is
                 included in the Auth Reply message."
            REFERENCE
                 "Table 376, IEEE Std 802.16-2004"
            ::= { wmanIf2SsPkmTekEntry 4 }

    wmanIf2SsPkmTekEncryptAlgorithm OBJECT-TYPE
            SYNTAX      WmanIf2TekEncryptAlgId
            MAX-ACCESS  read-only
            STATUS      current
            DESCRIPTION
                "The TEK key encryption algorithm attribute that is
                 included in the Auth Reply message."
            REFERENCE
                 "Table 377, IEEE Std 802.16-2004"
            ::= { wmanIf2SsPkmTekEntry 5 }

    wmanIf2SsPkmOlderTekSequenceNumber OBJECT-TYPE
            SYNTAX      Integer32 (0 .. 3)
            MAX-ACCESS  read-only
            STATUS      current
            DESCRIPTION
                "At all times the BS maintains two sets of active
                 generations of keying material per SAID. One set
                 corresponds to the 'older' generation of keying material,
                 the second set corresponds to the 'newer' generation of
                 keying material. The newer generation has a key sequence
                 number one greater than (modulo 4) that of the older
                 generation. This object provides the older TEK sequence
                 number in the Key Reply message for an SS."
            REFERENCE
                 "Subclause 11.9.8 in IEEE Std 802.16-2004"
            ::= { wmanIf2SsPkmTekEntry 6 }

    wmanIf2SsPkmOlderTekLifetime OBJECT-TYPE
            SYNTAX      Integer32 (1800 .. 604800)
            UNITS       "seconds"
            MAX-ACCESS  read-only
            STATUS      current
            DESCRIPTION
                "This object provides the older TEK Remaining Lifetime."
            REFERENCE
                 "Subclause 11.9.8 in IEEE Std 802.16-2004"
            ::= { wmanIf2SsPkmTekEntry 7 }

    wmanIf2SsPkmNewerTekSequenceNumber OBJECT-TYPE
            SYNTAX      Integer32 (0 .. 3)
            MAX-ACCESS  read-only
            STATUS      current
            DESCRIPTION
                "This object provides the newer TEK sequence
                 number in the Key Reply message for an SS."
            REFERENCE
                 "Subclause 11.9.8 in IEEE Std 802.16-2004"
            ::= { wmanIf2SsPkmTekEntry 8 }

    wmanIf2SsPkmNewerTekLifetime OBJECT-TYPE
```

```
            SYNTAX      Integer32 (1800 .. 604800)
            UNITS       "seconds"
            MAX-ACCESS  read-only
            STATUS      current
            DESCRIPTION
                "This object provides the newer TEK Remaining Lifetime."
            REFERENCE
                 "Subclause 11.9.8 in IEEE Std 802.16-2004"
            ::= { wmanIf2SsPkmTekEntry 9 }

    wmanIf2SsPkmKeyRejectError OBJECT-TYPE
            SYNTAX      WmanIf2PkmErrorCode
            MAX-ACCESS  read-only
            STATUS      current
            DESCRIPTION
                "The Error Code in the most recent Key Reject message
                 received from the BS.

                 The valid error codes are:
                   0 - no failure
                   2 - unauthorized SAID"
            REFERENCE
                 "IEEE Std 802.16-2004; Table 371"
            ::= { wmanIf2SsPkmTekEntry 10 }

    wmanIf2SsPkmTekInvalidError OBJECT-TYPE
            SYNTAX      WmanIf2PkmErrorCode
            MAX-ACCESS  read-only
            STATUS      current
            DESCRIPTION
                "The Error Code in the most recent TEK Invalid message
                 received from the BS.

                 The valid error codes are:
                   0 - no failure
                   4 - invalid key sequence"
            REFERENCE
                 "IEEE Std 802.16-2004; Table 371"
            ::= { wmanIf2SsPkmTekEntry 11 }

    wmanIf2SsPkmLastTekExpireTime OBJECT-TYPE
            SYNTAX      DateAndTime
            MAX-ACCESS  read-only
            STATUS      current
            DESCRIPTION
                "This object is the time when the last TEK expires.
                 wmanIf2SsPkmLastTekExpireTime = Time(last TEK[Key Reply])
                                                 + TEK lifetime
                 If this FSM has only one authorization key, then
                 wmanIf2SsPkmLastTekExpireTime = the activation of FSM."
            ::= { wmanIf2SsPkmTekEntry 12 }

    wmanIf2SsPkmLatestTekExpireTime OBJECT-TYPE
            SYNTAX      DateAndTime
            MAX-ACCESS  read-only
            STATUS      current
            DESCRIPTION
                "This object is the time when the latest TEK expires."
            ::= { wmanIf2SsPkmTekEntry 13 }

    wmanIf2SsPkmTekState OBJECT-TYPE
            SYNTAX      WmanIf2TekState
            MAX-ACCESS  read-only
            STATUS      current
```

```
            DESCRIPTION
                "The value of this object is the state of the indicated TEK
                 FSM. The start(1) state indicates that FSM is in its
                 initial state."
            ::= { wmanIf2SsPkmTekEntry 14 }
```

2.6 wmanIf2SsPkmV2Objects ASN.1 Code Change

13.2 ASN.1 Definitions of MIB Modules

13.2.3 wmanIf2Mib

[Add wmanIf2SsPkmV2Objects as the following in WMAN-IF2-MIB:]

```
wmanIf2SsPkmV2Objects OBJECT IDENTIFIER ::= { wmanIf2SsPkmObjects 2 }

--
-- Table wmanIf2SsPkmV2AttributeTable
--
wmanIf2SsPkmV2AttributeTable OBJECT-TYPE
        SYNTAX      SEQUENCE OF WmanIf2SsPkmV2AttributeEntry
        MAX-ACCESS  not-accessible
        STATUS      current
        DESCRIPTION
            "This table contains the PKM attributes that are needed
             to PKM operation."
        REFERENCE
            "Table 343 in IEEE Std 802.16-2004 and 802.16e-2005"
        ::= { wmanIf2SsPkmV2Objects  1 }

wmanIf2SsPkmV2AttributeEntry OBJECT-TYPE
        SYNTAX      WmanIf2SsPkmV2AttributeEntry
        MAX-ACCESS  not-accessible
        STATUS      current
        DESCRIPTION
            "Each entry contains objects that define the PKM attributes
             of each BS and SS. The table is indexed by ifIndex that is
             associated with the SS."
        INDEX       { ifIndex }
        ::= { wmanIf2SsPkmV2AttributeTable  1 }

WmanIf2SsPkmV2AttributeEntry ::= SEQUENCE {
        wmanIf2SsPkmPmkPrehandshakeLifetime     Integer32,
        wmanIf2SsPkmPmkLifetime                 Integer32,
        wmanIf2SsSaChallengeTimeout             Integer32,
        wmanIf2SsMaxSaTekChallenge              Integer32,
        wmanIf2SsSaTekTimeout                   Integer32,
        wmanIf2SsMaxSaTekRequest                Integer32}

wmanIf2SsPkmPmkPrehandshakeLifetime OBJECT-TYPE
        SYNTAX      Integer32 (5 .. 900)
        UNITS       "seconds"
        MAX-ACCESS  read-only
        STATUS      current
        DESCRIPTION
            "This object defines the PMK or PAK prehandshake lifetime."
        REFERENCE
             "Table 343 in IEEE Std 802.16e-2005"
        DEFVAL          { 10 }
        ::= { wmanIf2SsPkmV2AttributeEntry 1 }

wmanIf2SsPkmPmkLifetime OBJECT-TYPE
        SYNTAX      Integer32 (60 .. 86400)
        UNITS       "seconds"
        MAX-ACCESS  read-only
        STATUS      current
        DESCRIPTION
```

```
                "This object defines PMK lifetime, if MSK lifetime is
                 unspecified (i.e., by AAA server)."
            REFERENCE
                 "Table 343 in IEEE Std 802.16e-2005"
            DEFVAL          { 3600 }
            ::= { wmanIf2SsPkmV2AttributeEntry 2 }

    wmanIf2SsSaChallengeTimeout OBJECT-TYPE
            SYNTAX      Integer32 (500 .. 2000)
            UNITS       "milliseconds"
            MAX-ACCESS  read-only
            STATUS      current
            DESCRIPTION
                "This object defines the timeout value for SA-TEKChallenge
                 retransmission."
            REFERENCE
                 "Table 343 in IEEE Std 802.16e-2005"
            DEFVAL          { 1000 }
            ::= { wmanIf2SsPkmV2AttributeEntry 3 }

    wmanIf2SsMaxSaTekChallenge OBJECT-TYPE
            SYNTAX      Integer32 (1 .. 3)
            MAX-ACCESS  read-only
            STATUS      current
            DESCRIPTION
                "This object defines the maximum number of SA-TEK-Challenge
                 transmissions."
            REFERENCE
                 "Table 343 in IEEE Std 802.16e-2005"
            DEFVAL          { 3 }
            ::= { wmanIf2SsPkmV2AttributeEntry 4 }

    wmanIf2SsSaTekTimeout OBJECT-TYPE
            SYNTAX      Integer32 (100 .. 1000)
            UNITS       "milliseconds"
            MAX-ACCESS  read-only
            STATUS      current
            DESCRIPTION
                "This object defines the timeout value for SA-TEKRequest
                 retransmission."
            REFERENCE
                 "Table 343 in IEEE Std 802.16e-2005"
            DEFVAL          { 300 }
            ::= { wmanIf2SsPkmV2AttributeEntry 5 }

    wmanIf2SsMaxSaTekRequest OBJECT-TYPE
            SYNTAX      Integer32 (1 .. 3)
            MAX-ACCESS  read-only
            STATUS      current
            DESCRIPTION
                "This object defines the maximum number of SA-TEK-Request
                 retransmission."
            REFERENCE
                 "Table 343 in IEEE Std 802.16e-2005"
            DEFVAL          { 3 }
            ::= { wmanIf2SsPkmV2AttributeEntry 6 }

    --
    -- Table wmanIf2SsPkmV2RsaAuthTable
    --
    wmanIf2SsPkmV2RsaAuthTable OBJECT-TYPE
            SYNTAX      SEQUENCE OF WmanIf2SsPkmV2RsaAuthEntry
            MAX-ACCESS  not-accessible
            STATUS      current
```

```
            DESCRIPTION
                "This table contains information related to PKMV2
                 RSA based authorization process."
            REFERENCE
                "Subclause 6.3.2.3.9.11 in IEEE Std 802.16e-2005"
            ::= { wmanIf2SsPkmV2Objects 2 }

    wmanIf2SsPkmV2RsaAuthEntry OBJECT-TYPE
            SYNTAX      WmanIf2SsPkmV2RsaAuthEntry
            MAX-ACCESS  not-accessible
            STATUS      current
            DESCRIPTION
                "The table is indexed by ifIndex."
            INDEX       { ifIndex }
            ::= { wmanIf2SsPkmV2RsaAuthTable  1 }

    WmanIf2SsPkmV2RsaAuthEntry ::= SEQUENCE {
            wmanIf2SsPkmV2BsCertificate             OCTET STRING,
            wmanIf2SsPkmV2SsCertificate             OCTET STRING,
            wmanIf2SsPkmV2SaId                      INTEGER,
            wmanIf2SsPkmV2SsRandom                  OCTET STRING,
            wmanIf2SsPkmV2BsRandom                  OCTET STRING,
            wmanIf2SsPkmV2AuthKeySequenceNumber     Integer32,
            wmanIf2SsPkmV2AuthKeyLifetime           Integer32,
            wmanIf2SsPkmV2AuthFailure               WmanIf2PkmErrorCode,
            wmanIf2SsPkmV2LastAkExpireTime          DateAndTime,
            wmanIf2SsPkmV2LatestAkExpireTime        DateAndTime}

    wmanIf2SsPkmV2BsCertificate OBJECT-TYPE
            SYNTAX      OCTET STRING (SIZE(0..65535))
            MAX-ACCESS  read-only
            STATUS      current
            DESCRIPTION
                "BS sends the BS-Certificate in the PKMV2 RSA-Reply message
                 for BS-SS mutual authentication. It is the DER-encoded
                 ASN.1 X.509 BS Certificate."
            REFERENCE
                "Subclause 11.9.24 in IEEE Std 802.16e-2005"
            ::= { wmanIf2SsPkmV2RsaAuthEntry 1 }

    wmanIf2SsPkmV2SsCertificate OBJECT-TYPE
            SYNTAX      OCTET STRING (SIZE(0..65535))
            MAX-ACCESS  read-only
            STATUS      current
            DESCRIPTION
                "SS sends the SS-Certificate in the PKMV2 RSA-Request
                 message. It contains an X.509 SS certificate issued by the
                 SS's manufacturer. The SS's X.509 certificate is a
                 public-key certificate which binds the SS's identifying
                 information to its RSA public key in a verifiable manner.
                 The X.509 certificate is digitally signed by the SS's
                 manufacturer, and that signature can be verified by a BS
                 that knows the manufacturer's public key.
                 The manufacturer's public key is placed in an X.509
                 certification authority (CA) certificate, which in turn
                 is signed by a higher level CA."
            REFERENCE
                "Subclause 11.9.12 in IEEE Std 802.16-2004"
            ::= { wmanIf2SsPkmV2RsaAuthEntry 2 }

    wmanIf2SsPkmV2SaId OBJECT-TYPE
            SYNTAX      INTEGER (0..65535)
            MAX-ACCESS  read-only
            STATUS      current
```

```
            DESCRIPTION
                "SS's primary SAID equal to the Basic CID. SS sends the SAID
                 in the PKMV2 RSA-Request message."
            REFERENCE
                 "Subclause 6.3.2.3.9.2 in IEEE Std 802.16-2004"
            ::= { wmanIf2SsPkmV2RsaAuthEntry 3 }

    wmanIf2SsPkmV2SsRandom OBJECT-TYPE
            SYNTAX      OCTET STRING (SIZE(8))
            MAX-ACCESS  read-only
            STATUS      current
            DESCRIPTION
                "This attribute contains a quantity that is pseudo random
                 number generated from the MS and used as fresh number for
                 mutual authorization message handshake. SS sends the SS-Random
                 in the PKMV2 RSA-Request message."
            REFERENCE
                "Subclause 11.9.21 in IEEE Std 802.16e-2005"
            ::= { wmanIf2SsPkmV2RsaAuthEntry 4 }

    wmanIf2SsPkmV2BsRandom OBJECT-TYPE
            SYNTAX      OCTET STRING (SIZE(8))
            MAX-ACCESS  read-only
            STATUS      current
            DESCRIPTION
                "This attribute contains a quantity that is pseudo random
                 number generated from the BS and used as fresh number for
                 mutual authorization message handshake.BS sends the BS-Random
                 in the PKMV2 RSA-Reply message."
            REFERENCE
                "Subclause 11.9.22 in IEEE Std 802.16e-2005"
            ::= { wmanIf2SsPkmV2RsaAuthEntry 5 }

    wmanIf2SsPkmV2AuthKeySequenceNumber OBJECT-TYPE
            SYNTAX      Integer32 (0 .. 15)
            MAX-ACCESS  read-only
            STATUS      current
            DESCRIPTION
                "This object provides the most recent authorization key
                 sequence number in the PKMV2 RSA-Reply message for an SS."
            REFERENCE
                 "Subclause 11.9.5 in IEEE Std 802.16e-2005"
            ::= { wmanIf2SsPkmV2RsaAuthEntry 6 }

    wmanIf2SsPkmV2AuthKeyLifetime OBJECT-TYPE
            SYNTAX      Integer32 (86400..6048000)
            UNITS       "seconds"
            MAX-ACCESS  read-only
            STATUS      current
            DESCRIPTION
                "This object defines the lifetime of an authorization
                 key (AK) the BS assigns to a SS. BS sends the key lifetime
                 in the PKMV2 RSA-Reply message."
            REFERENCE
                 "Subclause 11.9.4 in IEEE Std 802.16e-2005"
            ::= { wmanIf2SsPkmV2RsaAuthEntry 7 }

    wmanIf2SsPkmV2AuthFailure OBJECT-TYPE
            SYNTAX      WmanIf2PkmErrorCode
            MAX-ACCESS  read-only
            STATUS      current
            DESCRIPTION
                "BS returs PKMV2 RSA-Rejects message if an authorization
                 failure is detected.
```

```
"
        REFERENCE
             "Subclause 11.9.10 in IEEE Std 802.16-2004"
        ::= { wmanIf2SsPkmV2RsaAuthEntry 8 }

wmanIf2SsPkmV2LastAkExpireTime OBJECT-TYPE
        SYNTAX      DateAndTime
        MAX-ACCESS  read-only
        STATUS      current
        DESCRIPTION
            "This object is the time when the last AK expires.
             wmanIf2SsPkmV2LastAkExpireTime = Time(last AK[RSA-Reply])
                                                + AK lifetime
             If this FSM has only one authorization key, then
             wmanIf2SsPkmV2LastAkExpireTime = the activation of FSM."
        ::= { wmanIf2SsPkmV2RsaAuthEntry 9 }

wmanIf2SsPkmV2LatestAkExpireTime OBJECT-TYPE
        SYNTAX      DateAndTime
        MAX-ACCESS  read-only
        STATUS      current
        DESCRIPTION
            "This object is the time when the latest AK expires."
        ::= { wmanIf2SsPkmV2RsaAuthEntry 10 }

--
-- Table wmanIf2SsPkmV2TekTable
--
wmanIf2SsPkmV2TekTable OBJECT-TYPE
        SYNTAX      SEQUENCE OF WmanIf2SsPkmV2TekEntry
        MAX-ACCESS  not-accessible
        STATUS      current
        DESCRIPTION
            "This table contains the TEK attributes that are associated
             with each SAID."
        ::= { wmanIf2SsPkmV2Objects 3 }

wmanIf2SsPkmV2TekEntry OBJECT-TYPE
        SYNTAX      WmanIf2SsPkmV2TekEntry
        MAX-ACCESS  not-accessible
        STATUS      current
        DESCRIPTION
            "This table is double indexed by ifIndex and
             wmanIf2SsPkmSaidIndex."
        INDEX       { ifIndex,
                      wmanIf2SsPkmV2SaidIndex }
        ::= { wmanIf2SsPkmV2TekTable  1 }

WmanIf2SsPkmV2TekEntry ::= SEQUENCE {
        wmanIf2SsPkmV2SaidIndex                 INTEGER,
        wmanIf2SsPkmV2SaType                    WmanIf2SaType,
        wmanIf2SsPkmV2OlderTekSequenceNumber    Integer32,
        wmanIf2SsPkmV2OlderTekLifetime          Integer32,
        wmanIf2SsPkmV2NewerTekSequenceNumber    Integer32,
        wmanIf2SsPkmV2NewerTekLifetime          Integer32,
        wmanIf2SsPkmV2AuthInvalidError          WmanIf2PkmErrorCode,
        wmanIf2SsPkmV2LastTekExpireTime         DateAndTime,
        wmanIf2SsPkmV2LatestTekExpireTime       DateAndTime}

wmanIf2SsPkmV2SaidIndex OBJECT-TYPE
        SYNTAX      INTEGER (0 .. 65535)
        MAX-ACCESS  not-accessible
        STATUS      current
        DESCRIPTION
```

```
            "SAID index to the wmanIf2SsPkmV2TekTable."
        ::= { wmanIf2SsPkmV2TekEntry 1 }

wmanIf2SsPkmV2SaType OBJECT-TYPE
        SYNTAX      WmanIf2SaType
        MAX-ACCESS  read-only
        STATUS      current
        DESCRIPTION
            "SA Type attribute that is included in the Auth Reply
             message."
        ::= { wmanIf2SsPkmV2TekEntry 2 }

wmanIf2SsPkmV2OlderTekSequenceNumber OBJECT-TYPE
        SYNTAX      Integer32 (0 .. 3)
        MAX-ACCESS  read-only
        STATUS      current
        DESCRIPTION
            "At all times the BS maintains two sets of active
             generations of keying material per SAID. One set
             corresponds to the 'older' generation of keying material,
             the second set corresponds to the 'newer' generation of
             keying material. The newer generation has a key sequence
             number one greater than (modulo 4) that of the older
             generation. This object provides the older TEK sequence
             number in the Key Reply message for an SS."
        REFERENCE
             "Subclause 11.9.8 in IEEE Std 802.16-2004"
        ::= { wmanIf2SsPkmV2TekEntry 3 }

wmanIf2SsPkmV2OlderTekLifetime OBJECT-TYPE
        SYNTAX      Integer32 (1800 .. 604800)
        UNITS       "seconds"
        MAX-ACCESS  read-only
        STATUS      current
        DESCRIPTION
            "This object provides the older TEK Remaining Lifetime."
        REFERENCE
             "Subclause 11.9.8 in IEEE Std 802.16-2004"
        ::= { wmanIf2SsPkmV2TekEntry 4 }

wmanIf2SsPkmV2NewerTekSequenceNumber OBJECT-TYPE
        SYNTAX      Integer32 (0 .. 3)
        MAX-ACCESS  read-only
        STATUS      current
        DESCRIPTION
            "This object provides the newer TEK sequence
             number in the Key Reply message for an SS."
        REFERENCE
             "Subclause 11.9.8 in IEEE Std 802.16-2004"
        ::= { wmanIf2SsPkmV2TekEntry 5 }

wmanIf2SsPkmV2NewerTekLifetime OBJECT-TYPE
        SYNTAX      Integer32 (1800 .. 604800)
        UNITS       "seconds"
        MAX-ACCESS  read-only
        STATUS      current
        DESCRIPTION
            "This object provides the newer TEK Remaining Lifetime."
        REFERENCE
             "Subclause 11.9.8 in IEEE Std 802.16-2004"
        ::= { wmanIf2SsPkmV2TekEntry 6 }

wmanIf2SsPkmV2AuthInvalidError OBJECT-TYPE
        SYNTAX      WmanIf2PkmErrorCode
```

```
            MAX-ACCESS  read-only
            STATUS      current
            DESCRIPTION
                "BS returs Authorization Invalid message if an authorization
                 invlaid error is detected."
            REFERENCE
                 "Subclause 11.9.10 in IEEE Std 802.16-2004"
            ::= { wmanIf2SsPkmV2TekEntry 7 }

    wmanIf2SsPkmV2LastTekExpireTime OBJECT-TYPE
            SYNTAX      DateAndTime
            MAX-ACCESS  read-only
            STATUS      current
            DESCRIPTION
                "This object is the time when the last TEK expires.
                 wmanIf2SsPkmV2LastTekExpireTime = Time(last TEK[Key Reply])
                                                     + TEK lifetime
                 If this FSM has only one authorization key, then
                 wmanIf2SsPkmV2LastTekExpireTime = the activation of FSM."
            ::= { wmanIf2SsPkmV2TekEntry 8 }

    wmanIf2SsPkmV2LatestTekExpireTime OBJECT-TYPE
            SYNTAX      DateAndTime
            MAX-ACCESS  read-only
            STATUS      current
            DESCRIPTION
                "This object is the time when the latest TEK expires."
            ::= { wmanIf2SsPkmV2TekEntry 9 }
```