

Project	<b>IEEE 802.16 Broadband Wireless Access Working Group</b> < <a href="http://ieee802.org/16">http://ieee802.org/16</a> >
Title	<b>Proposed text and ASN.1 code to support PKMV1 and PKMV2</b>
Date Submitted	<b>2007-01-11</b>
Source(s)	Joey Chou Intel Corporation <a href="mailto:joey.chou@intel.com">[mailto:joey.chou@intel.com]</a>
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	<p>The contributor is familiar with the IEEE 802.16 Patent Policy and Procedures (Version 1.0) &lt;<a href="http://ieee802.org/16/ipr/patents/policy.html">http://ieee802.org/16/ipr/patents/policy.html</a>&gt;, 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."</p> <p>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 &lt;<a href="mailto:r.b.marks@ieee.org">mailto:r.b.marks@ieee.org</a>&gt; 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 &lt;<a href="http://ieee802.org/16/ipr/patents/notices">http://ieee802.org/16/ipr/patents/notices</a>&gt;.</p>

*Table of Content*

- 1. Introduction..... 4**
- 2. NRM IRP SNMP Solution Set change Proposal..... 4**
- 2.1 wmanlf2BsPkmObjects Changes..... 4**
- 2.2 wmanlf2SsPkmObjects Changes..... 6**
- 2.3 wmanlf2BsPkmObjects ASN.1 Code Change..... 8**
- 2.4 wmanlf2BsPkmV2Objects ASN.1 Code Change..... 20**
- 2.5 wmanlf2SsPkmObjects ASN.1 Code Change..... 28**
- 2.6 wmanlf2SsPkmV2Objects ASN.1 Code Change..... 37**

1

1

## 2 1. Introduction

2

3 This contribution proposes the text and ASN.1 code in wmanlf2Mib to support PKMV1 and PKMV2.

## 4 2. NRM IRP SNMP Solution Set change Proposal

4

### 5 2.1 wmanlf2BsPkmObjects Changes

5

#### 6 13.1.3.1 wmanlf2BsObjects

6

7 [\[Change Subclause 13.1.3.1.3 as the following:\]](#)

7

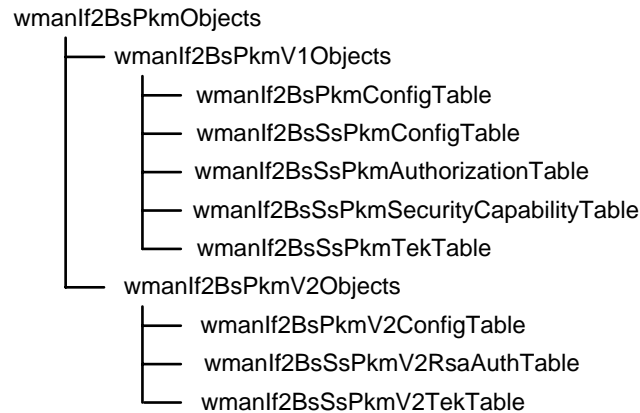
8

#### 9 13.1.3.1.3 wmanlf2BsPkmObjects

9

10 Figure 8 shows the structure of wmanlf2BsPkmObjects subtree that contains BS managed objects  
11 related to the MAC privacy management entity.

11



12

13

14

15

Figure 8— wmanlf2BsPkmObjects structure

#### 16 13.1.3.1.3.1 wmanlf2BsPkmV1Objects

16

##### 17 13.1.3.1.3.1.1 wmanlf2BsPkmConfigTable

17

18 wmanlf2BsPkmConfigTable contains the configuration of the PKM attributes that are needed to  
19 PKM operation.

19

##### 20 13.1.3.1.3.1.2 wmanlf2BsSsPkmConfigTable

20

21 wmanlf2BsSsPkmConfigTable contains the configuration of the PKM attributes on per SS basis.

21

##### 22 13.1.3.1.3.1.3 wmanlf2BsSsPkmAuthorizationTable

22

23 wmanlf2BsSsPkmAuthorizationTable contains information related to SS's authorization process.

23

1     **13.1.3.1.3.1.4 wmanIf2BsSsPkmSecurityCapabilityTable**

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

5     **13.1.3.1.3.1.5 wmanIf2BsSsPkmTekTable**

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

7     **13.1.3.1.3.2 wmanIf2BsPkmV2Objects**

8     **13.1.3.1.3.2.1 wmanIf2BsPkmV2ConfigTable**

9     wmanIf2BsPkmV2ConfigTable contains the configuration of the PKM attributes that are needed to  
10    PKM operation.

11    **13.1.3.1.3.2.2 wmanIf2BsSsPkmV2RsaAuthTable**

12    wmanIf2BsSsPkmV2RsaAuthTable contains information related to PKMV2 RSA based  
13    authorization process.

14    **13.1.3.1.3.2.3 wmanIf2BsSsPkmV2TekTable**

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

1 **2.2 wmanlf2SsPkmObjects Changes**

2 **13.1.3.1 wmanlf2BsObjects**

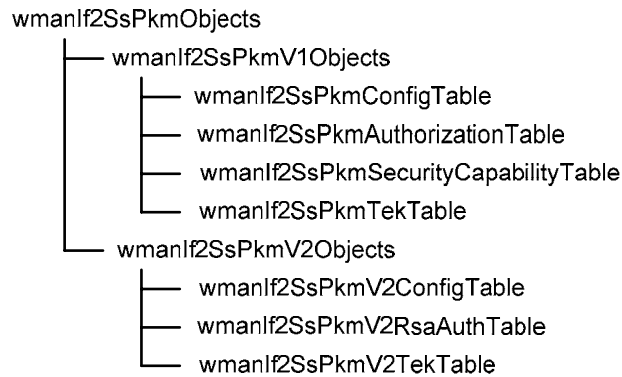
3 [\[Change Subclause 13.1.3.2.2 as the following:\]](#)

4

5 **13.1.3.2.2 wmanlf2SsPkmObjects**

6 Figure 12 shows the structure of wmanlf2SsPkmObjects subtree that contains subscriber station  
7 manageable objects related to the privacy management entity.

8



9

10

11

12

**Figure 12— wmanlf2SsPkmObjects structure**

13 **13.1.3.2.2.1 wmanlf2BsPkmV1Objects**

14 **13.1.3.2.2.1.1 wmanlf2SsPkmConfigTable**

15 wmanlf2SsPkmConfigTable provides the configuration of the PKM attributes that are needed to  
16 PKM operation.

17 **13.1.3.2.2.1.2 wmanlf2SsPkmAuthorizationTable**

18 wmanlf2SsPkmAuthorizationTable contains information that are related to SS's authorization  
19 proces.

20 **13.1.3.2.2.1.3 wmanlf2SsPkmSecurityCapabilityTable**

21 wmanlf2SsPkmSecurityCapabilityTable contains the SS's Security Capabilities that are conveyed  
22 by the Auth Request message. It contains the list of the cryptographic suite(s) an SS supports.

23 **13.1.3.2.2.1.4 wmanlf2SsPkmTekTable**

24 wmanlf2SsPkmTekTable contains the TEK attributes that are associated with each SAID.

1     **13.1.3.2.2.2 wmanIf2BsPkmV2Objects**

2     **13.1.3.2.2.2.1 wmanIf2SsPkmV2ConfigTable**

3     wmanIf2SsPkmV2ConfigTable contains the configuration of the PKM attributes that are needed to  
4     PKM operation.

5     **13.1.3.2.2.2.2 wmanIf2SsPkmV2RsaAuthTable**

6     wmanIf2SsPkmV2RsaAuthTable contains information related to PKMV2 RSA based authorization  
7     process.

8     **13.1.3.2.2.2.3 wmanIf2SsPkmV2TekTable**

9     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

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

```

7 WmanIf2AuthFailureType ::= TEXTUAL-CONVENTION
8     STATUS          current
9     DESCRIPTION
10        "The type of authorization failure leading to Auth Reject
11        message.
12         1 - no failure
13         2 - unauthorized SS
14         3 - unauthorized SAID
15         4 - the BS does not have the CA certificate belonging
16         to the issuer of an SS certificate
17         5 - SS certificate has an invalid signature
18         6 - ASN.1 parsing failure during verification of SS
19         certificate
20         7 - SS certificate is on the 'hot list'
21         8 - inconsistencies between certificate data and data
22         in accompanying PKM attributes
23         9 - SS and BS have incompatible security capabilities"
24     REFERENCE
25        "Subclause 11.9.10 in IEEE Std 802.16-2004"
26     SYNTAX          INTEGER {noFailure(1),
27                        unauthorizedSs(2),
28                        unauthorizedSaid(3),
29                        unknownManufactur(4),
30                        invalidSignature(5),
31                        asn1ParsingFailure(6),
32                        ssCaOnHotList(7),
33                        dataInconsistency(8),
34                        ssBsIncompatibleSc(9)}
35
36
37 WmanIf2AuthInvalidError ::= TEXTUAL-CONVENTION
38     STATUS          current
39     DESCRIPTION
40        "The type of error leading to Auth Invalid message.
41         1 - no error
42         2 - unauthorized SAID
43         3 - unsolicited
44         4 - invalid key sequence number
45         5 - key request authentication failure"
46     REFERENCE
47        "Subclause 11.9.10 in IEEE Std 802.16-2004"
48     SYNTAX          INTEGER {noError(1),
49                        unauthorizedSaid(2),
50                        unsolicited(3),
51                        invalidKeySeqNumber(4),
52                        keyReqAuthFailure(5)}
53
54
55 WmanIf2SaType ::= TEXTUAL-CONVENTION
56     STATUS          current
57     DESCRIPTION
58        "The type of Security Association (SA)."
```

```

1      REFERENCE
2          "Table 379 in IEEE Std 802.16-2004"
3      SYNTAX      INTEGER {primarySa(0),
4                  staticSa(1),
5                  dynamicSa(2)}
6
7
8      WmanIf2TekState ::= TEXTUAL-CONVENTION
9          STATUS      current
10         DESCRIPTION
11             "TEK State."
12         REFERENCE
13             "Subclause 7.2.5.1 in IEEE Std 802.16-2004"
14         SYNTAX      INTEGER {start(1),
15                             opWait(2),
16                             opReauthWait(3),
17                             operational(4),
18                             rekeyWait(5),
19                             rekeyReauthWait(6)}
20
21     --
22     -- Base station PKM group
23     -- wmanIf2BsPkmObjects contain the Base Station Privacy Sublayer objects
24     --
25     wmanIf2BsPkmObjects OBJECT IDENTIFIER ::= { wmanIf2BsObjects 3 }
26
27     wmanIf2BsPkmV1Objects OBJECT IDENTIFIER ::= { wmanIf2BsPkmObjects 1 }
28
29     --
30     -- Table wmanIf2BsPkmConfigTable
31     --
32     wmanIf2BsPkmConfigTable OBJECT-TYPE
33         SYNTAX      SEQUENCE OF WmanIf2BsPkmConfigEntry
34         MAX-ACCESS  not-accessible
35         STATUS      current
36         DESCRIPTION
37             "This table contains the configuration of the PKM
38             attributes that are needed to PKM operation."
39         REFERENCE
40             "Table 343 in IEEE Std 802.16-2004 and 802.16e-2005"
41         ::= { wmanIf2BsPkmV1Objects 1 }
42
43     wmanIf2BsPkmConfigEntry OBJECT-TYPE
44         SYNTAX      WmanIf2BsPkmConfigEntry
45         MAX-ACCESS  not-accessible
46         STATUS      current
47         DESCRIPTION
48             "Each entry contains objects that define the PKM attributes
49             of each BS wireless interface. The table is indexed by
50             ifIndex that is associated with the BS sector."
51         INDEX      { ifIndex }
52         ::= { wmanIf2BsPkmConfigTable 1 }
53
54     WmanIf2BsPkmConfigEntry ::= SEQUENCE {
55         wmanIf2BsPkmAkLifetime      Integer32,
56         wmanIf2BsPkmTekLifetime     Integer32,
57         wmanIf2BsPkmSelfSigManufCertTrust  INTEGER,
58         wmanIf2BsPkmCheckCertValidityPeriods  TruthValue}
59
60     wmanIf2BsPkmAkLifetime OBJECT-TYPE
61         SYNTAX      Integer32 (86400 .. 6048000)
62         UNITS      "seconds"
63         MAX-ACCESS  read-write
64         STATUS      current

```



```

1      DESCRIPTION
2          "This object defines the lifetime of a newly assigned
3          authorization key."
4      REFERENCE
5          "Table 343 in IEEE Std 802.16-2004"
6      DEFVAL      { 604800 }
7      ::= { wmanIf2BsPkmConfigEntry 1 }
8
9      wmanIf2BsPkmTekLifetime OBJECT-TYPE
10     SYNTAX      Integer32 (1800 .. 604800)
11     UNITS       "seconds"
12     MAX-ACCESS  read-write
13     STATUS      current
14     DESCRIPTION
15         "This object defines the lifetime of a newly assigned
16         Traffic Encryption Key (TEK)."

```

```

1      DESCRIPTION
2          "Each entry contains objects that define the PKM attributes
3          of each SS wireless interface. The table is indexed by
4          ifIndex and wmanIf2BsSsMacAddress."
5      INDEX          { ifIndex, wmanIf2BsSsMacAddress }
6      ::= { wmanIf2BsSsPkmConfigTable 1 }
7
8      WmanIf2BsSsPkmConfigEntry ::= SEQUENCE {
9          wmanIf2BsSsPkmAuthWaitTimeout      Integer32,
10         wmanIf2BsSsPkmReauthWaitTimeout    Integer32,
11         wmanIf2BsSsPkmAuthGraceTime       Integer32,
12         wmanIf2BsSsPkmOpWaitTimeout       Integer32,
13         wmanIf2BsSsPkmRekeyWaitTimeout    Integer32,
14         wmanIf2BsSsPkmTekGraceTime       Integer32,
15         wmanIf2BsSsPkmAuthRejectWaitTimeout Integer32,
16         wmanIf2BsSsPkmAuthReset          INTEGER}
17
18     wmanIf2BsSsPkmAuthWaitTimeout OBJECT-TYPE
19         SYNTAX      Integer32 (2 .. 30)
20         UNITS       "seconds"
21         MAX-ACCESS  read-write
22         STATUS      current
23         DESCRIPTION
24             "This object defines the Auth Req retransmission interval
25             from Auth Wait state."
26         REFERENCE
27             "Table 343 and subclause 11.9.19 in IEEE Std 802.16-2004"
28         DEFVAL     { 10 }
29         ::= { wmanIf2BsSsPkmConfigEntry 1 }
30
31     wmanIf2BsSsPkmReauthWaitTimeout OBJECT-TYPE
32         SYNTAX      Integer32 (2 .. 30)
33         UNITS       "seconds"
34         MAX-ACCESS  read-write
35         STATUS      current
36         DESCRIPTION
37             "This object defines the Auth Req retransmission interval
38             from Reauth Wait state."
39         REFERENCE
40             "Table 343 and subclause 11.9.19 in IEEE Std 802.16-2004"
41         DEFVAL     { 10 }
42         ::= { wmanIf2BsSsPkmConfigEntry 2 }
43
44     wmanIf2BsSsPkmAuthGraceTime OBJECT-TYPE
45         SYNTAX      Integer32 (300 .. 3024000)
46         UNITS       "seconds"
47         MAX-ACCESS  read-write
48         STATUS      current
49         DESCRIPTION
50             "The value of this object is the grace time for an
51             authorization key. A SS is expected to start trying to get
52             a new authorization key beginning AuthGraceTime seconds
53             before the authorization key actually expires."
54         REFERENCE
55             "Table 343 and subclause 11.9.19 in IEEE Std 802.16-2004"
56         DEFVAL     { 600 }
57         ::= { wmanIf2BsSsPkmConfigEntry 3 }
58
59     wmanIf2BsSsPkmOpWaitTimeout OBJECT-TYPE
60         SYNTAX      Integer32 (1 .. 10)
61         UNITS       "seconds"
62         MAX-ACCESS  read-write
63         STATUS      current
64         DESCRIPTION

```

```

1           "This object defines the Key Req retransmission interval
2           from Op Wait state."
3     REFERENCE
4           "Table 343 and subclause 11.9.19 in IEEE Std 802.16-2004"
5     DEFVAL      { 1 }
6     ::= { wmanIf2BsSsPkmConfigEntry 4 }
7
8     wmanIf2BsSsPkmRekeyWaitTimeout OBJECT-TYPE
9       SYNTAX      Integer32 (1 .. 10)
10      UNITS       "seconds"
11      MAX-ACCESS  read-write
12      STATUS      current
13      DESCRIPTION
14        "This object defines the Key Req retransmission interval
15        from Rekey Wait state."
16      REFERENCE
17        "Table 343 and subclause 11.9.19 in IEEE Std 802.16-2004"
18      DEFVAL      { 1 }
19      ::= { wmanIf2BsSsPkmConfigEntry 5 }
20
21     wmanIf2BsSsPkmTekGraceTime OBJECT-TYPE
22      SYNTAX      Integer32 (300 .. 3024000)
23      UNITS       "seconds"
24      MAX-ACCESS  read-write
25      STATUS      current
26      DESCRIPTION
27        "The value of this object is the grace time for the TEK in
28        seconds. The SS is expected to start trying to acquire a
29        new TEK beginning TEK GraceTime seconds before the
30        expiration of the most recent TEK."
31      REFERENCE
32        "Table 343 and subclause 11.9.19 in IEEE Std 802.16-2004"
33      DEFVAL      { 3600 }
34      ::= { wmanIf2BsSsPkmConfigEntry 6 }
35
36     wmanIf2BsSsPkmAuthRejectWaitTimeout OBJECT-TYPE
37      SYNTAX      Integer32 (10 .. 600)
38      UNITS       "seconds"
39      MAX-ACCESS  read-write
40      STATUS      current
41      DESCRIPTION
42        "This object defines the Delay before resending Auth Request
43        after receiving Auth Reject."
44      REFERENCE
45        "Table 343 and subclause 11.9.19 in IEEE Std 802.16-2004"
46      DEFVAL      { 60 }
47      ::= { wmanIf2BsSsPkmConfigEntry 7 }
48
49     wmanIf2BsSsPkmAuthReset OBJECT-TYPE
50      SYNTAX      INTEGER {noResetRequested(1),
51                        invalidateAuth(2),
52                        sendAuthInvalid(3),
53                        invalidateTeks(4)}
54      MAX-ACCESS  read-write
55      STATUS      current
56      DESCRIPTION
57        "Setting this object to:
58          1 - no reset
59          2 - causes the BS to invalidate the current SS
60             authorization key(s), but not to transmit an
61             Authorization Invalid message nor to invalidate
62             unicast TEKs.
63          3 - causes the BS to invalidate the current SS
64             authorization key(s), and to transmit an

```

```

1           Authorization Invalid message to the SS, but not
2           to invalidate unicast TEKs.
3           4 - causes the BS to invalidate the current SS
4           authorization key(s), to transmit an Authorization
5           Invalid message to the SS, and to invalidate all
6           unicast TEKs associated with this SS authorization.
7           Reading this object returns the most-recently-set value
8           of this object, or returns noResetRequested(1) if the
9           object has not been set since the last BS reboot."
10          ::= { wmanIf2BsSsPkmConfigEntry 8 }
11
12          --
13          -- Table wmanIf2BsSsPkmAuthorizationTable
14          --
15          wmanIf2BsSsPkmAuthorizationTable OBJECT-TYPE
16              SYNTAX          SEQUENCE OF WmanIf2BsSsPkmAuthorizationEntry
17              MAX-ACCESS      not-accessible
18              STATUS          current
19              DESCRIPTION
20                  "This table contains information related to SS's
21                  authorization process."
22              REFERENCE
23                  "Table 28 and 37 in IEEE Std 802.16-2004"
24              ::= { wmanIf2BsPkmV1Objects 3 }
25
26          wmanIf2BsSsPkmAuthorizationEntry OBJECT-TYPE
27              SYNTAX          WmanIf2BsSsPkmAuthorizationEntry
28              MAX-ACCESS      not-accessible
29              STATUS          current
30              DESCRIPTION
31                  "Each entry contains objects that define the SS
32                  authorization attributes for each SS associated with each
33                  BS sector. The table is indexed by ifIndex and
34                  wmanIf2BsSsMacAddress."
35              INDEX          { ifIndex, wmanIf2BsSsMacAddress }
36              ::= { wmanIf2BsSsPkmAuthorizationTable 1 }
37
38          WmanIf2BsSsPkmAuthorizationEntry ::= SEQUENCE {
39              wmanIf2BsSsPkmCaCertificate          OCTET STRING,
40              wmanIf2BsSsPkmSsCertificate          OCTET STRING,
41              wmanIf2BsSsPkmSaId                  INTEGER,
42              wmanIf2BsSsPkmAuthKeySequenceNumber Integer32,
43              wmanIf2BsSsPkmAuthKeyLifetime       Integer32,
44              wmanIf2BsSsPkmAuthFailure           WmanIf2AuthFailureType,
45              wmanIf2BsSsPkmLastAkExpireTime     DateAndTime,
46              wmanIf2BsSsPkmLatestAkExpireTime   DateAndTime,
47              wmanIf2BsSsPkmCertificateStatus     INTEGER}
48
49          wmanIf2BsSsPkmCaCertificate OBJECT-TYPE
50              SYNTAX          OCTET STRING (SIZE(0..65535))
51              MAX-ACCESS      read-only
52              STATUS          current
53              DESCRIPTION
54                  "SS sends the CA-Certificate in the Auth Info message. It
55                  contains an X.509 CA certificate for the manufacturer of
56                  the SS. The SS's X.509 user certificate shall have been
57                  issued by the CA identified by the X.509 CA certificate."
58              REFERENCE
59                  "Table 37 in IEEE Std 802.16-2004"
60              ::= { wmanIf2BsSsPkmAuthorizationEntry 1 }
61
62          wmanIf2BsSsPkmSsCertificate OBJECT-TYPE
63              SYNTAX          OCTET STRING (SIZE(0..65535))
64              MAX-ACCESS      read-only

```

```

1      STATUS      current
2      DESCRIPTION
3          "SS sends the SS-Certificate in the Auth Request message.
4          It contains an X.509 SS certificate issued by the SS's
5          manufacturer. The SS's X.509 certificate is a public-key
6          certificate which binds the SS's identifying information
7          to its RSA public key in a verifiable manner. The X.509
8          certificate is digitally signed by the SS's manufacturer,
9          and that signature can be verified by a BS that knows
10         the manufacturer's public key. The manufacturer's public
11         key is placed in an X.509 certification authority (CA)
12         certificate, which in turn is signed by a higher level CA."
13     REFERENCE
14         "Table 28 in IEEE Std 802.16-2004"
15     ::= { wmanIf2BsSsPkmAuthorizationEntry 2 }
16
17     wmanIf2BsSsPkmSaId OBJECT-TYPE
18         SYNTAX      INTEGER (0..65535)
19         MAX-ACCESS  read-only
20         STATUS      current
21         DESCRIPTION
22             "SS's primary SAID equal to the Basic CID."
23         REFERENCE
24             "Subclause 6.3.2.3.9.2 in IEEE Std 802.16-2004"
25     ::= { wmanIf2BsSsPkmAuthorizationEntry 3 }
26
27     wmanIf2BsSsPkmAuthKeySequenceNumber OBJECT-TYPE
28         SYNTAX      Integer32 (0 .. 15)
29         MAX-ACCESS  read-only
30         STATUS      current
31         DESCRIPTION
32             "This object provides the most recent authorization key
33             sequence number in the Auth Reply message for an SS."
34         REFERENCE
35             "Table 29 in IEEE Std 802.16-2004"
36     ::= { wmanIf2BsSsPkmAuthorizationEntry 4 }
37
38     wmanIf2BsSsPkmAuthKeyLifetime OBJECT-TYPE
39         SYNTAX      Integer32 (86400..6048000)
40         UNITS       "seconds"
41         MAX-ACCESS  read-only
42         STATUS      current
43         DESCRIPTION
44             "This object defines the lifetime of an authorization
45             key (AK) the BS assigns to a SS."
46         REFERENCE
47             "Table 343 in IEEE Std 802.16-2004"
48     ::= { wmanIf2BsSsPkmAuthorizationEntry 5 }
49
50     wmanIf2BsSsPkmAuthFailure OBJECT-TYPE
51         SYNTAX      WmanIf2AuthFailureType
52         MAX-ACCESS  read-only
53         STATUS      current
54         DESCRIPTION
55             "BS returns Authorization Rejects message if an authorization
56             failure is detected.
57
58             Failure type unknownManufactur(4)- ssBsIncompatibleSc(9) are
59             considered permanent authorization failure, since any
60             attempts of reauthorization would continue to result in
61             Authorization Rejects. Details about the cause of a
62             Permanent Authorization Failure may be reported to the SS
63             in an optional Display-String attribute that may accompany
64             the Error-Code attribute in Authorization Reject messages.

```

```

1
2     Note that the BS may log the Display-String attribute and
3     Authorization failures in wmanIfDevMib, and generate a trap
4     to an SNMP manager."
5     REFERENCE
6     "Subclause 11.9.10 in IEEE Std 802.16-2004"
7     ::= { wmanIf2BsSsPkmAuthorizationEntry 6 }
8
9     wmanIf2BsSsPkmLastAkExpireTime OBJECT-TYPE
10        SYNTAX      DateAndTime
11        MAX-ACCESS  read-only
12        STATUS      current
13        DESCRIPTION
14            "This object is the time when the last AK expires.
15             wmanIf2BsSsPkmLastAkExpireTime = Time(last AK[Auth Reply])
16             + AK lifetime
17             If this FSM has only one authorization key, then
18             wmanIf2BsSsPkmLastAkExpireTime = the activation of FSM."
19        ::= { wmanIf2BsSsPkmAuthorizationEntry 7 }
20
21        wmanIf2BsSsPkmLatestAkExpireTime OBJECT-TYPE
22            SYNTAX      DateAndTime
23            MAX-ACCESS  read-only
24            STATUS      current
25            DESCRIPTION
26                "This object is the time when the latest AK expires."
27            ::= { wmanIf2BsSsPkmAuthorizationEntry 8 }
28
29        wmanIf2BsSsPkmCertificateStatus OBJECT-TYPE
30            SYNTAX      INTEGER {unknown (0),
31                            validSsChained (1),
32                            validSsTrusted (2),
33                            invalidSsUntrusted (3),
34                            invalidCAUntrusted (4),
35                            invalidSsOther (5),
36                            invalidCAOther (6)}
37            MAX-ACCESS  read-only
38            STATUS      current
39            DESCRIPTION
40                "Contains the reason why a SS's certificate is deemed valid
41                 or invalid.
42                 0 - return unknown if the SS is running PKM mode
43                 1 - means the certificate is valid because it chains to
44                    a valid certificate
45                 2 - means the certificate is valid because it has been
46                    provisioned to be trusted
47                 3 - means the certificate is invalid because it has been
48                    provisioned to be untrusted.
49                 4 - means the certificate is invalid because it chains to
50                    an untrusted certificate.
51                 5 - refer to errors in parsing, validity periods, etc, of
52                    SS certificate
53                 6 - refer to errors in parsing, validity periods, etc, of
54                    CA certificate"
55            ::= { wmanIf2BsSsPkmAuthorizationEntry 9 }
56
57        --
58        -- Table wmanIf2BsSsPkmSecurityCapabilityTable
59        --
60        wmanIf2BsSsPkmSecurityCapabilityTable OBJECT-TYPE
61            SYNTAX      SEQUENCE OF WmanIf2BsSsPkmSecurityCapabilityEntry
62            MAX-ACCESS  not-accessible
63            STATUS      current
64            DESCRIPTION

```

```

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

```

```

1           "Table 377, IEEE Std 802.16-2004"
2       ::= { wmanIf2BsSsPkmSecurityCapabilityEntry 4 }
3
4       --
5       -- Table wmanIf2BsSsPkmTekTable
6       --
7       wmanIf2BsSsPkmTekTable OBJECT-TYPE
8           SYNTAX      SEQUENCE OF WmanIf2BsSsPkmTekEntry
9           MAX-ACCESS  not-accessible
10          STATUS      current
11          DESCRIPTION
12              "This table contains the TEK attributes that are associated
13              with each SAID."
14          ::= { wmanIf2BsPkmV1Objects 5 }
15
16       wmanIf2BsSsPkmTekEntry OBJECT-TYPE
17          SYNTAX      WmanIf2BsSsPkmTekEntry
18          MAX-ACCESS  not-accessible
19          STATUS      current
20          DESCRIPTION
21              "This table is triple indexed by ifIndex,
22              wmanIf2BsSsMacAddress, and wmanIf2BsSsPkmSaidIndex."
23          INDEX       { ifIndex,
24                      wmanIf2BsSsMacAddress,
25                      wmanIf2BsSsPkmSaidIndex }
26          ::= { wmanIf2BsSsPkmTekTable 1 }
27
28       WmanIf2BsSsPkmTekEntry ::= SEQUENCE {
29           wmanIf2BsSsPkmSaidIndex          INTEGER,
30           wmanIf2BsSsPkmSaType            WmanIf2SaType,
31           wmanIf2BsSsPkmTekDataEncryptAlgorithm WmanIf2DataEncryptAlgId,
32           wmanIf2BsSsPkmTekDataAuthentAlgorithm WmanIf2DataAuthAlgId,
33           wmanIf2BsSsPkmTekEncryptAlgorithm WmanIf2TekEncryptAlgId,
34           wmanIf2BsSsPkmOlderTekSequenceNumber Integer32,
35           wmanIf2BsSsPkmOlderTekLifetime    Integer32,
36           wmanIf2BsSsPkmNewerTekSequenceNumber Integer32,
37           wmanIf2BsSsPkmNewerTekLifetime    Integer32,
38           wmanIf2BsSsPkmAuthInvalidError    WmanIf2AuthInvalidError,
39           wmanIf2BsSsPkmLastTekExpireTime   DateAndTime,
40           wmanIf2BsSsPkmLatestTekExpireTime DateAndTime}
41
42       wmanIf2BsSsPkmSaidIndex OBJECT-TYPE
43          SYNTAX      INTEGER (0 .. 65535)
44          MAX-ACCESS  not-accessible
45          STATUS      current
46          DESCRIPTION
47              "SAID index to the wmanIf2BsSsPkmTekTable."
48          ::= { wmanIf2BsSsPkmTekEntry 1 }
49
50       wmanIf2BsSsPkmSaType OBJECT-TYPE
51          SYNTAX      WmanIf2SaType
52          MAX-ACCESS  read-only
53          STATUS      current
54          DESCRIPTION
55              "SA Type attribute that is included in the Auth Reply
56              message."
57          ::= { wmanIf2BsSsPkmTekEntry 2 }
58
59       wmanIf2BsSsPkmTekDataEncryptAlgorithm OBJECT-TYPE
60          SYNTAX      WmanIf2DataEncryptAlgId
61          MAX-ACCESS  read-only
62          STATUS      current
63          DESCRIPTION
64              "The data encryption algorithm attribute that is included

```



```

1         in the Auth Reply message."
2     REFERENCE
3         "Table 375, IEEE Std 802.16-2004"
4     ::= { wmanIf2BsSsPkmTekEntry 3 }
5
6     wmanIf2BsSsPkmTekDataAuthentAlgorithm OBJECT-TYPE
7         SYNTAX      WmanIf2DataAuthAlgId
8         MAX-ACCESS  read-only
9         STATUS      current
10        DESCRIPTION
11            "The data authentication algorithm attribute that is
12            included in the Auth Reply message."
13        REFERENCE
14            "Table 376, IEEE Std 802.16-2004"
15        ::= { wmanIf2BsSsPkmTekEntry 4 }
16
17        wmanIf2BsSsPkmTekEncryptAlgorithm OBJECT-TYPE
18            SYNTAX      WmanIf2TekEncryptAlgId
19            MAX-ACCESS  read-only
20            STATUS      current
21            DESCRIPTION
22                "The TEK key encryption algorithm attribute that is
23                included in the Auth Reply message."
24            REFERENCE
25                "Table 377, IEEE Std 802.16-2004"
26            ::= { wmanIf2BsSsPkmTekEntry 5 }
27
28        wmanIf2BsSsPkmOlderTekSequenceNumber OBJECT-TYPE
29            SYNTAX      Integer32 (0 .. 3)
30            MAX-ACCESS  read-only
31            STATUS      current
32            DESCRIPTION
33                "At all times the BS maintains two sets of active
34                generations of keying material per SAID. One set
35                corresponds to the 'older' generation of keying material,
36                the second set corresponds to the 'newer' generation of
37                keying material. The newer generation has a key sequence
38                number one greater than (modulo 4) that of the older
39                generation. This object provides the older TEK sequence
40                number in the Key Reply message for an SS."
41            REFERENCE
42                "Subclause 11.9.8 in IEEE Std 802.16-2004"
43            ::= { wmanIf2BsSsPkmTekEntry 6 }
44
45        wmanIf2BsSsPkmOlderTekLifetime OBJECT-TYPE
46            SYNTAX      Integer32 (1800 .. 604800)
47            UNITS        "seconds"
48            MAX-ACCESS  read-only
49            STATUS      current
50            DESCRIPTION
51                "This object provides the older TEK Remaining Lifetime."
52            REFERENCE
53                "Subclause 11.9.8 in IEEE Std 802.16-2004"
54            ::= { wmanIf2BsSsPkmTekEntry 7 }
55
56        wmanIf2BsSsPkmNewerTekSequenceNumber OBJECT-TYPE
57            SYNTAX      Integer32 (0 .. 3)
58            MAX-ACCESS  read-only
59            STATUS      current
60            DESCRIPTION
61                "This object provides the newer TEK sequence
62                number in the Key Reply message for an SS."
63            REFERENCE
64                "Subclause 11.9.8 in IEEE Std 802.16-2004"

```

```

1         ::= { wmanIf2BsSsPkmTekEntry 8 }
2
3 wmanIf2BsSsPkmNewerTekLifetime OBJECT-TYPE
4     SYNTAX      Integer32 (1800 .. 604800)
5     UNITS       "seconds"
6     MAX-ACCESS  read-only
7     STATUS      current
8     DESCRIPTION
9         "This object provides the newer TEK Remaining Lifetime."
10    REFERENCE
11        "Subclause 11.9.8 in IEEE Std 802.16-2004"
12    ::= { wmanIf2BsSsPkmTekEntry 9 }
13
14 wmanIf2BsSsPkmAuthInvalidError OBJECT-TYPE
15     SYNTAX      WmanIf2AuthInvalidError
16     MAX-ACCESS  read-only
17     STATUS      current
18     DESCRIPTION
19         "BS returns Authorization Invalid message if an authorization
20         invlaid error is detected.
21
22         Note that the BS may log the Display-String attribute and
23         Authorization invalid error in wmanIfDevMib."
24     REFERENCE
25         "Subclause 11.9.10 in IEEE Std 802.16-2004"
26     ::= { wmanIf2BsSsPkmTekEntry 10 }
27
28 wmanIf2BsSsPkmLastTekExpireTime OBJECT-TYPE
29     SYNTAX      DateAndTime
30     MAX-ACCESS  read-only
31     STATUS      current
32     DESCRIPTION
33         "This object is the time when the last TEK expires.
34         wmanIf2BsSsPkmLastTekExpireTime = Time(last TEK[Key Reply])
35         + TEK lifetime
36         If this FSM has only one authorization key, then
37         wmanIf2BsSsPkmLastTekExpireTime = the activation of FSM."
38     ::= { wmanIf2BsSsPkmTekEntry 11 }
39
40 wmanIf2BsSsPkmLatestTekExpireTime OBJECT-TYPE
41     SYNTAX      DateAndTime
42     MAX-ACCESS  read-only
43     STATUS      current
44     DESCRIPTION
45         "This object is the time when the latest TEK expires."
46     ::= { wmanIf2BsSsPkmTekEntry 12 }
47

```

## 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:]

```

7 wmanIf2BsPkmV2Objects OBJECT IDENTIFIER ::= { wmanIf2BsPkmObjects 2 }
8
9 --
10 -- Table wmanIf2BsPkmV2ConfigTable
11 --
12 wmanIf2BsPkmV2ConfigTable OBJECT-TYPE
13     SYNTAX      SEQUENCE OF WmanIf2BsPkmV2ConfigEntry
14     MAX-ACCESS  not-accessible
15     STATUS      current
16     DESCRIPTION
17         "This table contains the configuration of the PKM
18         attributes that are needed to PKM operation."
19     REFERENCE
20         "Table 343 in IEEE Std 802.16-2004 and 802.16e-2005"
21     ::= { wmanIf2BsPkmV2Objects 1 }
22
23 wmanIf2BsPkmV2ConfigEntry OBJECT-TYPE
24     SYNTAX      WmanIf2BsPkmV2ConfigEntry
25     MAX-ACCESS  not-accessible
26     STATUS      current
27     DESCRIPTION
28         "Each entry contains objects that define the PKM attributes
29         of each BS. The table is indexed by ifIndex that is
30         associated with the BS sector."
31     INDEX      { ifIndex }
32     ::= { wmanIf2BsPkmV2ConfigTable 1 }
33
34 WmanIf2BsPkmV2ConfigEntry ::= SEQUENCE {
35     wmanIf2BsPkmPmkPrehandshakeLifetime      Integer32,
36     wmanIf2BsPkmPmkLifetime                  Integer32,
37     wmanIf2BsSaChallengeTimeout              Integer32,
38     wmanIf2BsMaxSaTekChallenge               Integer32,
39     wmanIf2BsSaTekTimeout                    Integer32,
40     wmanIf2BsMaxSaTekRequest                  Integer32}
41
42 wmanIf2BsPkmPmkPrehandshakeLifetime OBJECT-TYPE
43     SYNTAX      Integer32 (5 .. 900)
44     UNITS       "seconds"
45     MAX-ACCESS  read-write
46     STATUS      current
47     DESCRIPTION
48         "This object defines the PMK or PAK prehandshake lifetime."
49     REFERENCE
50         "Table 343 in IEEE Std 802.16e-2005"
51     DEFVAL     { 10 }
52     ::= { wmanIf2BsPkmV2ConfigEntry 1 }
53
54 wmanIf2BsPkmPmkLifetime OBJECT-TYPE
55     SYNTAX      Integer32 (60 .. 86400)
56     UNITS       "seconds"
57     MAX-ACCESS  read-write
58     STATUS      current
59     DESCRIPTION

```

```

1           "This object defines PMK lifetime, if MSK lifetime is
2           unspecified (i.e., by AAA server)."
```

REFERENCE

```

4           "Table 343 in IEEE Std 802.16e-2005"
5           DEFVAL          { 3600 }
6           ::= { wmanIf2BsPkmV2ConfigEntry 2 }
7
8 wmanIf2BsSaChallengeTimeout OBJECT-TYPE
9     SYNTAX      Integer32 (500 .. 2000)
10    UNITS       "milliseconds"
11    MAX-ACCESS  read-write
12    STATUS      current
13    DESCRIPTION
14      "This object defines the timeout value for SA-TEKChallenge
15      retransmission."
16    REFERENCE
17      "Table 343 in IEEE Std 802.16e-2005"
18    DEFVAL      { 1000 }
19    ::= { wmanIf2BsPkmV2ConfigEntry 3 }
20
21 wmanIf2BsMaxSaTekChallenge OBJECT-TYPE
22    SYNTAX      Integer32 (1 .. 3)
23    MAX-ACCESS  read-write
24    STATUS      current
25    DESCRIPTION
26      "This object defines the maximum number of SA-TEK-Challenge
27      transmissions."
28    REFERENCE
29      "Table 343 in IEEE Std 802.16e-2005"
30    DEFVAL      { 3 }
31    ::= { wmanIf2BsPkmV2ConfigEntry 4 }
32
33 wmanIf2BsSaTekTimeout OBJECT-TYPE
34    SYNTAX      Integer32 (100 .. 1000)
35    UNITS       "milliseconds"
36    MAX-ACCESS  read-write
37    STATUS      current
38    DESCRIPTION
39      "This object defines the timeout value for SA-TEKRequest
40      retransmission."
41    REFERENCE
42      "Table 343 in IEEE Std 802.16e-2005"
43    DEFVAL      { 300 }
44    ::= { wmanIf2BsPkmV2ConfigEntry 5 }
45
46 wmanIf2BsMaxSaTekRequest OBJECT-TYPE
47    SYNTAX      Integer32 (1 .. 3)
48    MAX-ACCESS  read-write
49    STATUS      current
50    DESCRIPTION
51      "This object defines the maximum number of SA-TEK-Request
52      retransmission."
53    REFERENCE
54      "Table 343 in IEEE Std 802.16e-2005"
55    DEFVAL      { 3 }
56    ::= { wmanIf2BsPkmV2ConfigEntry 6 }
57
58 --
59 -- Table wmanIf2BsSsPkmV2RsaAuthTable
60 --
61 wmanIf2BsSsPkmV2RsaAuthTable OBJECT-TYPE
62    SYNTAX      SEQUENCE OF WmanIf2BsSsPkmV2RsaAuthEntry
63    MAX-ACCESS  not-accessible
64    STATUS      current
```

```

1      DESCRIPTION
2          "This table contains information related to PKMV2
3          RSA based authorization process."
4      REFERENCE
5          "Subclause 6.3.2.3.9.11 in IEEE Std 802.16e-2005"
6          ::= { wmanIf2BsPkmV2Objects 2 }
7
8      wmanIf2BsSsPkmV2RsaAuthEntry OBJECT-TYPE
9          SYNTAX      WmanIf2BsSsPkmV2RsaAuthEntry
10         MAX-ACCESS  not-accessible
11         STATUS      current
12         DESCRIPTION
13             "Each entry contains objects that define the SS
14             authorization attributes for each SS associated with each
15             BS sector. The table is indexed by ifIndex and
16             wmanIf2BsSsMacAddress."
17         INDEX       { ifIndex, wmanIf2BsSsMacAddress }
18         ::= { wmanIf2BsSsPkmV2RsaAuthTable 1 }
19
20     WmanIf2BsSsPkmV2RsaAuthEntry ::= SEQUENCE {
21         wmanIf2BsSsPkmV2BsCertificate      OCTET STRING,
22         wmanIf2BsSsPkmV2SsCertificate      OCTET STRING,
23         wmanIf2BsSsPkmV2SaId              INTEGER,
24         wmanIf2BsSsPkmV2SsRandom          OCTET STRING,
25         wmanIf2BsSsPkmV2BsRandom          OCTET STRING,
26         wmanIf2BsSsPkmV2AuthKeySequenceNumber Integer32,
27         wmanIf2BsSsPkmV2AuthKeyLifetime   Integer32,
28         wmanIf2BsSsPkmV2AuthResult        INTEGER,
29         wmanIf2BsSsPkmV2AuthFailure       WmanIf2AuthFailureType,
30         wmanIf2BsSsPkmV2LastAkExpireTime  DateAndTime,
31         wmanIf2BsSsPkmV2LatestAkExpireTime DateAndTime,
32         wmanIf2BsSsPkmV2CertificateStatus  INTEGER}
33
34     wmanIf2BsSsPkmV2BsCertificate OBJECT-TYPE
35         SYNTAX      OCTET STRING (SIZE(0..65535))
36         MAX-ACCESS  read-only
37         STATUS      current
38         DESCRIPTION
39             "BS sends the BS-Certificate in the PKMV2 RSA-Reply message
40             for BS-SS mutual authentication. It is the DER-encoded
41             ASN.1 X.509 BS Certificate."
42         REFERENCE
43             "Subclause 11.9.24 in IEEE Std 802.16e-2005"
44         ::= { wmanIf2BsSsPkmV2RsaAuthEntry 1 }
45
46     wmanIf2BsSsPkmV2SsCertificate OBJECT-TYPE
47         SYNTAX      OCTET STRING (SIZE(0..65535))
48         MAX-ACCESS  read-only
49         STATUS      current
50         DESCRIPTION
51             "SS sends the SS-Certificate in the PKMV2 RSA-Request
52             message. It contains an X.509 SS certificate issued by the
53             SS's manufacturer. The SS's X.509 certificate is a
54             public-key certificate which binds the SS's identifying
55             information to its RSA public key in a verifiable manner.
56             The X.509 certificate is digitally signed by the SS's
57             manufacturer, and that signature can be verified by a BS
58             that knows the manufacturer's public key.
59             The manufacturer's public key is placed in an X.509
60             certification authority (CA) certificate, which in turn
61             is signed by a higher level CA."
62         REFERENCE
63             "Subclause 11.9.12 in IEEE Std 802.16-2004"
64         ::= { wmanIf2BsSsPkmV2RsaAuthEntry 2 }

```

```

1
2 wmanIf2BsSsPkmV2SaId OBJECT-TYPE
3     SYNTAX      INTEGER (0..65535)
4     MAX-ACCESS  read-only
5     STATUS      current
6     DESCRIPTION
7         "SS's primary SAID equal to the Basic CID. SS sends the SAID
8         in the PKMV2 RSA-Request message."
9     REFERENCE
10        "Subclause 6.3.2.3.9.2 in IEEE Std 802.16-2004"
11    ::= { wmanIf2BsSsPkmV2RsaAuthEntry 3 }
12
13 wmanIf2BsSsPkmV2SsRandom OBJECT-TYPE
14     SYNTAX      OCTET STRING (SIZE(8))
15     MAX-ACCESS  read-only
16     STATUS      current
17     DESCRIPTION
18         "This attribute contains a quantity that is pseudo random
19         number generated from the MS and used as fresh number for
20         mutual authorization message handshake. SS sends the SS-Random
21         in the PKMV2 RSA-Request message."
22     REFERENCE
23        "Subclause 11.9.21 in IEEE Std 802.16e-2005"
24    ::= { wmanIf2BsSsPkmV2RsaAuthEntry 4 }
25
26 wmanIf2BsSsPkmV2BsRandom OBJECT-TYPE
27     SYNTAX      OCTET STRING (SIZE(8))
28     MAX-ACCESS  read-only
29     STATUS      current
30     DESCRIPTION
31         "This attribute contains a quantity that is pseudo random
32         number generated from the BS and used as fresh number for
33         mutual authorization message handshake. BS sends the BS-Random
34         in the PKMV2 RSA-Reply message."
35     REFERENCE
36        "Subclause 11.9.22 in IEEE Std 802.16e-2005"
37    ::= { wmanIf2BsSsPkmV2RsaAuthEntry 5 }
38
39 wmanIf2BsSsPkmV2AuthKeySequenceNumber OBJECT-TYPE
40     SYNTAX      Integer32 (0 .. 15)
41     MAX-ACCESS  read-only
42     STATUS      current
43     DESCRIPTION
44         "This object provides the most recent authorization key
45         sequence number in the PKMV2 RSA-Reply message for an SS."
46     REFERENCE
47        "Subclause 11.9.5 in IEEE Std 802.16e-2005"
48    ::= { wmanIf2BsSsPkmV2RsaAuthEntry 6 }
49
50 wmanIf2BsSsPkmV2AuthKeyLifetime OBJECT-TYPE
51     SYNTAX      Integer32 (86400..6048000)
52     UNITS       "seconds"
53     MAX-ACCESS  read-only
54     STATUS      current
55     DESCRIPTION
56         "This object defines the lifetime of an authorization
57         key (AK) the BS assigns to a SS. BS sends the key lifetime
58         in the PKMV2 RSA-Reply message."
59     REFERENCE
60        "Subclause 11.9.4 in IEEE Std 802.16e-2005"
61    ::= { wmanIf2BsSsPkmV2RsaAuthEntry 7 }
62
63 wmanIf2BsSsPkmV2AuthResult OBJECT-TYPE
64     SYNTAX      INTEGER {success(0),

```

```

1           reject(1)}
2     MAX-ACCESS  read-only
3     STATUS      current
4     DESCRIPTION
5         "This attribute contains the result code of the RSA-based
6         authorization. SS sends the result code in PKMV2
7         RSA-Acknowledgement message."
8     REFERENCE
9         "Subclause 11.9.4 in IEEE Std 802.16e-2005"
10    ::= { wmanIf2BsSsPkmV2RsaAuthEntry 8 }
11
12 wmanIf2BsSsPkmV2AuthFailure OBJECT-TYPE
13     SYNTAX      WmanIf2AuthFailureType
14     MAX-ACCESS  read-only
15     STATUS      current
16     DESCRIPTION
17         "BS returns PKMV2 RSA-Rejects message if an authorization
18         failure is detected.
19
20         Failure type unknownManufactur(4)- ssBsIncompatibleSc(9) are
21         considered permanent authorization failure, since any
22         attempts of reauthorization would continue to result in
23         Authorization Rejects. Details about the cause of a
24         Permanent Authorization Failure may be reported to the SS
25         in an optional Display-String attribute that may accompany
26         the Error-Code attribute in Authorization Reject messages.
27
28         Note that the BS may log the Display-String attribute and
29         Authorization failures in wmanIfDevMib, and generate a trap
30         to an SNMP manager."
31     REFERENCE
32         "Subclause 11.9.10 in IEEE Std 802.16-2004"
33     ::= { wmanIf2BsSsPkmV2RsaAuthEntry 9 }
34
35 wmanIf2BsSsPkmV2LastAkExpireTime OBJECT-TYPE
36     SYNTAX      DateAndTime
37     MAX-ACCESS  read-only
38     STATUS      current
39     DESCRIPTION
40         "This object is the time when the last AK expires.
41         wmanIf2BsSsPkmV2LastAkExpireTime = Time(last AK[RSA-Reply])
42         + AK lifetime
43         If this FSM has only one authorization key, then
44         wmanIf2BsSsPkmV2LastAkExpireTime = the activation of FSM."
45     ::= { wmanIf2BsSsPkmV2RsaAuthEntry 10 }
46
47 wmanIf2BsSsPkmV2LatestAkExpireTime OBJECT-TYPE
48     SYNTAX      DateAndTime
49     MAX-ACCESS  read-only
50     STATUS      current
51     DESCRIPTION
52         "This object is the time when the latest AK expires."
53     ::= { wmanIf2BsSsPkmV2RsaAuthEntry 11 }
54
55 wmanIf2BsSsPkmV2CertificateStatus OBJECT-TYPE
56     SYNTAX      INTEGER {unknown (0),
57                     validSsChained (1),
58                     validSsTrusted (2),
59                     invalidSsUntrusted (3),
60                     invalidCAUntrusted (4),
61                     invalidSsOther (5),
62                     invalidCAOther (6)}
63     MAX-ACCESS  read-only
64     STATUS      current

```

```

1      DESCRIPTION
2          "Contains the reason why a SS's certificate is deemed valid
3          or invalid.
4          0 - return unknown if the SS is running PKM mode
5          1 - means the certificate is valid because it chains to
6          a valid certificate
7          2 - means the certificate is valid because it has been
8          provisioned to be trusted
9          3 - means the certificate is invalid because it has been
10         provisioned to be untrusted.
11         4 - means the certificate is invalid because it chains to
12         an untrusted certificate.
13         5 - refer to errors in parsing, validity periods, etc, of
14         SS certificate
15         6 - refer to errors in parsing, validity periods, etc, of
16         CA certificate"
17     ::= { wmanIf2BsSsPkmV2RsaAuthEntry 12 }
18
19     --
20     -- Table wmanIf2BsSsPkmV2TekTable
21     --
22     wmanIf2BsSsPkmV2TekTable OBJECT-TYPE
23         SYNTAX      SEQUENCE OF WmanIf2BsSsPkmV2TekEntry
24         MAX-ACCESS  not-accessible
25         STATUS      current
26         DESCRIPTION
27             "This table contains the TEK attributes that are associated
28             with each SAID."
29         ::= { wmanIf2BsPkmV2Objects 3 }
30
31     wmanIf2BsSsPkmV2TekEntry OBJECT-TYPE
32         SYNTAX      WmanIf2BsSsPkmV2TekEntry
33         MAX-ACCESS  not-accessible
34         STATUS      current
35         DESCRIPTION
36             "This table is triple indexed by ifIndex,
37             wmanIf2BsSsMacAddress, and wmanIf2BsSsPkmSaidIndex."
38         INDEX      { ifIndex,
39                     wmanIf2BsSsMacAddress,
40                     wmanIf2BsSsPkmV2SaidIndex }
41         ::= { wmanIf2BsSsPkmV2TekTable 1 }
42
43     WmanIf2BsSsPkmV2TekEntry ::= SEQUENCE {
44         wmanIf2BsSsPkmV2SaidIndex      INTEGER,
45         wmanIf2BsSsPkmV2SaType         WmanIf2SaType,
46         wmanIf2BsSsPkmV2OlderTekSequenceNumber Integer32,
47         wmanIf2BsSsPkmV2OlderTekLifetime Integer32,
48         wmanIf2BsSsPkmV2NewerTekSequenceNumber Integer32,
49         wmanIf2BsSsPkmV2NewerTekLifetime Integer32,
50         wmanIf2BsSsPkmV2AuthInvalidError WmanIf2AuthInvalidError,
51         wmanIf2BsSsPkmV2LastTekExpireTime DateAndTime,
52         wmanIf2BsSsPkmV2LatestTekExpireTime DateAndTime}
53
54     wmanIf2BsSsPkmV2SaidIndex OBJECT-TYPE
55         SYNTAX      INTEGER (0 .. 65535)
56         MAX-ACCESS  not-accessible
57         STATUS      current
58         DESCRIPTION
59             "SAID index to the wmanIf2BsSsPkmV2TekTable."
60         ::= { wmanIf2BsSsPkmV2TekEntry 1 }
61
62     wmanIf2BsSsPkmV2SaType OBJECT-TYPE
63         SYNTAX      WmanIf2SaType
64         MAX-ACCESS  read-only

```



```

1      STATUS      current
2      DESCRIPTION
3          "SA Type attribute that is included in the Auth Reply
4          message."
5      ::= { wmanIf2BsSsPkmV2TekEntry 2 }
6
7      wmanIf2BsSsPkmV2OlderTekSequenceNumber OBJECT-TYPE
8          SYNTAX      Integer32 (0 .. 3)
9          MAX-ACCESS  read-only
10         STATUS      current
11         DESCRIPTION
12             "At all times the BS maintains two sets of active
13             generations of keying material per SAID. One set
14             corresponds to the 'older' generation of keying material,
15             the second set corresponds to the 'newer' generation of
16             keying material. The newer generation has a key sequence
17             number one greater than (modulo 4) that of the older
18             generation. This object provides the older TEK sequence
19             number in the Key Reply message for an SS."
20         REFERENCE
21             "Subclause 11.9.8 in IEEE Std 802.16-2004"
22         ::= { wmanIf2BsSsPkmV2TekEntry 3 }
23
24         wmanIf2BsSsPkmV2OlderTekLifetime OBJECT-TYPE
25             SYNTAX      Integer32 (1800 .. 604800)
26             UNITS      "seconds"
27             MAX-ACCESS  read-only
28             STATUS      current
29             DESCRIPTION
30                 "This object provides the older TEK Remaining Lifetime."
31             REFERENCE
32                 "Subclause 11.9.8 in IEEE Std 802.16-2004"
33             ::= { wmanIf2BsSsPkmV2TekEntry 4 }
34
35         wmanIf2BsSsPkmV2NewerTekSequenceNumber OBJECT-TYPE
36             SYNTAX      Integer32 (0 .. 3)
37             MAX-ACCESS  read-only
38             STATUS      current
39             DESCRIPTION
40                 "This object provides the newer TEK sequence
41                 number in the Key Reply message for an SS."
42             REFERENCE
43                 "Subclause 11.9.8 in IEEE Std 802.16-2004"
44             ::= { wmanIf2BsSsPkmV2TekEntry 5 }
45
46         wmanIf2BsSsPkmV2NewerTekLifetime OBJECT-TYPE
47             SYNTAX      Integer32 (1800 .. 604800)
48             UNITS      "seconds"
49             MAX-ACCESS  read-only
50             STATUS      current
51             DESCRIPTION
52                 "This object provides the newer TEK Remaining Lifetime."
53             REFERENCE
54                 "Subclause 11.9.8 in IEEE Std 802.16-2004"
55             ::= { wmanIf2BsSsPkmV2TekEntry 6 }
56
57         wmanIf2BsSsPkmV2AuthInvalidError OBJECT-TYPE
58             SYNTAX      WmanIf2AuthInvalidError
59             MAX-ACCESS  read-only
60             STATUS      current
61             DESCRIPTION
62                 "BS returns Authorization Invalid message if an authorization
63                 invlaid error is detected.
64

```

```
1           Note that the BS may log the Display-String attribute and
2           Authorization invalid error in wmanIfDevMib."
3 REFERENCE
4           "Subclause 11.9.10 in IEEE Std 802.16-2004"
5 ::= { wmanIf2BsSsPkmV2TekEntry 7 }
6
7 wmanIf2BsSsPkmV2LastTekExpireTime OBJECT-TYPE
8     SYNTAX      DateAndTime
9     MAX-ACCESS  read-only
10    STATUS      current
11    DESCRIPTION
12       "This object is the time when the last TEK expires.
13         wmanIf2BsSsPkmV2LastTekExpireTime = Time(last TEK[Key Reply])
14                                           + TEK lifetime
15         If this FSM has only one authorization key, then
16         wmanIf2BsSsPkmV2LastTekExpireTime = the activation of FSM."
17 ::= { wmanIf2BsSsPkmV2TekEntry 8 }
18
19 wmanIf2BsSsPkmV2LatestTekExpireTime OBJECT-TYPE
20     SYNTAX      DateAndTime
21     MAX-ACCESS  read-only
22     STATUS      current
23     DESCRIPTION
24       "This object is the time when the latest TEK expires."
25 ::= { wmanIf2BsSsPkmV2TekEntry 9 }
26
27
```

## 1 2.5 wmanIf2SsPkmObjects ASN.1 Code Change

### 2 13.2 ASN.1 Definitions of MIB Modules

#### 3 13.2.3 wmanIf2Mib

4 [\[Change wmanIf2SsPkmObjects to the following in WMAN-IF2-MIB:\]](#)

```

5
6 --
7 -- Subscriber station PKM group
8 -- wmanIf2SsPkmObjects contain the Subscriber Station Privacy Sublayer
9 -- objects
10 --
11 wmanIf2SsPkmObjects OBJECT IDENTIFIER ::= { wmanIf2SsObjects 2 }
12
13 wmanIf2SsPkmV1Objects OBJECT IDENTIFIER ::= { wmanIf2SsPkmObjects 1 }
14
15 --
16 -- Table wmanIf2SsPkmConfigTable
17 --
18 wmanIf2SsPkmConfigTable OBJECT-TYPE
19     SYNTAX          SEQUENCE OF WmanIf2SsPkmConfigEntry
20     MAX-ACCESS     not-accessible
21     STATUS          current
22     DESCRIPTION
23         "This table provides the configuration of the PKM
24         attributes that are needed to PKM operation."
25     REFERENCE
26         "Table 343 in IEEE Std 802.16-2004 and 802.16e-2005"
27     ::= { wmanIf2SsPkmV1Objects 1 }
28
29 wmanIf2SsPkmConfigEntry OBJECT-TYPE
30     SYNTAX          WmanIf2SsPkmConfigEntry
31     MAX-ACCESS     not-accessible
32     STATUS          current
33     DESCRIPTION
34         "The table is indexed by ifIndex."
35     INDEX           { ifIndex }
36     ::= { wmanIf2SsPkmConfigTable 1 }
37
38 WmanIf2SsPkmConfigEntry ::= SEQUENCE {
39     wmanIf2SsPkmAuthWaitTimeout          Integer32,
40     wmanIf2SsPkmReauthWaitTimeout       Integer32,
41     wmanIf2SsPkmAuthGraceTime           Integer32,
42     wmanIf2SsPkmOpWaitTimeout           Integer32,
43     wmanIf2SsPkmRekeyWaitTimeout        Integer32,
44     wmanIf2SsPkmTekGraceTime             Integer32,
45     wmanIf2SsPkmAuthRejectWaitTimeout   Integer32}
46
47 wmanIf2SsPkmAuthWaitTimeout OBJECT-TYPE
48     SYNTAX          Integer32 (2 .. 30)
49     UNITS           "seconds"
50     MAX-ACCESS     read-only
51     STATUS          current
52     DESCRIPTION
53         "This object defines the Auth Req retransmission interval
54         from Auth Wait state."
55     REFERENCE
56         "Table 343 and subclause 11.9.19 in IEEE Std 802.16-2004"
57     DEFVAL         { 10 }
58     ::= { wmanIf2SsPkmConfigEntry 1 }
59

```

```

1  wmanIf2SsPkmReauthWaitTimeout OBJECT-TYPE
2      SYNTAX      Integer32 (2 .. 30)
3      UNITS       "seconds"
4      MAX-ACCESS  read-only
5      STATUS      current
6      DESCRIPTION
7          "This object defines the Auth Req retransmission interval
8              from Reauth Wait state."
9      REFERENCE
10         "Table 343 and subclause 11.9.19 in IEEE Std 802.16-2004"
11     DEFVAL      { 10 }
12     ::= { wmanIf2SsPkmConfigEntry 2 }
13
14  wmanIf2SsPkmAuthGraceTime OBJECT-TYPE
15      SYNTAX      Integer32 (300 .. 3024000)
16      UNITS       "seconds"
17      MAX-ACCESS  read-only
18      STATUS      current
19      DESCRIPTION
20         "The value of this object is the grace time for an
21             authorization key. A SS is expected to start trying to get
22             a new authorization key beginning AuthGraceTime seconds
23             before the authorization key actually expires."
24     REFERENCE
25         "Table 343 and subclause 11.9.19 in IEEE Std 802.16-2004"
26     DEFVAL      { 600 }
27     ::= { wmanIf2SsPkmConfigEntry 3 }
28
29  wmanIf2SsPkmOpWaitTimeout OBJECT-TYPE
30      SYNTAX      Integer32 (1 .. 10)
31      UNITS       "seconds"
32      MAX-ACCESS  read-only
33      STATUS      current
34      DESCRIPTION
35         "This object defines the Key Req retransmission interval
36             from Op Wait state."
37     REFERENCE
38         "Table 343 and subclause 11.9.19 in IEEE Std 802.16-2004"
39     DEFVAL      { 1 }
40     ::= { wmanIf2SsPkmConfigEntry 4 }
41
42  wmanIf2SsPkmRekeyWaitTimeout OBJECT-TYPE
43      SYNTAX      Integer32 (1 .. 10)
44      UNITS       "seconds"
45      MAX-ACCESS  read-only
46      STATUS      current
47      DESCRIPTION
48         "This object defines the Key Req retransmission interval
49             from Rekey Wait state."
50     REFERENCE
51         "Table 343 and subclause 11.9.19 in IEEE Std 802.16-2004"
52     DEFVAL      { 1 }
53     ::= { wmanIf2SsPkmConfigEntry 5 }
54
55  wmanIf2SsPkmTekGraceTime OBJECT-TYPE
56      SYNTAX      Integer32 (300 .. 3024000)
57      UNITS       "seconds"
58      MAX-ACCESS  read-only
59      STATUS      current
60      DESCRIPTION
61         "The value of this object is the grace time for the TEK in
62             seconds. The SS is expected to start trying to acquire a
63             new TEK beginning TEK GraceTime seconds before the
64             expiration of the most recent TEK."

```

```

1      REFERENCE
2          "Table 343 and subclause 11.9.19 in IEEE Std 802.16-2004"
3      DEFVAL      { 3600 }
4      ::= { wmanIf2SsPkmConfigEntry 6 }
5
6      wmanIf2SsPkmAuthRejectWaitTimeout OBJECT-TYPE
7          SYNTAX      Integer32 (10 .. 600)
8          UNITS        "seconds"
9          MAX-ACCESS  read-only
10         STATUS      current
11         DESCRIPTION
12             "This object defines the Delay before resending Auth Request
13             after receiving Auth Reject."
14         REFERENCE
15             "Table 343 and subclause 11.9.19 in IEEE Std 802.16-2004"
16         DEFVAL      { 60 }
17         ::= { wmanIf2SsPkmConfigEntry 7 }
18
19     --
20     -- Table wmanIf2SsPkmAuthorizationTable
21     --
22     wmanIf2SsPkmAuthorizationTable OBJECT-TYPE
23         SYNTAX      SEQUENCE OF WmanIf2SsPkmAuthorizationEntry
24         MAX-ACCESS  not-accessible
25         STATUS      current
26         DESCRIPTION
27             "This table contains information that are related to SS's
28             authorization process."
29         REFERENCE
30             "Table 28 and 37 in IEEE Std 802.16-2004"
31         ::= { wmanIf2SsPkmV1Objects 2 }
32
33     wmanIf2SsPkmAuthorizationEntry OBJECT-TYPE
34         SYNTAX      WmanIf2SsPkmAuthorizationEntry
35         MAX-ACCESS  not-accessible
36         STATUS      current
37         DESCRIPTION
38             "This table is indexed by ifIndex"
39         INDEX      { ifIndex }
40         ::= { wmanIf2SsPkmAuthorizationTable 1 }
41
42     WmanIf2SsPkmAuthorizationEntry ::= SEQUENCE {
43         wmanIf2SsPkmCaCertificate      OCTET STRING,
44         wmanIf2SsPkmSsCertificate      OCTET STRING,
45         wmanIf2SsPkmSaId               INTEGER,
46         wmanIf2SsPkmAuthKeySequenceNumber Integer32,
47         wmanIf2SsPkmAuthKeyLifetime    Integer32,
48         wmanIf2SsPkmAuthFailure        WmanIf2AuthFailureType,
49         wmanIf2SsPkmLastAkExpireTime   DateAndTime,
50         wmanIf2SsPkmLatestAkExpireTime DateAndTime}
51
52     wmanIf2SsPkmCaCertificate OBJECT-TYPE
53         SYNTAX      OCTET STRING (SIZE(0..65535))
54         MAX-ACCESS  read-only
55         STATUS      current
56         DESCRIPTION
57             "SS sends the CA-Certificate in the Auth Info message. It
58             contains an X.509 CA certificate for the manufacturer of
59             the SS. The SS's X.509 user certificate shall have been
60             issued by the CA identified by the X.509 CA certificate."
61         REFERENCE
62             "Table 37 in IEEE Std 802.16-2004"
63         ::= { wmanIf2SsPkmAuthorizationEntry 1 }
64

```

```

1  wmanIf2SsPkmSsCertificate OBJECT-TYPE
2      SYNTAX          OCTET STRING (SIZE(0..65535))
3      MAX-ACCESS      read-only
4      STATUS          current
5      DESCRIPTION
6          "SS sends the SS-Certificate in the Auth Request message.
7          It contains an X.509 SS certificate issued by the SS's
8          manufacturer. The SS's X.509 certificate is a public-key
9          certificate which binds the SS's identifying information
10         to its RSA public key in a verifiable manner. The X.509
11         certificate is digitally signed by the SS's manufacturer,
12         and that signature can be verified by a BS that knows
13         the manufacturer's public key. The manufacturer's public
14         key is placed in an X.509 certification authority (CA)
15         certificate, which in turn is signed by a higher level CA."
16     REFERENCE
17         "Table 28 in IEEE Std 802.16-2004"
18     ::= { wmanIf2SsPkmAuthorizationEntry 2 }
19
20  wmanIf2SsPkmSaId OBJECT-TYPE
21      SYNTAX          INTEGER (0..65535)
22      MAX-ACCESS      read-only
23      STATUS          current
24      DESCRIPTION
25          "SS's primary SAID equal to the Basic CID."
26     REFERENCE
27         "Subclause 6.3.2.3.9.2 in IEEE Std 802.16-2004"
28     ::= { wmanIf2SsPkmAuthorizationEntry 3 }
29
30  wmanIf2SsPkmAuthKeySequenceNumber OBJECT-TYPE
31      SYNTAX          Integer32 (0 .. 15)
32      MAX-ACCESS      read-only
33      STATUS          current
34      DESCRIPTION
35          "This object provides the most recent authorization key
36          sequence number in the Auth Reply message for an SS."
37     REFERENCE
38         "Table 29 in IEEE Std 802.16-2004"
39     ::= { wmanIf2SsPkmAuthorizationEntry 4 }
40
41  wmanIf2SsPkmAuthKeyLifetime OBJECT-TYPE
42      SYNTAX          Integer32 (86400..6048000)
43      UNITS           "seconds"
44      MAX-ACCESS      read-only
45      STATUS          current
46      DESCRIPTION
47          "This object defines the lifetime of an authorization
48          key (AK) the BS assigns to a SS."
49     REFERENCE
50         "Table 343 in IEEE Std 802.16-2004"
51     ::= { wmanIf2SsPkmAuthorizationEntry 5 }
52
53  wmanIf2SsPkmAuthFailure OBJECT-TYPE
54      SYNTAX          WmanIf2AuthFailureType
55      MAX-ACCESS      read-only
56      STATUS          current
57      DESCRIPTION
58          "BS returns Authorization Rejects message if an authorization
59          failure is detected.
60
61          Failure type unknownManufactur(4) - ssBsIncompatibleSc(9) are
62          considered permanent authorization failure, since any
63          attempts of reauthorization would continue to result in
64          Authorization Rejects. Details about the cause of a

```

```

1           Permanent Authorization Failure may be reported to the SS
2           in an optional Display-String attribute that may accompany
3           the Error-Code attribute in Authorization Reject messages."
4 REFERENCE
5           "Subclause 11.9.10 in IEEE Std 802.16-2004"
6 ::= { wmanIf2SsPkmAuthorizationEntry 6 }
7
8 wmanIf2SsPkmLastAkExpireTime OBJECT-TYPE
9     SYNTAX      DateAndTime
10    MAX-ACCESS  read-only
11    STATUS      current
12    DESCRIPTION
13       "This object is the time when the last AK expires.
14       wmanIf2SsPkmLastAkExpireTime = Time(last AK[Auth Reply])
15       + AK lifetime
16       If this FSM has only one authorization key, then
17       wmanIf2SsPkmLastAkExpireTime = the activation of FSM."
18 ::= { wmanIf2SsPkmAuthorizationEntry 7 }
19
20 wmanIf2SsPkmLatestAkExpireTime OBJECT-TYPE
21     SYNTAX      DateAndTime
22     MAX-ACCESS  read-only
23     STATUS      current
24     DESCRIPTION
25       "This object is the time when the latest AK expires."
26 ::= { wmanIf2SsPkmAuthorizationEntry 8 }
27
28 --
29 -- Table wmanIf2SsPkmSecurityCapabilityTable
30 --
31 wmanIf2SsPkmSecurityCapabilityTable OBJECT-TYPE
32     SYNTAX      SEQUENCE OF WmanIf2SsPkmSecurityCapabilityEntry
33     MAX-ACCESS  not-accessible
34     STATUS      current
35     DESCRIPTION
36       "This table contains the SS's Security Capabilities that are
37       conveyed by the Auth Request message. It contains the list
38       of the cryptographic suite(s) an SS supports."
39     REFERENCE
40       "Subclause 11.9.13 in IEEE Std 802.16-2004"
41 ::= { wmanIf2SsPkmV1Objects 3 }
42
43 wmanIf2SsPkmSecurityCapabilityEntry OBJECT-TYPE
44     SYNTAX      WmanIf2SsPkmSecurityCapabilityEntry
45     MAX-ACCESS  not-accessible
46     STATUS      current
47     DESCRIPTION
48       "This table is indexed by wmanIf2SsSecurityCapIndex."
49     INDEX      { wmanIf2SsPkmSecurityCapIndex }
50 ::= { wmanIf2SsPkmSecurityCapabilityTable 1 }
51
52 WmanIf2SsPkmSecurityCapabilityEntry ::= SEQUENCE {
53     wmanIf2SsPkmSecurityCapIndex      INTEGER,
54     wmanIf2SsPkmScDataEncryptAlgorithm WmanIf2DataEncryptAlgId,
55     wmanIf2SsPkmScDataAuthentAlgorithm WmanIf2DataAuthAlgId,
56     wmanIf2SsPkmScEncryptAlgorithm    WmanIf2TekEncryptAlgId}
57
58 wmanIf2SsPkmSecurityCapIndex OBJECT-TYPE
59     SYNTAX      INTEGER (1 .. 65535)
60     MAX-ACCESS  not-accessible
61     STATUS      current
62     DESCRIPTION
63       "The index value which uniquely identifies an entry
64       in the wmanIf2SsPkmSecurityCapabilityTable"

```

```

1      ::= { wmanIf2SsPkmSecurityCapabilityEntry 1 }
2
3      wmanIf2SsPkmScDataEncryptAlgorithm OBJECT-TYPE
4          SYNTAX      WmanIf2DataEncryptAlgId
5          MAX-ACCESS  read-only
6          STATUS      current
7          DESCRIPTION
8              "The value of this object is the data encryption algorithm
9              being utilized."
10         REFERENCE
11             "Table 375, IEEE Std 802.16-2004"
12         ::= { wmanIf2SsPkmSecurityCapabilityEntry 2 }
13
14         wmanIf2SsPkmScDataAuthentAlgorithm OBJECT-TYPE
15             SYNTAX      WmanIf2DataAuthAlgId
16             MAX-ACCESS  read-only
17             STATUS      current
18             DESCRIPTION
19                 "The value of this object is the data authentication
20                 algorithm being utilized."
21             REFERENCE
22                 "Table 376, IEEE Std 802.16-2004"
23             ::= { wmanIf2SsPkmSecurityCapabilityEntry 3 }
24
25         wmanIf2SsPkmScEncryptAlgorithm OBJECT-TYPE
26             SYNTAX      WmanIf2TekEncryptAlgId
27             MAX-ACCESS  read-only
28             STATUS      current
29             DESCRIPTION
30                 "The value of this object is the TEK key encryption
31                 algorithm being utilized."
32             REFERENCE
33                 "Table 377, IEEE Std 802.16-2004"
34             ::= { wmanIf2SsPkmSecurityCapabilityEntry 4 }
35
36         --
37         -- Table wmanIf2SsPkmTekTable
38         --
39         wmanIf2SsPkmTekTable OBJECT-TYPE
40             SYNTAX      SEQUENCE OF WmanIf2SsPkmTekEntry
41             MAX-ACCESS  not-accessible
42             STATUS      current
43             DESCRIPTION
44                 "This table contains the TEK attributes that are associated
45                 with each SAID."
46             ::= { wmanIf2SsPkmV1Objects 4 }
47
48         wmanIf2SsPkmTekEntry OBJECT-TYPE
49             SYNTAX      WmanIf2SsPkmTekEntry
50             MAX-ACCESS  not-accessible
51             STATUS      current
52             DESCRIPTION
53                 "This table is double indexed by ifIndex and
54                 wmanIf2SsSaidIndex."
55             INDEX      { ifIndex, wmanIf2SsPkmSaidIndex }
56             ::= { wmanIf2SsPkmTekTable 1 }
57
58         WmanIf2SsPkmTekEntry ::= SEQUENCE {
59             wmanIf2SsPkmSaidIndex          INTEGER,
60             wmanIf2SsPkmSaType             WmanIf2SaType,
61             wmanIf2SsPkmTekDataEncryptAlgorithm WmanIf2DataEncryptAlgId,
62             wmanIf2SsPkmTekDataAuthentAlgorithm WmanIf2DataAuthAlgId,
63             wmanIf2SsPkmTekEncryptAlgorithm WmanIf2TekEncryptAlgId,
64             wmanIf2SsPkmOlderTekSequenceNumber Integer32,

```



```

1          wmanIf2SsPkmOlderTekLifetime                Integer32,
2          wmanIf2SsPkmNewerTekSequenceNumber          Integer32,
3          wmanIf2SsPkmNewerTekLifetime                Integer32,
4          wmanIf2SsPkmAuthInvalidError                WmanIf2AuthInvalidError,
5          wmanIf2SsPkmLastTekExpireTime                DateAndTime,
6          wmanIf2SsPkmLatestTekExpireTime              DateAndTime,
7          wmanIf2SsPkmTekState                          WmanIf2TekState}
8
9  wmanIf2SsPkmSaIdIndex OBJECT-TYPE
10     SYNTAX      INTEGER (0 .. 65535)
11     MAX-ACCESS  not-accessible
12     STATUS      current
13     DESCRIPTION
14         "SAID index to the wmanIf2SsPkmSaDescriptorTable."
15     ::= { wmanIf2SsPkmTekEntry 1 }
16
17  wmanIf2SsPkmSaType OBJECT-TYPE
18     SYNTAX      WmanIf2SaType
19     MAX-ACCESS  read-only
20     STATUS      current
21     DESCRIPTION
22         "SA Type attribute that is included in the Auth Reply
23         message."
24     ::= { wmanIf2SsPkmTekEntry 2 }
25
26  wmanIf2SsPkmTekDataEncryptAlgorithm OBJECT-TYPE
27     SYNTAX      WmanIf2DataEncryptAlgId
28     MAX-ACCESS  read-only
29     STATUS      current
30     DESCRIPTION
31         "The data encryption algorithm attribute that is included
32         in the Auth Reply message."
33     REFERENCE
34         "Table 375, IEEE Std 802.16-2004"
35     ::= { wmanIf2SsPkmTekEntry 3 }
36
37  wmanIf2SsPkmTekDataAuthentAlgorithm OBJECT-TYPE
38     SYNTAX      WmanIf2DataAuthAlgId
39     MAX-ACCESS  read-only
40     STATUS      current
41     DESCRIPTION
42         "The data authentication algorithm attribute that is
43         included in the Auth Reply message."
44     REFERENCE
45         "Table 376, IEEE Std 802.16-2004"
46     ::= { wmanIf2SsPkmTekEntry 4 }
47
48  wmanIf2SsPkmTekEncryptAlgorithm OBJECT-TYPE
49     SYNTAX      WmanIf2TekEncryptAlgId
50     MAX-ACCESS  read-only
51     STATUS      current
52     DESCRIPTION
53         "The TEK key encryption algorithm attribute that is
54         included in the Auth Reply message."
55     REFERENCE
56         "Table 377, IEEE Std 802.16-2004"
57     ::= { wmanIf2SsPkmTekEntry 5 }
58
59  wmanIf2SsPkmOlderTekSequenceNumber OBJECT-TYPE
60     SYNTAX      Integer32 (0 .. 3)
61     MAX-ACCESS  read-only
62     STATUS      current
63     DESCRIPTION
64         "At all times the BS maintains two sets of active

```

```

1         generations of keying material per SAID. One set
2         corresponds to the 'older' generation of keying material,
3         the second set corresponds to the 'newer' generation of
4         keying material. The newer generation has a key sequence
5         number one greater than (modulo 4) that of the older
6         generation. This object provides the older TEK sequence
7         number in the Key Reply message for an SS."
8     REFERENCE
9         "Subclause 11.9.8 in IEEE Std 802.16-2004"
10    ::= { wmanIf2SsPkmTekEntry 6 }
11
12    wmanIf2SsPkmOlderTekLifetime OBJECT-TYPE
13        SYNTAX      Integer32 (1800 .. 604800)
14        UNITS       "seconds"
15        MAX-ACCESS  read-only
16        STATUS      current
17        DESCRIPTION
18            "This object provides the older TEK Remaining Lifetime."
19        REFERENCE
20            "Subclause 11.9.8 in IEEE Std 802.16-2004"
21    ::= { wmanIf2SsPkmTekEntry 7 }
22
23    wmanIf2SsPkmNewerTekSequenceNumber OBJECT-TYPE
24        SYNTAX      Integer32 (0 .. 3)
25        MAX-ACCESS  read-only
26        STATUS      current
27        DESCRIPTION
28            "This object provides the newer TEK sequence
29            number in the Key Reply message for an SS."
30        REFERENCE
31            "Subclause 11.9.8 in IEEE Std 802.16-2004"
32    ::= { wmanIf2SsPkmTekEntry 8 }
33
34    wmanIf2SsPkmNewerTekLifetime OBJECT-TYPE
35        SYNTAX      Integer32 (1800 .. 604800)
36        UNITS       "seconds"
37        MAX-ACCESS  read-only
38        STATUS      current
39        DESCRIPTION
40            "This object provides the newer TEK Remaining Lifetime."
41        REFERENCE
42            "Subclause 11.9.8 in IEEE Std 802.16-2004"
43    ::= { wmanIf2SsPkmTekEntry 9 }
44
45    wmanIf2SsPkmAuthInvalidError OBJECT-TYPE
46        SYNTAX      WmanIf2AuthInvalidError
47        MAX-ACCESS  read-only
48        STATUS      current
49        DESCRIPTION
50            "BS returns Authorization Invalid message if an authorization
51            invlaid error is detected."
52        REFERENCE
53            "Subclause 11.9.10 in IEEE Std 802.16-2004"
54    ::= { wmanIf2SsPkmTekEntry 10 }
55
56    wmanIf2SsPkmLastTekExpireTime OBJECT-TYPE
57        SYNTAX      DateAndTime
58        MAX-ACCESS  read-only
59        STATUS      current
60        DESCRIPTION
61            "This object is the time when the last TEK expires.
62            wmanIf2SsPkmLastTekExpireTime = Time(last TEK[Key Reply])
63            + TEK lifetime
64            If this FSM has only one authorization key, then

```

```
1           wmanIf2SsPkmLastTekExpireTime = the activation of FSM."
2       ::= { wmanIf2SsPkmTekEntry 11 }
3
4 wmanIf2SsPkmLatestTekExpireTime OBJECT-TYPE
5     SYNTAX      DateAndTime
6     MAX-ACCESS  read-only
7     STATUS      current
8     DESCRIPTION
9         "This object is the time when the latest TEK expires."
10    ::= { wmanIf2SsPkmTekEntry 12 }
11
12 wmanIf2SsPkmTekState OBJECT-TYPE
13     SYNTAX      WmanIf2TekState
14     MAX-ACCESS  read-only
15     STATUS      current
16     DESCRIPTION
17         "The value of this object is the state of the indicated TEK
18         FSM. The start(1) state indicates that FSM is in its
19         initial state."
20    ::= { wmanIf2SsPkmTekEntry 13 }
21
```

## 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:]

```

7 wmanIf2SsPkmV2Objects OBJECT IDENTIFIER ::= { wmanIf2SsPkmObjects 2 }
8
9 --
10 -- Table wmanIf2SsPkmV2ConfigTable
11 --
12 wmanIf2SsPkmV2ConfigTable OBJECT-TYPE
13     SYNTAX      SEQUENCE OF WmanIf2SsPkmV2ConfigEntry
14     MAX-ACCESS  not-accessible
15     STATUS      current
16     DESCRIPTION
17         "This table contains the configuration of the PKM
18         attributes that are needed to PKM operation."
19     REFERENCE
20         "Table 343 in IEEE Std 802.16-2004 and 802.16e-2005"
21     ::= { wmanIf2SsPkmV2Objects 1 }
22
23 wmanIf2SsPkmV2ConfigEntry OBJECT-TYPE
24     SYNTAX      WmanIf2SsPkmV2ConfigEntry
25     MAX-ACCESS  not-accessible
26     STATUS      current
27     DESCRIPTION
28         "Each entry contains objects that define the PKM attributes
29         of each BS and SS. The table is indexed by ifIndex that is
30         associated with the SS."
31     INDEX       { ifIndex }
32     ::= { wmanIf2SsPkmV2ConfigTable 1 }
33
34 WmanIf2SsPkmV2ConfigEntry ::= SEQUENCE {
35     wmanIf2SsPkmPmkPrehandshakeLifetime      Integer32,
36     wmanIf2SsPkmPmkLifetime                  Integer32,
37     wmanIf2SsSaChallengeTimeout              Integer32,
38     wmanIf2SsMaxSaTekChallenge               Integer32,
39     wmanIf2SsSaTekTimeout                    Integer32,
40     wmanIf2SsMaxSaTekRequest                 Integer32}
41
42 wmanIf2SsPkmPmkPrehandshakeLifetime OBJECT-TYPE
43     SYNTAX      Integer32 (5 .. 900)
44     UNITS       "seconds"
45     MAX-ACCESS  read-only
46     STATUS      current
47     DESCRIPTION
48         "This object defines the PMK or PAK prehandshake lifetime."
49     REFERENCE
50         "Table 343 in IEEE Std 802.16e-2005"
51     DEFVAL     { 10 }
52     ::= { wmanIf2SsPkmV2ConfigEntry 1 }
53
54 wmanIf2SsPkmPmkLifetime OBJECT-TYPE
55     SYNTAX      Integer32 (60 .. 86400)
56     UNITS       "seconds"
57     MAX-ACCESS  read-only
58     STATUS      current
59     DESCRIPTION

```

```

1           "This object defines PMK lifetime, if MSK lifetime is
2           unspecified (i.e., by AAA server)."
```

REFERENCE

```

4           "Table 343 in IEEE Std 802.16e-2005"
5           DEFVAL          { 3600 }
6           ::= { wmanIf2SsPkmV2ConfigEntry 2 }
7
8 wmanIf2SsSaChallengeTimeout OBJECT-TYPE
9     SYNTAX          Integer32 (500 .. 2000)
10    UNITS           "milliseconds"
11    MAX-ACCESS      read-only
12    STATUS          current
13    DESCRIPTION
14      "This object defines the timeout value for SA-TEKChallenge
15      retransmission."
16    REFERENCE
17      "Table 343 in IEEE Std 802.16e-2005"
18    DEFVAL          { 1000 }
19    ::= { wmanIf2SsPkmV2ConfigEntry 3 }
20
21 wmanIf2SsMaxSaTekChallenge OBJECT-TYPE
22    SYNTAX          Integer32 (1 .. 3)
23    MAX-ACCESS      read-only
24    STATUS          current
25    DESCRIPTION
26      "This object defines the maximum number of SA-TEK-Challenge
27      transmissions."
28    REFERENCE
29      "Table 343 in IEEE Std 802.16e-2005"
30    DEFVAL          { 3 }
31    ::= { wmanIf2SsPkmV2ConfigEntry 4 }
32
33 wmanIf2SsSaTekTimeout OBJECT-TYPE
34    SYNTAX          Integer32 (100 .. 1000)
35    UNITS           "milliseconds"
36    MAX-ACCESS      read-only
37    STATUS          current
38    DESCRIPTION
39      "This object defines the timeout value for SA-TEKRequest
40      retransmission."
41    REFERENCE
42      "Table 343 in IEEE Std 802.16e-2005"
43    DEFVAL          { 300 }
44    ::= { wmanIf2SsPkmV2ConfigEntry 5 }
45
46 wmanIf2SsMaxSaTekRequest OBJECT-TYPE
47    SYNTAX          Integer32 (1 .. 3)
48    MAX-ACCESS      read-only
49    STATUS          current
50    DESCRIPTION
51      "This object defines the maximum number of SA-TEK-Request
52      retransmission."
53    REFERENCE
54      "Table 343 in IEEE Std 802.16e-2005"
55    DEFVAL          { 3 }
56    ::= { wmanIf2SsPkmV2ConfigEntry 6 }
57
58 --
59 -- Table wmanIf2SsPkmV2RsaAuthTable
60 --
61 wmanIf2SsPkmV2RsaAuthTable OBJECT-TYPE
62    SYNTAX          SEQUENCE OF WmanIf2SsPkmV2RsaAuthEntry
63    MAX-ACCESS      not-accessible
64    STATUS          current
```

```

1      DESCRIPTION
2          "This table contains information related to PKMV2
3          RSA based authorization process."
4      REFERENCE
5          "Subclause 6.3.2.3.9.11 in IEEE Std 802.16e-2005"
6          ::= { wmanIf2SsPkmV2Objects 2 }
7
8      wmanIf2SsPkmV2RsaAuthEntry OBJECT-TYPE
9          SYNTAX      WmanIf2SsPkmV2RsaAuthEntry
10         MAX-ACCESS  not-accessible
11         STATUS      current
12         DESCRIPTION
13             "The table is indexed by ifIndex."
14         INDEX       { ifIndex }
15         ::= { wmanIf2SsPkmV2RsaAuthTable 1 }
16
17     WmanIf2SsPkmV2RsaAuthEntry ::= SEQUENCE {
18         wmanIf2SsPkmV2BsCertificate      OCTET STRING,
19         wmanIf2SsPkmV2SsCertificate      OCTET STRING,
20         wmanIf2SsPkmV2SaId               INTEGER,
21         wmanIf2SsPkmV2SsRandom           OCTET STRING,
22         wmanIf2SsPkmV2BsRandom           OCTET STRING,
23         wmanIf2SsPkmV2AuthKeySequenceNumber Integer32,
24         wmanIf2SsPkmV2AuthKeyLifetime   Integer32,
25         wmanIf2SsPkmV2AuthFailure        WmanIf2AuthFailureType,
26         wmanIf2SsPkmV2LastAkExpireTime  DateAndTime,
27         wmanIf2SsPkmV2LatestAkExpireTime DateAndTime}
28
29     wmanIf2SsPkmV2BsCertificate OBJECT-TYPE
30         SYNTAX      OCTET STRING (SIZE(0..65535))
31         MAX-ACCESS  read-only
32         STATUS      current
33         DESCRIPTION
34             "BS sends the BS-Certificate in the PKMV2 RSA-Reply message
35             for BS-SS mutual authentication. It is the DER-encoded
36             ASN.1 X.509 BS Certificate."
37         REFERENCE
38             "Subclause 11.9.24 in IEEE Std 802.16e-2005"
39         ::= { wmanIf2SsPkmV2RsaAuthEntry 1 }
40
41     wmanIf2SsPkmV2SsCertificate OBJECT-TYPE
42         SYNTAX      OCTET STRING (SIZE(0..65535))
43         MAX-ACCESS  read-only
44         STATUS      current
45         DESCRIPTION
46             "SS sends the SS-Certificate in the PKMV2 RSA-Request
47             message. It contains an X.509 SS certificate issued by the
48             SS's manufacturer. The SS's X.509 certificate is a
49             public-key certificate which binds the SS's identifying
50             information to its RSA public key in a verifiable manner.
51             The X.509 certificate is digitally signed by the SS's
52             manufacturer, and that signature can be verified by a BS
53             that knows the manufacturer's public key.
54             The manufacturer's public key is placed in an X.509
55             certification authority (CA) certificate, which in turn
56             is signed by a higher level CA."
57         REFERENCE
58             "Subclause 11.9.12 in IEEE Std 802.16-2004"
59         ::= { wmanIf2SsPkmV2RsaAuthEntry 2 }
60
61     wmanIf2SsPkmV2SaId OBJECT-TYPE
62         SYNTAX      INTEGER (0..65535)
63         MAX-ACCESS  read-only
64         STATUS      current

```

```

1      DESCRIPTION
2          "SS's primary SAID equal to the Basic CID. SS sends the SAID
3          in the PKMV2 RSA-Request message."
4      REFERENCE
5          "Subclause 6.3.2.3.9.2 in IEEE Std 802.16-2004"
6          ::= { wmanIf2SsPkmV2RsaAuthEntry 3 }
7
8      wmanIf2SsPkmV2SsRandom OBJECT-TYPE
9          SYNTAX      OCTET STRING (SIZE(8))
10         MAX-ACCESS  read-only
11         STATUS      current
12         DESCRIPTION
13             "This attribute contains a quantity that is pseudo random
14             number generated from the MS and used as fresh number for
15             mutual authorization message handshake. SS sends the SS-Random
16             in the PKMV2 RSA-Request message."
17         REFERENCE
18             "Subclause 11.9.21 in IEEE Std 802.16e-2005"
19             ::= { wmanIf2SsPkmV2RsaAuthEntry 4 }
20
21     wmanIf2SsPkmV2BsRandom OBJECT-TYPE
22         SYNTAX      OCTET STRING (SIZE(8))
23         MAX-ACCESS  read-only
24         STATUS      current
25         DESCRIPTION
26             "This attribute contains a quantity that is pseudo random
27             number generated from the BS and used as fresh number for
28             mutual authorization message handshake. BS sends the BS-Random
29             in the PKMV2 RSA-Reply message."
30         REFERENCE
31             "Subclause 11.9.22 in IEEE Std 802.16e-2005"
32             ::= { wmanIf2SsPkmV2RsaAuthEntry 5 }
33
34     wmanIf2SsPkmV2AuthKeySequenceNumber OBJECT-TYPE
35         SYNTAX      Integer32 (0 .. 15)
36         MAX-ACCESS  read-only
37         STATUS      current
38         DESCRIPTION
39             "This object provides the most recent authorization key
40             sequence number in the PKMV2 RSA-Reply message for an SS."
41         REFERENCE
42             "Subclause 11.9.5 in IEEE Std 802.16e-2005"
43             ::= { wmanIf2SsPkmV2RsaAuthEntry 6 }
44
45     wmanIf2SsPkmV2AuthKeyLifetime OBJECT-TYPE
46         SYNTAX      Integer32 (86400..6048000)
47         UNITS       "seconds"
48         MAX-ACCESS  read-only
49         STATUS      current
50         DESCRIPTION
51             "This object defines the lifetime of an authorization
52             key (AK) the BS assigns to a SS. BS sends the key lifetime
53             in the PKMV2 RSA-Reply message."
54         REFERENCE
55             "Subclause 11.9.4 in IEEE Std 802.16e-2005"
56             ::= { wmanIf2SsPkmV2RsaAuthEntry 7 }
57
58     wmanIf2SsPkmV2AuthFailure OBJECT-TYPE
59         SYNTAX      WmanIf2AuthFailureType
60         MAX-ACCESS  read-only
61         STATUS      current
62         DESCRIPTION
63             "BS returns PKMV2 RSA-Rejects message if an authorization
64             failure is detected."

```

```

1
2     Failure type unknownManufactur(4)- ssBsIncompatibleSc(9) are
3     considered permanent authorization failure, since any
4     attempts of reauthorization would continue to result in
5     Authorization Rejects. Details about the cause of a
6     Permanent Authorization Failure may be reported to the SS
7     in an optional Display-String attribute that may accompany
8     the Error-Code attribute in Authorization Reject messages.
9
10    Note that the BS may log the Display-String attribute and
11    Authorization failures in wmanIfDevMib, and generate a trap
12    to an SNMP manager."
13    REFERENCE
14        "Subclause 11.9.10 in IEEE Std 802.16-2004"
15    ::= { wmanIf2SsPkmV2RsaAuthEntry 8 }
16
17    wmanIf2SsPkmV2LastAkExpireTime OBJECT-TYPE
18        SYNTAX      DateAndTime
19        MAX-ACCESS  read-only
20        STATUS      current
21        DESCRIPTION
22            "This object is the time when the last AK expires.
23             wmanIf2SsPkmV2LastAkExpireTime = Time(last AK[RSA-Reply])
24             + AK lifetime
25             If this FSM has only one authorization key, then
26             wmanIf2SsPkmV2LastAkExpireTime = the activation of FSM."
27    ::= { wmanIf2SsPkmV2RsaAuthEntry 9 }
28
29    wmanIf2SsPkmV2LatestAkExpireTime OBJECT-TYPE
30        SYNTAX      DateAndTime
31        MAX-ACCESS  read-only
32        STATUS      current
33        DESCRIPTION
34            "This object is the time when the latest AK expires."
35    ::= { wmanIf2SsPkmV2RsaAuthEntry 10 }
36
37    --
38    -- Table wmanIf2SsPkmV2TekTable
39    --
40    wmanIf2SsPkmV2TekTable OBJECT-TYPE
41        SYNTAX      SEQUENCE OF WmanIf2SsPkmV2TekEntry
42        MAX-ACCESS  not-accessible
43        STATUS      current
44        DESCRIPTION
45            "This table contains the TEK attributes that are associated
46             with each SAID."
47    ::= { wmanIf2SsPkmV2Objects 3 }
48
49    wmanIf2SsPkmV2TekEntry OBJECT-TYPE
50        SYNTAX      WmanIf2SsPkmV2TekEntry
51        MAX-ACCESS  not-accessible
52        STATUS      current
53        DESCRIPTION
54            "This table is double indexed by ifIndex and
55             wmanIf2SsPkmSaidIndex."
56        INDEX      { ifIndex,
57                   wmanIf2SsPkmV2SaidIndex }
58    ::= { wmanIf2SsPkmV2TekTable 1 }
59
60    WmanIf2SsPkmV2TekEntry ::= SEQUENCE {
61        wmanIf2SsPkmV2SaidIndex          INTEGER,
62        wmanIf2SsPkmV2SaType             WmanIf2SaType,
63        wmanIf2SsPkmV2OlderTekSequenceNumber Integer32,
64        wmanIf2SsPkmV2OlderTekLifetime  Integer32,

```



```

1          wmanIf2SsPkmV2NewerTekSequenceNumber      Integer32,
2          wmanIf2SsPkmV2NewerTekLifetime           Integer32,
3          wmanIf2SsPkmV2AuthInvalidError           WmanIf2AuthInvalidError,
4          wmanIf2SsPkmV2LastTekExpireTime           DateAndTime,
5          wmanIf2SsPkmV2LatestTekExpireTime         DateAndTime}
6
7  wmanIf2SsPkmV2SaidIndex OBJECT-TYPE
8      SYNTAX      INTEGER (0 .. 65535)
9      MAX-ACCESS  not-accessible
10     STATUS      current
11     DESCRIPTION
12         "SAID index to the wmanIf2SsPkmV2TekTable."
13     ::= { wmanIf2SsPkmV2TekEntry 1 }
14
15  wmanIf2SsPkmV2SaType OBJECT-TYPE
16     SYNTAX      WmanIf2SaType
17     MAX-ACCESS  read-only
18     STATUS      current
19     DESCRIPTION
20         "SA Type attribute that is included in the Auth Reply
21         message."
22     ::= { wmanIf2SsPkmV2TekEntry 2 }
23
24  wmanIf2SsPkmV2OlderTekSequenceNumber OBJECT-TYPE
25     SYNTAX      Integer32 (0 .. 3)
26     MAX-ACCESS  read-only
27     STATUS      current
28     DESCRIPTION
29         "At all times the BS maintains two sets of active
30         generations of keying material per SAID. One set
31         corresponds to the 'older' generation of keying material,
32         the second set corresponds to the 'newer' generation of
33         keying material. The newer generation has a key sequence
34         number one greater than (modulo 4) that of the older
35         generation. This object provides the older TEK sequence
36         number in the Key Reply message for an SS."
37     REFERENCE
38         "Subclause 11.9.8 in IEEE Std 802.16-2004"
39     ::= { wmanIf2SsPkmV2TekEntry 3 }
40
41  wmanIf2SsPkmV2OlderTekLifetime OBJECT-TYPE
42     SYNTAX      Integer32 (1800 .. 604800)
43     UNITS       "seconds"
44     MAX-ACCESS  read-only
45     STATUS      current
46     DESCRIPTION
47         "This object provides the older TEK Remaining Lifetime."
48     REFERENCE
49         "Subclause 11.9.8 in IEEE Std 802.16-2004"
50     ::= { wmanIf2SsPkmV2TekEntry 4 }
51
52  wmanIf2SsPkmV2NewerTekSequenceNumber OBJECT-TYPE
53     SYNTAX      Integer32 (0 .. 3)
54     MAX-ACCESS  read-only
55     STATUS      current
56     DESCRIPTION
57         "This object provides the newer TEK sequence
58         number in the Key Reply message for an SS."
59     REFERENCE
60         "Subclause 11.9.8 in IEEE Std 802.16-2004"
61     ::= { wmanIf2SsPkmV2TekEntry 5 }
62
63  wmanIf2SsPkmV2NewerTekLifetime OBJECT-TYPE
64     SYNTAX      Integer32 (1800 .. 604800)

```

```

1          UNITS          "seconds"
2          MAX-ACCESS    read-only
3          STATUS        current
4          DESCRIPTION
5              "This object provides the newer TEK Remaining Lifetime."
6          REFERENCE
7              "Subclause 11.9.8 in IEEE Std 802.16-2004"
8          ::= { wmanIf2SsPkmV2TekEntry 6 }
9
10         wmanIf2SsPkmV2AuthInvalidError OBJECT-TYPE
11             SYNTAX      WmanIf2AuthInvalidError
12             MAX-ACCESS  read-only
13             STATUS      current
14             DESCRIPTION
15                 "BS returns Authorization Invalid message if an authorization
16                 invalid error is detected.
17
18                 Note that the BS may log the Display-String attribute and
19                 Authorization invalid error in wmanIfDevMib."
20             REFERENCE
21                 "Subclause 11.9.10 in IEEE Std 802.16-2004"
22             ::= { wmanIf2SsPkmV2TekEntry 7 }
23
24         wmanIf2SsPkmV2LastTekExpireTime OBJECT-TYPE
25             SYNTAX      DateAndTime
26             MAX-ACCESS  read-only
27             STATUS      current
28             DESCRIPTION
29                 "This object is the time when the last TEK expires.
30                 wmanIf2SsPkmV2LastTekExpireTime = Time(last TEK[Key Reply])
31                 + TEK lifetime
32                 If this FSM has only one authorization key, then
33                 wmanIf2SsPkmV2LastTekExpireTime = the activation of FSM."
34             ::= { wmanIf2SsPkmV2TekEntry 8 }
35
36         wmanIf2SsPkmV2LatestTekExpireTime OBJECT-TYPE
37             SYNTAX      DateAndTime
38             MAX-ACCESS  read-only
39             STATUS      current
40             DESCRIPTION
41                 "This object is the time when the latest TEK expires."
42             ::= { wmanIf2SsPkmV2TekEntry 9 }
43
44
45
46
47
48
49
50

```

- 1
- 2
- 3
- 4

