

Project	IEEE 802.16 Broadband Wireless Access Working Group < http://ieee802.org/16 >
Title	Proposed text and ASN.1 code to support PKMV1 and PKMV2
Date Submitted	2007-01-18
Source(s)	Joey Chou Intel Corporation [mailto:joey.chou@intel.com]
Re:	
Abstract	This contribution proposes the text and ASN.1 code in wmanIf2Mib to support PKMV1 and PKMV2.
Purpose	Adoption
Notice	This document has been prepared to assist IEEE 802.16. It is offered as a basis for discussion and is not binding on the contributing individual(s) or organization(s). The material in this document is subject to change in form and content after further study. The contributor(s) reserve(s) the right to add, amend or withdraw material contained herein.
Release	The contributor grants a free, irrevocable license to the IEEE to incorporate material contained in this contribution, and any modifications thereof, in the creation of an IEEE Standards publication; to copyright in the IEEE's name any IEEE Standards publication even though it may include portions of this contribution; and at the IEEE's sole discretion to permit others to reproduce in whole or in part the resulting IEEE Standards publication. The contributor also acknowledges and accepts that this contribution may be made public by IEEE 802.16.
Patent Policy and Procedures	<p>The contributor is familiar with the IEEE 802.16 Patent Policy and Procedures (Version 1.0) <http://ieee802.org/16/ipr/patents/policy.html>, including the statement "IEEE standards may include the known use of patent(s), including patent applications, if there is technical justification in the opinion of the standards-developing committee and provided the IEEE receives assurance from the patent holder that it will license applicants under reasonable terms and conditions for the purpose of implementing the standard."</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 <mailto:r.b.marks@ieee.org> as early as possible, in written or electronic form, of any patents (granted or under application) that may cover technology that is under consideration by or has been approved by IEEE 802.16. The Chair will disclose this notification via the IEEE 802.16 web site <http://ieee802.org/16/ipr/patents/notices>.</p>

Table of Content

- 1. Introduction..... 3**
- 2. NRM IRP SNMP Solution Set change Proposal..... 3**
- 2.1 wmanlf2BsPkmObjects Changes..... 3**
- 2.2 wmanlf2SsPkmObjects Changes..... 5**
- 2.3 wmanlf2BsPkmObjects ASN.1 Code Change..... 7**
- 2.4 wmanlf2BsPkmV2Objects ASN.1 Code Change..... 23**
- 2.5 wmanlf2SsPkmObjects ASN.1 Code Change..... 31**
- 2.6 wmanlf2SsPkmV2Objects ASN.1 Code Change..... 41**

1

1

2. Introduction

2

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

2. NRM IRP SNMP Solution Set change Proposal

4

2.1 wmanlf2BsPkmObjects Changes

5

13.1.3.1 wmanlf2BsObjects

6

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

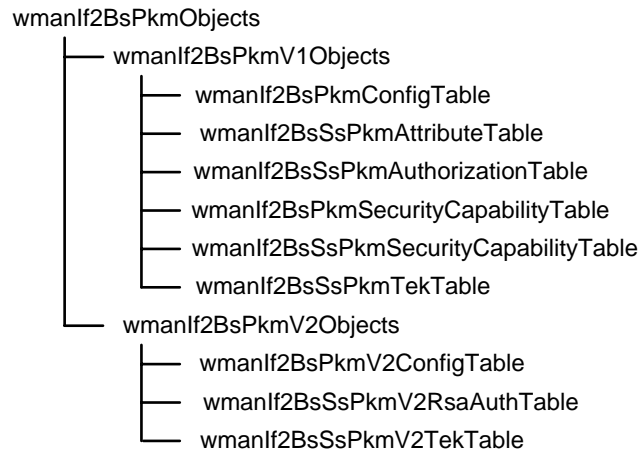
7

8

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.



12

13

14

15

Figure 8— wmanlf2BsPkmObjects structure

13.1.3.1.3.1 wmanlf2BsPkmV1Objects

16

13.1.3.1.3.1.1 wmanlf2BsPkmConfigTable

17

18 wmanlf2BsPkmConfigTable contains the configuration of the PKM attributes that are to be used for
19 BS and all SSs that are connected to such BS .

13.1.3.1.3.1.2 wmanlf2BsSsPkmAttributeTable

20

21 wmanlf2BsSsPkmAttributeTable contains the PKM attributes on per SS basis.

13.1.3.1.3.1.3 wmanlf2BsSsPkmAuthorizationTable

22

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

2 **13.1.3.1.3.1.4 wmanlf2BsPkmSecurityCapabilityTable**

3 wmanlf2BsSsPkmSecurityCapabilityTable contains the list of the cryptographic suite(s) an BS
4 supports.

5 **13.1.3.1.3.1.5 wmanlf2BsSsPkmSecurityCapabilityTable**

6 wmanlf2BsSsPkmSecurityCapabilityTable contains the SS's Security Capabilities that are
7 conveyed by the Auth Request message. It contains the list of the cryptographic suite(s) an SS
8 supports.

9 **13.1.3.1.3.1.6 wmanlf2BsSsPkmTekTable**

10 wmanlf2BsSsPkmTekTable contains the TEK attributes that are associated with each SAID.

11 **13.1.3.1.3.2 wmanlf2BsPkmV2Objects**

12 **13.1.3.1.3.2.1 wmanlf2BsPkmV2ConfigTable**

13 wmanlf2BsPkmV2ConfigTable contains the PKM attributes that are needed to PKM operation.

14 **13.1.3.1.3.2.2 wmanlf2BsSsPkmV2RsaAuthTable**

15 wmanlf2BsSsPkmV2RsaAuthTable contains information related to PKMV2 RSA based
16 authorization process.

17 **13.1.3.1.3.2.3 wmanlf2BsSsPkmV2TekTable**

18 wmanlf2BsSsPkmV2TekTable contains the TEK attributes that are associated with each SAID.

1 2.2 wmanlf2SsPkmObjects Changes

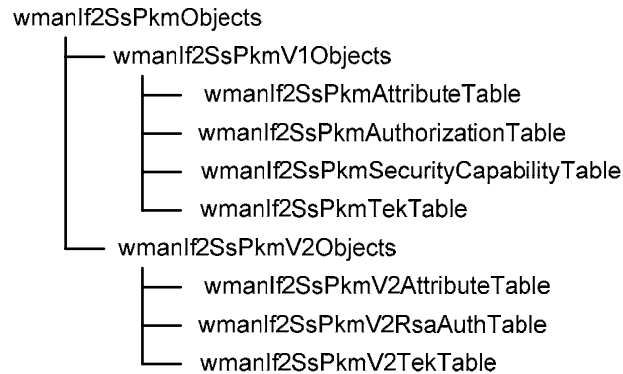
2 13.1.3.1 wmanlf2BsObjects

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

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

Figure 12— wmanlf2SsPkmObjects structure

11

12 13.1.3.2.2.1 wmanlf2BsPkmV1Objects

13 13.1.3.2.2.1.1 wmanlf2SsPkmAttributeTable

14 wmanlf2SsPkmAttributeTable provides the configuration of the PKM attributes that are needed to
15 PKM operation.

16 13.1.3.2.2.1.2 wmanlf2SsPkmAuthorizationTable

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

19 13.1.3.2.2.1.3 wmanlf2SsPkmSecurityCapabilityTable

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

22 13.1.3.2.2.1.4 wmanlf2SsPkmTekTable

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

24 13.1.3.2.2.2 wmanlf2BsPkmV2Objects

1 **13.1.3.2.2.2.1 wmanIf2SsPkmV2AttributeTable**

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

3 **13.1.3.2.2.2.2 wmanIf2SsPkmV2RsaAuthTable**

4 wmanIf2SsPkmV2RsaAuthTable contains information related to PKMV2 RSA based authorization
5 process.

6 **13.1.3.2.2.2.3 wmanIf2SsPkmV2TekTable**

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

2.3 wmanIf2BsPkmObjects ASN.1 Code Change

13.2 ASN.1 Definitions of MIB Modules

13.2.3 wmanIf2Mib

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

```

7 WmanIf2PkmErrorCode ::= TEXTUAL-CONVENTION
8     STATUS      current
9     DESCRIPTION
10        "This error code provides further information about an
11        Authorization Reject, Key Reject, Authorization Invalid,
12        or TEK Invalid.
13
14        0 - no failure
15        1 - unauthorized SS
16        2 - unauthorized SAID
17        3 - unsolicited
18        4 - invalid key sequence
19        5 - key request authentication failure
20
21        The following are error code for permanent authorization
22        failure that indicates any reattempts at authorization
23        would continue to result in Authorization Rejects.
24
25        6 - the BS does not have the CA certificate belonging
26        to the issuer of an SS certificate
27        7 - SS certificate has an invalid signature
28        8 - ASN.1 parsing failure during verification of SS
29        certificate
30        9 - SS certificate is on the 'hot list'
31        10 - inconsistencies between certificate data and data
32        in accompanying PKM attributes
33        11 - SS and BS have incompatible security capabilities"
34 REFERENCE
35     "Subclause 11.9.10 in IEEE Std 802.16-2004"
36 SYNTAX      INTEGER {noFailure(0),
37                    unauthorizedSs(1),
38                    unauthorizedSaid(2),
39                    unsolicited(3),
40                    invalidKeySequence(4),
41                    keyReqAuthFailure(5),
42                    unknownManufactur(6),
43                    invalidSignature(7),
44                    asn1ParsingFailure(8),
45                    ssCaOnHotList(9),
46                    dataInconsistency(10),
47                    ssBsIncompatibleSc(11)}
48
49
50 WmanIf2SaType ::= TEXTUAL-CONVENTION
51     STATUS      current
52     DESCRIPTION
53        "The type of Security Association (SA)."
```

REFERENCE

```

54     "Table 379 in IEEE Std 802.16-2004"
55 SYNTAX      INTEGER {primarySa(0),
56                    staticSa(1),
57                    dynamicSa(2)}
```

```

1
2 WmanIf2TekState ::= TEXTUAL-CONVENTION
3     STATUS      current
4     DESCRIPTION
5         "TEK State."
6     REFERENCE
7         "Subclause 7.2.5.1 in IEEE Std 802.16-2004"
8     SYNTAX      INTEGER {start(1),
9                 opWait(2),
10                opReauthWait(3),
11                operational(4),
12                rekeyWait(5),
13                rekeyReauthWait(6)}
14
15
16 WmanIf2CertificateStat ::= TEXTUAL-CONVENTION
17     STATUS      current
18     DESCRIPTION
19         "The reason why a SS's certificate is deemed valid
20         or invalid:
21
22         0 - return unknown if the SS is running PKM mode
23         1 - means the certificate is valid because it chains
24             to a valid certificate
25         2 - means the certificate is valid because it has been
26             provisioned to be trusted
27         3 - means the certificate is invalid because it has been
28             provisioned to be untrusted.
29         4 - means the certificate is invalid because it chains
30             to an untrusted certificate.
31         5 - refer to errors in parsing, validity periods, etc,
32             of SS certificate
33         6 - refer to errors in parsing, validity periods, etc,
34             of CA certificate"
35     REFERENCE
36         "Subclause 7.2.5.1 in IEEE Std 802.16-2004"
37     SYNTAX      INTEGER {unknown (0),
38                 validSsChained (1),
39                 validSsTrusted (2),
40                 invalidSsUntrusted (3),
41                 invalidCAUntrusted (4),
42                 invalidSsOther (5),
43                 invalidCAOther (6)}
44
45 --
46 -- Base station PKM group
47 -- wmanIf2BsPkmObjects contain the Base Station Privacy Sublayer objects
48 --
49 wmanIf2BsPkmObjects OBJECT IDENTIFIER ::= { wmanIf2BsObjects 3 }
50
51 wmanIf2BsPkmV1Objects OBJECT IDENTIFIER ::= { wmanIf2BsPkmObjects 1 }
52
53 -- Table wmanIf2BsPkmConfigTable
54 --
55 wmanIf2BsPkmConfigTable OBJECT-TYPE
56     SYNTAX      SEQUENCE OF WmanIf2BsPkmConfigEntry
57     MAX-ACCESS  not-accessible
58     STATUS      current
59     DESCRIPTION
60         "This table contains the configuration of the PKM
61         attributes that are to be used for BS and SS."
62     REFERENCE
63         "Table 343 in IEEE Std 802.16-2004 and 802.16e-2005"
64     ::= { wmanIf2BsPkmV1Objects 1 }

```



```

1
2 wmanIf2BsPkmConfigEntry OBJECT-TYPE
3     SYNTAX      WmanIf2BsPkmConfigEntry
4     MAX-ACCESS  not-accessible
5     STATUS      current
6     DESCRIPTION
7         "Each entry contains objects that define the PKM attributes
8         of each BS wireless interface, and all SSS that are
9         connected with such BS. The table is indexed by ifIndex
10        that is associated with the BS sector."
11     INDEX       { ifIndex }
12     ::= { wmanIf2BsPkmConfigTable 1 }
13
14 WmanIf2BsPkmConfigEntry ::= SEQUENCE {
15     wmanIf2BsPkmAkLifetime      Integer32,
16     wmanIf2BsPkmTekLifetime     Integer32,
17     wmanIf2BsPkmSelfSigManufCertTrust  INTEGER,
18     wmanIf2BsPkmAuthWaitTimeout Integer32,
19     wmanIf2BsPkmReauthWaitTimeout Integer32,
20     wmanIf2BsPkmAuthGraceTime  Integer32,
21     wmanIf2BsPkmOpWaitTimeout  Integer32,
22     wmanIf2BsPkmRekeyWaitTimeout Integer32,
23     wmanIf2BsPkmTekGraceTime   Integer32,
24     wmanIf2BsPkmAuthRejectWaitTimeout Integer32,
25     wmanIf2BsPkmCheckCertValidityPeriods TruthValue}
26
27 wmanIf2BsPkmAkLifetime OBJECT-TYPE
28     SYNTAX      Integer32 (86400 .. 6048000)
29     UNITS       "seconds"
30     MAX-ACCESS  read-write
31     STATUS      current
32     DESCRIPTION
33         "This object defines the lifetime of a newly assigned
34         authorization key."
35     REFERENCE
36         "Table 343 in IEEE Std 802.16-2004"
37     DEFVAL     { 604800 }
38     ::= { wmanIf2BsPkmConfigEntry 1 }
39
40 wmanIf2BsPkmTekLifetime OBJECT-TYPE
41     SYNTAX      Integer32 (1800 .. 604800)
42     UNITS       "seconds"
43     MAX-ACCESS  read-write
44     STATUS      current
45     DESCRIPTION
46         "This object defines the lifetime of a newly assigned
47         Traffic Encryption Key(TEK).".
48     REFERENCE
49         "Table 343 in IEEE Std 802.16-2004"
50     DEFVAL     { 43200 }
51     ::= { wmanIf2BsPkmConfigEntry 2 }
52
53 wmanIf2BsPkmSelfSigManufCertTrust OBJECT-TYPE
54     SYNTAX      INTEGER {trusted (1),
55                       untrusted (2)}
56     MAX-ACCESS  read-write
57     STATUS      current
58     DESCRIPTION
59         "This object determines the default trust of all (new)
60         self-signed manufacturer certificates obtained after
61         setting the object."
62     ::= { wmanIf2BsPkmConfigEntry 3 }
63
64 wmanIf2BsPkmAuthWaitTimeout OBJECT-TYPE

```

```

1      SYNTAX      Integer32 (2 .. 30)
2      UNITS       "seconds"
3      MAX-ACCESS  read-write
4      STATUS      current
5      DESCRIPTION
6          "This object defines the Auth Req retransmission interval
7           from Auth Wait state."
8      REFERENCE
9          "Table 343 and subclause 11.9.19 in IEEE Std 802.16-2004"
10     DEFVAL      { 10 }
11     ::= { wmanIf2BsPkmConfigEntry 4 }
12
13     wmanIf2BsPkmReauthWaitTimeout OBJECT-TYPE
14     SYNTAX      Integer32 (2 .. 30)
15     UNITS       "seconds"
16     MAX-ACCESS  read-write
17     STATUS      current
18     DESCRIPTION
19         "This object defines the Auth Req retransmission interval
20          from Reauth Wait state."
21     REFERENCE
22         "Table 343 and subclause 11.9.19 in IEEE Std 802.16-2004"
23     DEFVAL      { 10 }
24     ::= { wmanIf2BsPkmConfigEntry 5 }
25
26     wmanIf2BsPkmAuthGraceTime OBJECT-TYPE
27     SYNTAX      Integer32 (300 .. 3024000)
28     UNITS       "seconds"
29     MAX-ACCESS  read-write
30     STATUS      current
31     DESCRIPTION
32         "The value of this object is the grace time for an
33          authorization key. A SS is expected to start trying to get
34          a new authorization key beginning AuthGraceTime seconds
35          before the authorization key actually expires."
36     REFERENCE
37         "Table 343 and subclause 11.9.19 in IEEE Std 802.16-2004"
38     DEFVAL      { 600 }
39     ::= { wmanIf2BsPkmConfigEntry 6 }
40
41     wmanIf2BsPkmOpWaitTimeout OBJECT-TYPE
42     SYNTAX      Integer32 (1 .. 10)
43     UNITS       "seconds"
44     MAX-ACCESS  read-write
45     STATUS      current
46     DESCRIPTION
47         "This object defines the Key Req retransmission interval
48          from Op Wait state."
49     REFERENCE
50         "Table 343 and subclause 11.9.19 in IEEE Std 802.16-2004"
51     DEFVAL      { 1 }
52     ::= { wmanIf2BsPkmConfigEntry 7 }
53
54     wmanIf2BsPkmRekeyWaitTimeout OBJECT-TYPE
55     SYNTAX      Integer32 (1 .. 10)
56     UNITS       "seconds"
57     MAX-ACCESS  read-write
58     STATUS      current
59     DESCRIPTION
60         "This object defines the Key Req retransmission interval
61          from Rekey Wait state."
62     REFERENCE
63         "Table 343 and subclause 11.9.19 in IEEE Std 802.16-2004"
64     DEFVAL      { 1 }

```

```

1      ::= { wmanIf2BsPkmConfigEntry 8 }
2
3  wmanIf2BsPkmTekGraceTime OBJECT-TYPE
4      SYNTAX      Integer32 (300 .. 3024000)
5      UNITS       "seconds"
6      MAX-ACCESS  read-write
7      STATUS      current
8      DESCRIPTION
9          "The value of this object is the grace time for the TEK in
10         seconds. The SS is expected to start trying to acquire a
11         new TEK beginning TEK GraceTime seconds before the
12         expiration of the most recent TEK."
13     REFERENCE
14         "Table 343 and subclause 11.9.19 in IEEE Std 802.16-2004"
15     DEFVAL      { 3600 }
16     ::= { wmanIf2BsPkmConfigEntry 9 }
17
18  wmanIf2BsPkmAuthRejectWaitTimeout OBJECT-TYPE
19      SYNTAX      Integer32 (10 .. 600)
20      UNITS       "seconds"
21      MAX-ACCESS  read-write
22      STATUS      current
23      DESCRIPTION
24          "This object defines the Delay before resending Auth Request
25         after receiving Auth Reject."
26     REFERENCE
27         "Table 343 and subclause 11.9.19 in IEEE Std 802.16-2004"
28     DEFVAL      { 60 }
29     ::= { wmanIf2BsPkmConfigEntry 10 }
30
31  wmanIf2BsPkmCheckCertValidityPeriods OBJECT-TYPE
32      SYNTAX      TruthValue
33      MAX-ACCESS  read-write
34      STATUS      current
35      DESCRIPTION
36          "Setting this object to TRUE causes all certificates
37         received thereafter to have their validity periods (and
38         their chain's validity periods) checked against the current
39         time of day. A FALSE setting will cause all certificates
40         received Thereafter to not have their validity periods
41         (nor their chain's validity periods) checked against the
42         current time of day."
43     ::= { wmanIf2BsPkmConfigEntry 11 }
44
45  -- Table wmanIf2BsSsPkmConfigTable
46  --
47  wmanIf2BsSsPkmAttributeTable OBJECT-TYPE
48      SYNTAX      SEQUENCE OF WmanIf2BsSsPkmAttributeEntry
49      MAX-ACCESS  not-accessible
50      STATUS      current
51      DESCRIPTION
52          "This table contains the the PKM attributes that are needed
53         to PKM operation."
54     REFERENCE
55         "Table 343 in IEEE Std 802.16-2004 and 802.16e-2005"
56     ::= { wmanIf2BsPkmV1Objects 2 }
57
58  wmanIf2BsSsPkmAttributeEntry OBJECT-TYPE
59      SYNTAX      WmanIf2BsSsPkmAttributeEntry
60      MAX-ACCESS  not-accessible
61      STATUS      current
62      DESCRIPTION
63          "Each entry contains objects that show the PKM attributes
64         of each SS wireless interface. The table is indexed by

```

```

1         ifIndex and wmanIf2BsSsMacAddress."
2     INDEX        { ifIndex, wmanIf2BsSsMacAddress }
3     ::= { wmanIf2BsSsPkmAttributeTable 1 }
4
5     WmanIf2BsSsPkmAttributeEntry ::= SEQUENCE {
6         wmanIf2BsSsPkmAuthWaitTimeout      Integer32,
7         wmanIf2BsSsPkmReauthWaitTimeout    Integer32,
8         wmanIf2BsSsPkmAuthGraceTime        Integer32,
9         wmanIf2BsSsPkmOpWaitTimeout        Integer32,
10        wmanIf2BsSsPkmRekeyWaitTimeout     Integer32,
11        wmanIf2BsSsPkmTekGraceTime         Integer32,
12        wmanIf2BsSsPkmAuthRejectWaitTimeout Integer32}
13
14    wmanIf2BsSsPkmAuthWaitTimeout OBJECT-TYPE
15        SYNTAX      Integer32 (2 .. 30)
16        UNITS       "seconds"
17        MAX-ACCESS  read-only
18        STATUS      current
19        DESCRIPTION
20            "This object defines the Auth Req retransmission interval
21             from Auth Wait state."
22        REFERENCE
23            "Table 343 and subclause 11.9.19 in IEEE Std 802.16-2004"
24        DEFVAL      { 10 }
25        ::= { wmanIf2BsSsPkmAttributeEntry 1 }
26
27    wmanIf2BsSsPkmReauthWaitTimeout OBJECT-TYPE
28        SYNTAX      Integer32 (2 .. 30)
29        UNITS       "seconds"
30        MAX-ACCESS  read-only
31        STATUS      current
32        DESCRIPTION
33            "This object defines the Auth Req retransmission interval
34             from Reauth Wait state."
35        REFERENCE
36            "Table 343 and subclause 11.9.19 in IEEE Std 802.16-2004"
37        DEFVAL      { 10 }
38        ::= { wmanIf2BsSsPkmAttributeEntry 2 }
39
40    wmanIf2BsSsPkmAuthGraceTime OBJECT-TYPE
41        SYNTAX      Integer32 (300 .. 3024000)
42        UNITS       "seconds"
43        MAX-ACCESS  read-only
44        STATUS      current
45        DESCRIPTION
46            "The value of this object is the grace time for an
47             authorization key. A SS is expected to start trying to get
48             a new authorization key beginning AuthGraceTime seconds
49             before the authorization key actually expires."
50        REFERENCE
51            "Table 343 and subclause 11.9.19 in IEEE Std 802.16-2004"
52        DEFVAL      { 600 }
53        ::= { wmanIf2BsSsPkmAttributeEntry 3 }
54
55    wmanIf2BsSsPkmOpWaitTimeout OBJECT-TYPE
56        SYNTAX      Integer32 (1 .. 10)
57        UNITS       "seconds"
58        MAX-ACCESS  read-only
59        STATUS      current
60        DESCRIPTION
61            "This object defines the Key Req retransmission interval
62             from Op Wait state."
63        REFERENCE
64            "Table 343 and subclause 11.9.19 in IEEE Std 802.16-2004"

```

```

1         DEFVAL          { 1 }
2         ::= { wmanIf2BsSsPkmAttributeEntry 4 }
3
4 wmanIf2BsSsPkmRekeyWaitTimeout OBJECT-TYPE
5     SYNTAX      Integer32 (1 .. 10)
6     UNITS       "seconds"
7     MAX-ACCESS  read-only
8     STATUS      current
9     DESCRIPTION
10        "This object defines the Key Req retransmission interval
11         from Rekey Wait state."
12     REFERENCE
13        "Table 343 and subclause 11.9.19 in IEEE Std 802.16-2004"
14     DEFVAL      { 1 }
15     ::= { wmanIf2BsSsPkmAttributeEntry 5 }
16
17 wmanIf2BsSsPkmTekGraceTime OBJECT-TYPE
18     SYNTAX      Integer32 (300 .. 3024000)
19     UNITS       "seconds"
20     MAX-ACCESS  read-only
21     STATUS      current
22     DESCRIPTION
23        "The value of this object is the grace time for the TEK in
24         seconds. The SS is expected to start trying to acquire a
25         new TEK beginning TEK GraceTime seconds before the
26         expiration of the most recent TEK."
27     REFERENCE
28        "Table 343 and subclause 11.9.19 in IEEE Std 802.16-2004"
29     DEFVAL      { 3600 }
30     ::= { wmanIf2BsSsPkmAttributeEntry 6 }
31
32 wmanIf2BsSsPkmAuthRejectWaitTimeout OBJECT-TYPE
33     SYNTAX      Integer32 (10 .. 600)
34     UNITS       "seconds"
35     MAX-ACCESS  read-only
36     STATUS      current
37     DESCRIPTION
38        "This object defines the Delay before resending Auth Request
39         after receiving Auth Reject."
40     REFERENCE
41        "Table 343 and subclause 11.9.19 in IEEE Std 802.16-2004"
42     DEFVAL      { 60 }
43     ::= { wmanIf2BsSsPkmAttributeEntry 7 }
44
45 -- Table wmanIf2BsSsPkmAuthorizationTable
46 --
47 wmanIf2BsSsPkmAuthorizationTable OBJECT-TYPE
48     SYNTAX      SEQUENCE OF WmanIf2BsSsPkmAuthorizationEntry
49     MAX-ACCESS  not-accessible
50     STATUS      current
51     DESCRIPTION
52        "This table contains information related to SS's
53         authorization process."
54     REFERENCE
55        "Table 28 and 37 in IEEE Std 802.16-2004"
56     ::= { wmanIf2BsSsPkmV1Objects 3 }
57
58 wmanIf2BsSsPkmAuthorizationEntry OBJECT-TYPE
59     SYNTAX      WmanIf2BsSsPkmAuthorizationEntry
60     MAX-ACCESS  not-accessible
61     STATUS      current
62     DESCRIPTION
63        "Each entry contains objects that define the SS
64         authorization attributes for each SS associated with each

```

```

1         BS sector. The table is indexed by ifIndex and
2         wmanIf2BsSsMacAddress."
3     INDEX        { ifIndex, wmanIf2BsSsPkmAuthMacAddress }
4     ::= { wmanIf2BsSsPkmAuthorizationTable 1 }
5
6     WmanIf2BsSsPkmAuthorizationEntry ::= SEQUENCE {
7         wmanIf2BsSsPkmAuthMacAddress      MacAddress,
8         wmanIf2BsSsPkmCaCertificate       OCTET STRING,
9         wmanIf2BsSsPkmSsCertificate       OCTET STRING,
10        wmanIf2BsSsPkmSaId                INTEGER,
11        wmanIf2BsSsPkmAuthKeySequenceNumber Integer32,
12        wmanIf2BsSsPkmAuthKeyLifetime     Integer32,
13        wmanIf2BsSsPkmAuthRejectError     WmanIf2PkmErrorCode,
14        wmanIf2BsSsPkmAuthInvalidError    WmanIf2PkmErrorCode,
15        wmanIf2BsSsPkmLastAkExpireTime    DateAndTime,
16        wmanIf2BsSsPkmLatestAkExpireTime  DateAndTime,
17        wmanIf2BsSsPkmCertificateStatus    WmanIf2CertificateStat,
18        wmanIf2BsSsPkmAuthReset          INTEGER}
19
20     wmanIf2BsSsPkmAuthMacAddress OBJECT-TYPE
21         SYNTAX      MacAddress
22         MAX-ACCESS  not-accessible
23         STATUS      current
24         DESCRIPTION
25             "The value of this object is the physical address of the SS
26             to which the authorization association applies."
27         ::= { wmanIf2BsSsPkmAuthorizationEntry 1 }
28
29     wmanIf2BsSsPkmCaCertificate OBJECT-TYPE
30         SYNTAX      OCTET STRING (SIZE(0..65535))
31         MAX-ACCESS  read-only
32         STATUS      current
33         DESCRIPTION
34             "SS sends the CA-Certificate in the Auth Info message. It
35             contains an X.509 CA certificate for the manufacturer of
36             the SS. The SS's X.509 user certificate shall have been
37             issued by the CA identified by the X.509 CA certificate."
38         REFERENCE
39             "Table 37 in IEEE Std 802.16-2004"
40         ::= { wmanIf2BsSsPkmAuthorizationEntry 2 }
41
42     wmanIf2BsSsPkmSsCertificate OBJECT-TYPE
43         SYNTAX      OCTET STRING (SIZE(0..65535))
44         MAX-ACCESS  read-only
45         STATUS      current
46         DESCRIPTION
47             "SS sends the SS-Certificate in the Auth Request message.
48             It contains an X.509 SS certificate issued by the SS's
49             manufacturer. The SS's X.509 certificate is a public-key
50             certificate which binds the SS's identifying information
51             to its RSA public key in a verifiable manner. The X.509
52             certificate is digitally signed by the SS's manufacturer,
53             and that signature can be verified by a BS that knows
54             the manufacturer's public key. The manufacturer's public
55             key is placed in an X.509 certification authority (CA)
56             certificate, which in turn is signed by a higher level CA."
57         REFERENCE
58             "Table 28 in IEEE Std 802.16-2004"
59         ::= { wmanIf2BsSsPkmAuthorizationEntry 3 }
60
61     wmanIf2BsSsPkmSaId 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."
3      REFERENCE
4          "Subclause 6.3.2.3.9.2 in IEEE Std 802.16-2004"
5          ::= { wmanIf2BsSsPkmAuthorizationEntry 4 }
6
7      wmanIf2BsSsPkmAuthKeySequenceNumber OBJECT-TYPE
8          SYNTAX      Integer32 (0 .. 15)
9          MAX-ACCESS  read-only
10         STATUS      current
11         DESCRIPTION
12             "This object provides the most recent authorization key
13             sequence number in the Auth Reply message for an SS."
14         REFERENCE
15             "Table 29 in IEEE Std 802.16-2004"
16             ::= { wmanIf2BsSsPkmAuthorizationEntry 5 }
17
18         wmanIf2BsSsPkmAuthKeyLifetime OBJECT-TYPE
19             SYNTAX      Integer32 (86400..6048000)
20             UNITS       "seconds"
21             MAX-ACCESS  read-only
22             STATUS      current
23             DESCRIPTION
24                 "This object defines the lifetime of an authorization
25                 key (AK) the BS assigns to a SS."
26             REFERENCE
27                 "Table 343 in IEEE Std 802.16-2004"
28                 ::= { wmanIf2BsSsPkmAuthorizationEntry 6 }
29
30         wmanIf2BsSsPkmAuthRejectError OBJECT-TYPE
31             SYNTAX      WmanIf2PkmErrorCode
32             MAX-ACCESS  read-only
33             STATUS      current
34             DESCRIPTION
35                 "The Error Code in most recent Authorization Reject message
36                 transmitted to the SS."
37
38                 The valid codes are:
39                     0 - no failure
40                     1 - unauthorized SS
41                     2 - unauthorized SAID
42                     6..11 - permanent authorization failure"
43             REFERENCE
44                 "Table 371, Subclause 11.9.10, in IEEE Std 802.16-2004"
45                 ::= { wmanIf2BsSsPkmAuthorizationEntry 7 }
46
47         wmanIf2BsSsPkmAuthInvalidError OBJECT-TYPE
48             SYNTAX      WmanIf2PkmErrorCode
49             MAX-ACCESS  read-only
50             STATUS      current
51             DESCRIPTION
52                 "The Error Code in most recent Authorization Invalid message
53                 transmitted to the SS."
54
55                 The valid codes are:
56                     0 - no failure
57                     1 - unauthorized SS
58                     3 - unsolicited
59                     4 - invalid key sequence
60                     5 - key request authentication failure"
61
62             REFERENCE
63                 "Table 371, Subclause 11.9.10, in IEEE Std 802.16-2004"
64                 ::= { wmanIf2BsSsPkmAuthorizationEntry 8 }

```

```

1
2 wmanIf2BsSsPkmLastAkExpireTime OBJECT-TYPE
3     SYNTAX      DateAndTime
4     MAX-ACCESS  read-only
5     STATUS      current
6     DESCRIPTION
7         "This object is the time when the last AK expires.
8         wmanIf2BsSsPkmLastAkExpireTime = Time(last AK[Auth Reply])
9         + AK lifetime
10        If this FSM has only one authorization key, then
11        wmanIf2BsSsPkmLastAkExpireTime = the activation of FSM."
12    ::= { wmanIf2BsSsPkmAuthorizationEntry 9 }
13
14 wmanIf2BsSsPkmLatestAkExpireTime OBJECT-TYPE
15     SYNTAX      DateAndTime
16     MAX-ACCESS  read-only
17     STATUS      current
18     DESCRIPTION
19         "This object is the time when the latest AK expires."
20    ::= { wmanIf2BsSsPkmAuthorizationEntry 10 }
21
22 wmanIf2BsSsPkmCertificateStatus OBJECT-TYPE
23     SYNTAX      WmanIf2CertificateStat
24     MAX-ACCESS  read-only
25     STATUS      current
26     DESCRIPTION
27         "Indicate the reason why a SS's certificate is deemed valid
28         or invalid."
29    ::= { wmanIf2BsSsPkmAuthorizationEntry 11 }
30
31 wmanIf2BsSsPkmAuthReset OBJECT-TYPE
32     SYNTAX      INTEGER {noResetRequested(1),
33                    invalidateAuth(2),
34                    sendAuthInvalid(3),
35                    invalidateTeks(4)}
36     MAX-ACCESS  read-write
37     STATUS      current
38     DESCRIPTION
39         "Setting this object to:
40         1 - no reset
41         2 - causes the BS to invalidate the current SS
42         authorization key(s), but not to transmit an
43         Authorization Invalid message nor to invalidate
44         unicast TEKs.
45         3 - causes the BS to invalidate the current SS
46         authorization key(s), and to transmit an
47         Authorization Invalid message to the SS, but not
48         to invalidate unicast TEKs.
49         4 - causes the BS to invalidate the current SS
50         authorization key(s), to transmit an Authorization
51         Invalid message to the SS, and to invalidate all
52         unicast TEKs associated with this SS authorization.
53         Reading this object returns the most-recently-set value
54         of this object, or returns noResetRequested(1) if the
55         object has not been set since the last BS reboot."
56    ::= { wmanIf2BsSsPkmAuthorizationEntry 12 }
57
58 ---- Table wmanIf2BsPkmSecurityCapabilityTable
59 --
60 wmanIf2BsPkmSecurityCapabilityTable OBJECT-TYPE
61     SYNTAX      SEQUENCE OF WmanIf2BsPkmSecurityCapabilityEntry
62     MAX-ACCESS  not-accessible
63     STATUS      current
64     DESCRIPTION

```



```

1           "This table contains the the list of the cryptographic
2           suite(s) an SS supports."
3     REFERENCE
4           "Subclause 11.9.13 in IEEE Std 802.16-2004"
5     ::= { wmanIf2BsPkmV1Objects 4 }
6
7     wmanIf2BsPkmSecurityCapabilityEntry OBJECT-TYPE
8     SYNTAX      WmanIf2BsPkmSecurityCapabilityEntry
9     MAX-ACCESS  not-accessible
10    STATUS      current
11    DESCRIPTION
12      "This table is triple indexed by ifIndex and
13      wmanIf2BsSsSecurityCapIndex."
14    INDEX       { ifIndex,
15                wmanIf2BsPkmSecurityCapIndex }
16    ::= { wmanIf2BsPkmSecurityCapabilityTable 1 }
17
18    WmanIf2BsPkmSecurityCapabilityEntry ::= SEQUENCE {
19      wmanIf2BsPkmSecurityCapIndex      INTEGER,
20      wmanIf2BsPkmScDataEncryptAlgorithm WmanIf2DataEncryptAlgId,
21      wmanIf2BsPkmScDataAuthentAlgorithm WmanIf2DataAuthAlgId,
22      wmanIf2BsPkmScEncryptAlgorithm    WmanIf2TekEncryptAlgId}
23
24    wmanIf2BsPkmSecurityCapIndex OBJECT-TYPE
25    SYNTAX      INTEGER (1 .. 65535)
26    MAX-ACCESS  not-accessible
27    STATUS      current
28    DESCRIPTION
29      "The index value which uniquely identifies an entry
30      in the wmanIf2BsPkmSecurityCapabilityTable"
31    ::= { wmanIf2BsPkmSecurityCapabilityEntry 1 }
32
33    wmanIf2BsPkmScDataEncryptAlgorithm OBJECT-TYPE
34    SYNTAX      WmanIf2DataEncryptAlgId
35    MAX-ACCESS  read-only
36    STATUS      current
37    DESCRIPTION
38      "The value of this object is the data encryption algorithm
39      being utilized."
40    REFERENCE
41      "Table 375, IEEE Std 802.16-2004"
42    ::= { wmanIf2BsPkmSecurityCapabilityEntry 2 }
43
44    wmanIf2BsPkmScDataAuthentAlgorithm OBJECT-TYPE
45    SYNTAX      WmanIf2DataAuthAlgId
46    MAX-ACCESS  read-only
47    STATUS      current
48    DESCRIPTION
49      "The value of this object is the data authentication
50      algorithm being utilized."
51    REFERENCE
52      "Table 376, IEEE Std 802.16-2004"
53    ::= { wmanIf2BsPkmSecurityCapabilityEntry 3 }
54
55    wmanIf2BsPkmScEncryptAlgorithm OBJECT-TYPE
56    SYNTAX      WmanIf2TekEncryptAlgId
57    MAX-ACCESS  read-only
58    STATUS      current
59    DESCRIPTION
60      "The value of this object is the TEK key encryption
61      algorithm being utilized."
62    REFERENCE
63      "Table 377, IEEE Std 802.16-2004"
64    ::= { wmanIf2BsPkmSecurityCapabilityEntry 4 }

```

```

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

```

```

1  wmanIf2BsSsPkmScEncryptAlgorithm OBJECT-TYPE
2      SYNTAX      WmanIf2TekEncryptAlgId
3      MAX-ACCESS  read-only
4      STATUS      current
5      DESCRIPTION
6          "The value of this object is the TEK key encryption
7              algorithm being utilized."
8      REFERENCE
9          "Table 377, IEEE Std 802.16-2004"
10     ::= { wmanIf2BsSsPkmSecurityCapabilityEntry 4 }
11
12 -- Table wmanIf2BsSsPkmTekTable
13 --
14 wmanIf2BsSsPkmTekTable OBJECT-TYPE
15     SYNTAX      SEQUENCE OF WmanIf2BsSsPkmTekEntry
16     MAX-ACCESS  not-accessible
17     STATUS      current
18     DESCRIPTION
19         "This table contains the TEK attributes that are associated
20             with each SAID."
21     ::= { wmanIf2BsPkmV1Objects 6 }
22
23 wmanIf2BsSsPkmTekEntry OBJECT-TYPE
24     SYNTAX      WmanIf2BsSsPkmTekEntry
25     MAX-ACCESS  not-accessible
26     STATUS      current
27     DESCRIPTION
28         "This table is triple indexed by ifIndex,
29             wmanIf2BsSsMacAddress, and wmanIf2BsSsPkmSaidIndex."
30     INDEX      { ifIndex,
31                 wmanIf2BsSsMacAddress,
32                 wmanIf2BsSsPkmSaidIndex }
33     ::= { wmanIf2BsSsPkmTekTable 1 }
34
35 WmanIf2BsSsPkmTekEntry ::= SEQUENCE {
36     wmanIf2BsSsPkmSaidIndex          INTEGER,
37     wmanIf2BsSsPkmSaType             WmanIf2SaType,
38     wmanIf2BsSsPkmTekDataEncryptAlgorithm WmanIf2DataEncryptAlgId,
39     wmanIf2BsSsPkmTekDataAuthAlgorithm WmanIf2DataAuthAlgId,
40     wmanIf2BsSsPkmTekEncryptAlgorithm WmanIf2TekEncryptAlgId,
41     wmanIf2BsSsPkmOlderTekSequenceNumber Integer32,
42     wmanIf2BsSsPkmOlderTekLifetime    Integer32,
43     wmanIf2BsSsPkmNewerTekSequenceNumber Integer32,
44     wmanIf2BsSsPkmNewerTekLifetime   Integer32,
45     wmanIf2BsSsPkmKeyRejectError      WmanIf2PkmErrorCode,
46     wmanIf2BsSsPkmTekInvalidError     WmanIf2PkmErrorCode,
47     wmanIf2BsSsPkmLastTekExpireTime   DateAndTime,
48     wmanIf2BsSsPkmLatestTekExpireTime DateAndTime,
49     wmanIf2BsSsPkmTekReset            TruthValue}
50
51 wmanIf2BsSsPkmSaidIndex OBJECT-TYPE
52     SYNTAX      INTEGER (0 .. 65535)
53     MAX-ACCESS  not-accessible
54     STATUS      current
55     DESCRIPTION
56         "SAID index to the wmanIf2BsSsPkmTekTable."
57     ::= { wmanIf2BsSsPkmTekEntry 1 }
58
59 wmanIf2BsSsPkmSaType OBJECT-TYPE
60     SYNTAX      WmanIf2SaType
61     MAX-ACCESS  read-only
62     STATUS      current
63     DESCRIPTION
64         "SA Type attribute that is included in the Auth Reply

```

```

1         message."
2         ::= { wmanIf2BsSsPkmTekEntry 2 }
3
4 wmanIf2BsSsPkmTekDataEncryptAlgorithm OBJECT-TYPE
5     SYNTAX      WmanIf2DataEncryptAlgId
6     MAX-ACCESS  read-only
7     STATUS      current
8     DESCRIPTION
9         "The data encryption algorithm attribute that is included
10        in the Auth Reply message."
11    REFERENCE
12        "Table 375, IEEE Std 802.16-2004"
13    ::= { wmanIf2BsSsPkmTekEntry 3 }
14
15 wmanIf2BsSsPkmTekDataAuthentAlgorithm OBJECT-TYPE
16     SYNTAX      WmanIf2DataAuthAlgId
17     MAX-ACCESS  read-only
18     STATUS      current
19     DESCRIPTION
20         "The data authentication algorithm attribute that is
21        included in the Auth Reply message."
22    REFERENCE
23        "Table 376, IEEE Std 802.16-2004"
24    ::= { wmanIf2BsSsPkmTekEntry 4 }
25
26 wmanIf2BsSsPkmTekEncryptAlgorithm OBJECT-TYPE
27     SYNTAX      WmanIf2TekEncryptAlgId
28     MAX-ACCESS  read-only
29     STATUS      current
30     DESCRIPTION
31         "The TEK key encryption algorithm attribute that is
32        included in the Auth Reply message."
33    REFERENCE
34        "Table 377, IEEE Std 802.16-2004"
35    ::= { wmanIf2BsSsPkmTekEntry 5 }
36
37 wmanIf2BsSsPkmOlderTekSequenceNumber OBJECT-TYPE
38     SYNTAX      Integer32 (0 .. 3)
39     MAX-ACCESS  read-only
40     STATUS      current
41     DESCRIPTION
42         "At all times the BS maintains two sets of active
43        generations of keying material per SAID. One set
44        corresponds to the 'older' generation of keying material,
45        the second set corresponds to the 'newer' generation of
46        keying material. The newer generation has a key sequence
47        number one greater than (modulo 4) that of the older
48        generation. This object provides the older TEK sequence
49        number in the Key Reply message for an SS."
50    REFERENCE
51        "Subclause 11.9.8 in IEEE Std 802.16-2004"
52    ::= { wmanIf2BsSsPkmTekEntry 6 }
53
54 wmanIf2BsSsPkmOlderTekLifetime OBJECT-TYPE
55     SYNTAX      Integer32 (1800 .. 604800)
56     UNITS       "seconds"
57     MAX-ACCESS  read-only
58     STATUS      current
59     DESCRIPTION
60         "This object provides the older TEK Remaining Lifetime."
61    REFERENCE
62        "Subclause 11.9.8 in IEEE Std 802.16-2004"
63    ::= { wmanIf2BsSsPkmTekEntry 7 }
64

```

```

1  wmanIf2BsSsPkmNewerTekSequenceNumber OBJECT-TYPE
2      SYNTAX      Integer32 (0 .. 3)
3      MAX-ACCESS  read-only
4      STATUS      current
5      DESCRIPTION
6          "This object provides the newer 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     ::= { wmanIf2BsSsPkmTekEntry 8 }
11
12  wmanIf2BsSsPkmNewerTekLifetime 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 newer TEK Remaining Lifetime."
19      REFERENCE
20          "Subclause 11.9.8 in IEEE Std 802.16-2004"
21     ::= { wmanIf2BsSsPkmTekEntry 9 }
22
23  wmanIf2BsSsPkmKeyRejectError OBJECT-TYPE
24      SYNTAX      WmanIf2PkmErrorCode
25      MAX-ACCESS  read-only
26      STATUS      current
27      DESCRIPTION
28          "The Error Code in the most recent Key Reject message sent
29          in response to a Key Request for this SAID.
30
31          The valid error codes are:
32              0 - no failure
33              2 - unauthorized SAID"
34      REFERENCE
35          "IEEE Std 802.16-2004; Table 371"
36     ::= { wmanIf2BsSsPkmTekEntry 10 }
37
38  wmanIf2BsSsPkmTekInvalidError OBJECT-TYPE
39      SYNTAX      WmanIf2PkmErrorCode
40      MAX-ACCESS  read-only
41      STATUS      current
42      DESCRIPTION
43          "The Error Code in the most recent TEK Invalid message sent
44          in association with this SAID.
45
46          The valid error codes are:
47              0 - no failure
48              4 - invalid key sequence"
49      REFERENCE
50          "IEEE Std 802.16-2004; Table 371"
51     ::= { wmanIf2BsSsPkmTekEntry 11 }
52
53  wmanIf2BsSsPkmLastTekExpireTime OBJECT-TYPE
54      SYNTAX      DateAndTime
55      MAX-ACCESS  read-only
56      STATUS      current
57      DESCRIPTION
58          "This object is the time when the last TEK expires.
59          wmanIf2BsSsPkmLastTekExpireTime = Time(last TEK[Key Reply])
60          + TEK lifetime
61          If this FSM has only one authorization key, then
62          wmanIf2BsSsPkmLastTekExpireTime = the activation of FSM."
63     ::= { wmanIf2BsSsPkmTekEntry 12 }
64

```

```
1  wmanIf2BsSsPkmLatestTekExpireTime OBJECT-TYPE
2      SYNTAX      DateAndTime
3      MAX-ACCESS  read-only
4      STATUS      current
5      DESCRIPTION
6          "This object is the time when the latest TEK expires."
7      ::= { wmanIf2BsSsPkmTekEntry 13 }
8
9  wmanIf2BsSsPkmTekReset OBJECT-TYPE
10     SYNTAX      TruthValue
11     MAX-ACCESS  read-write
12     STATUS      current
13     DESCRIPTION
14         "Setting this object to TRUE causes the BS to invalidate
15         the current active TEK(s) (plural due to key transition
16         periods), and to generate a new TEK for the associated
17         SAID; the BS MAY also generate an unsolicited TEK Invalid
18         message, to optimize the TEK synchronization between the BS
19         and the SS. Reading this object always returns FALSE."
20     ::= { wmanIf2BsSsPkmTekEntry 14 }
21
```

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       WmanIf2PkmErrorCode,
30         wmanIf2BsSsPkmV2LastAkExpireTime  DateAndTime,
31         wmanIf2BsSsPkmV2LatestAkExpireTime DateAndTime,
32         wmanIf2BsSsPkmV2CertificateStatus WmanIf2CertificateStat}
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      WmanIf2PkmErrorCode
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      WmanIf2CertificateStat
57     MAX-ACCESS read-only
58     STATUS current
59     DESCRIPTION
60         "Indicate the reason why a SS's certificate is deemed valid
61         or invalid."
62    ::= { wmanIf2BsSsPkmV2RsaAuthEntry 12 }
63
64 --

```

```

1  -- Table wmanIf2BsSsPkmV2TekTable
2  --
3  wmanIf2BsSsPkmV2TekTable OBJECT-TYPE
4      SYNTAX          SEQUENCE OF WmanIf2BsSsPkmV2TekEntry
5      MAX-ACCESS      not-accessible
6      STATUS          current
7      DESCRIPTION
8          "This table contains the TEK attributes that are associated
9          with each SAID."
10     ::= { wmanIf2BsPkmV2Objects 3 }
11
12  wmanIf2BsSsPkmV2TekEntry OBJECT-TYPE
13      SYNTAX          WmanIf2BsSsPkmV2TekEntry
14      MAX-ACCESS      not-accessible
15      STATUS          current
16      DESCRIPTION
17          "This table is triple indexed by ifIndex,
18          wmanIf2BsSsMacAddress, and wmanIf2BsSsPkmSaidIndex."
19      INDEX           { ifIndex,
20                      wmanIf2BsSsMacAddress,
21                      wmanIf2BsSsPkmV2SaidIndex }
22     ::= { wmanIf2BsSsPkmV2TekTable 1 }
23
24  WmanIf2BsSsPkmV2TekEntry ::= SEQUENCE {
25      wmanIf2BsSsPkmV2SaidIndex          INTEGER,
26      wmanIf2BsSsPkmV2SaType             WmanIf2SaType,
27      wmanIf2BsSsPkmV2OlderTekSequenceNumber Integer32,
28      wmanIf2BsSsPkmV2OlderTekLifetime   Integer32,
29      wmanIf2BsSsPkmV2NewerTekSequenceNumber Integer32,
30      wmanIf2BsSsPkmV2NewerTekLifetime   Integer32,
31      wmanIf2BsSsPkmV2AuthInvalidError   WmanIf2PkmErrorCode,
32      wmanIf2BsSsPkmV2LastTekExpireTime  DateAndTime,
33      wmanIf2BsSsPkmV2LatestTekExpireTime DateAndTime}
34
35  wmanIf2BsSsPkmV2SaidIndex OBJECT-TYPE
36      SYNTAX          INTEGER (0 .. 65535)
37      MAX-ACCESS      not-accessible
38      STATUS          current
39      DESCRIPTION
40          "SAID index to the wmanIf2BsSsPkmV2TekTable."
41     ::= { wmanIf2BsSsPkmV2TekEntry 1 }
42
43  wmanIf2BsSsPkmV2SaType OBJECT-TYPE
44      SYNTAX          WmanIf2SaType
45      MAX-ACCESS      read-only
46      STATUS          current
47      DESCRIPTION
48          "SA Type attribute that is included in the Auth Reply
49          message."
50     ::= { wmanIf2BsSsPkmV2TekEntry 2 }
51
52  wmanIf2BsSsPkmV2OlderTekSequenceNumber OBJECT-TYPE
53      SYNTAX          Integer32 (0 .. 3)
54      MAX-ACCESS      read-only
55      STATUS          current
56      DESCRIPTION
57          "At all times the BS maintains two sets of active
58          generations of keying material per SAID. One set
59          corresponds to the 'older' generation of keying material,
60          the second set corresponds to the 'newer' generation of
61          keying material. The newer generation has a key sequence
62          number one greater than (modulo 4) that of the older
63          generation. This object provides the older TEK sequence
64          number in the Key Reply message for an SS."

```

```

1      REFERENCE
2          "Subclause 11.9.8 in IEEE Std 802.16-2004"
3      ::= { wmanIf2BsSsPkmV2TekEntry 3 }
4
5      wmanIf2BsSsPkmV2OlderTekLifetime OBJECT-TYPE
6          SYNTAX      Integer32 (1800 .. 604800)
7          UNITS       "seconds"
8          MAX-ACCESS  read-only
9          STATUS      current
10         DESCRIPTION
11             "This object provides the older TEK Remaining Lifetime."
12         REFERENCE
13             "Subclause 11.9.8 in IEEE Std 802.16-2004"
14         ::= { wmanIf2BsSsPkmV2TekEntry 4 }
15
16         wmanIf2BsSsPkmV2NewerTekSequenceNumber OBJECT-TYPE
17             SYNTAX      Integer32 (0 .. 3)
18             MAX-ACCESS  read-only
19             STATUS      current
20             DESCRIPTION
21                 "This object provides the newer TEK sequence
22                 number in the Key Reply message for an SS."
23             REFERENCE
24                 "Subclause 11.9.8 in IEEE Std 802.16-2004"
25             ::= { wmanIf2BsSsPkmV2TekEntry 5 }
26
27         wmanIf2BsSsPkmV2NewerTekLifetime OBJECT-TYPE
28             SYNTAX      Integer32 (1800 .. 604800)
29             UNITS       "seconds"
30             MAX-ACCESS  read-only
31             STATUS      current
32             DESCRIPTION
33                 "This object provides the newer TEK Remaining Lifetime."
34             REFERENCE
35                 "Subclause 11.9.8 in IEEE Std 802.16-2004"
36             ::= { wmanIf2BsSsPkmV2TekEntry 6 }
37
38         wmanIf2BsSsPkmV2AuthInvalidError OBJECT-TYPE
39             SYNTAX      WmanIf2PkmErrorCode
40             MAX-ACCESS  read-only
41             STATUS      current
42             DESCRIPTION
43                 "BS returns Authorization Invalid message if an authorization
44                 invlaid error is detected.
45
46                 Note that the BS may log the Display-String attribute and
47                 Authorization invalid error in wmanIfDevMib."
48             REFERENCE
49                 "Subclause 11.9.10 in IEEE Std 802.16-2004"
50             ::= { wmanIf2BsSsPkmV2TekEntry 7 }
51
52         wmanIf2BsSsPkmV2LastTekExpireTime OBJECT-TYPE
53             SYNTAX      DateAndTime
54             MAX-ACCESS  read-only
55             STATUS      current
56             DESCRIPTION
57                 "This object is the time when the last TEK expires.
58                 wmanIf2BsSsPkmV2LastTekExpireTime = Time(last TEK[Key Reply])
59                 + TEK lifetime
60                 If this FSM has only one authorization key, then
61                 wmanIf2BsSsPkmV2LastTekExpireTime = the activation of FSM."
62             ::= { wmanIf2BsSsPkmV2TekEntry 8 }
63
64         wmanIf2BsSsPkmV2LatestTekExpireTime OBJECT-TYPE

```

```
1          SYNTAX      DateAndTime
2          MAX-ACCESS  read-only
3          STATUS      current
4          DESCRIPTION
5              "This object is the time when the latest TEK expires."
6          ::= { wmanIf2BsSsPkmV2TekEntry 9 }
7
```

1 2.5 wmanIf2SsPkmObjects ASN.1 Code Change

2 13.2 ASN.1 Definitions of MIB Modules

3 13.2.3 wmanIf2Mib

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

```

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 wmanIf2SsPkmAttributeTable
17 --
18 wmanIf2SsPkmAttributeTable OBJECT-TYPE
19     SYNTAX          SEQUENCE OF WmanIf2SsPkmAttributeEntry
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 wmanIf2SsPkmAttributeEntry OBJECT-TYPE
30     SYNTAX          WmanIf2SsPkmAttributeEntry
31     MAX-ACCESS     not-accessible
32     STATUS          current
33     DESCRIPTION
34         "The table is indexed by ifIndex."
35     INDEX           { ifIndex }
36     ::= { wmanIf2SsPkmAttributeTable 1 }
37
38 WmanIf2SsPkmAttributeEntry ::= 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     ::= { wmanIf2SsPkmAttributeEntry 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     ::= { wmanIf2SsPkmAttributeEntry 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     ::= { wmanIf2SsPkmAttributeEntry 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     ::= { wmanIf2SsPkmAttributeEntry 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     ::= { wmanIf2SsPkmAttributeEntry 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      ::= { wmanIf2SsPkmAttributeEntry 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         ::= { wmanIf2SsPkmAttributeEntry 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         wmanIf2SsPkmAuthRejectError     WmanIf2PkmErrorCode,
49         wmanIf2SsPkmAuthInvalidError    WmanIf2PkmErrorCode,
50         wmanIf2SsPkmLastAkExpireTime    DateAndTime,
51         wmanIf2SsPkmLatestAkExpireTime  DateAndTime,
52         wmanIf2SsPkmAuthReset           TruthValue}
53
54     wmanIf2SsPkmCaCertificate OBJECT-TYPE
55         SYNTAX      OCTET STRING (SIZE(0..65535))
56         MAX-ACCESS  read-only
57         STATUS      current
58         DESCRIPTION
59             "SS sends the CA-Certificate in the Auth Info message. It
60             contains an X.509 CA certificate for the manufacturer of
61             the SS. The SS's X.509 user certificate shall have been
62             issued by the CA identified by the X.509 CA certificate."
63         REFERENCE
64             "Table 37 in IEEE Std 802.16-2004"

```

```

1      ::= { wmanIf2SsPkmAuthorizationEntry 1 }
2
3      wmanIf2SsPkmSsCertificate OBJECT-TYPE
4          SYNTAX      OCTET STRING (SIZE(0..65535))
5          MAX-ACCESS  read-only
6          STATUS      current
7          DESCRIPTION
8              "SS sends the SS-Certificate in the Auth Request message.
9              It contains an X.509 SS certificate issued by the SS's
10             manufacturer. The SS's X.509 certificate is a public-key
11             certificate which binds the SS's identifying information
12             to its RSA public key in a verifiable manner. The X.509
13             certificate is digitally signed by the SS's manufacturer,
14             and that signature can be verified by a BS that knows
15             the manufacturer's public key. The manufacturer's public
16             key is placed in an X.509 certification authority (CA)
17             certificate, which in turn is signed by a higher level CA."
18          REFERENCE
19              "Table 28 in IEEE Std 802.16-2004"
20          ::= { wmanIf2SsPkmAuthorizationEntry 2 }
21
22      wmanIf2SsPkmSaId OBJECT-TYPE
23          SYNTAX      INTEGER (0..65535)
24          MAX-ACCESS  read-only
25          STATUS      current
26          DESCRIPTION
27              "SS's primary SAID equal to the Basic CID."
28          REFERENCE
29              "Subclause 6.3.2.3.9.2 in IEEE Std 802.16-2004"
30          ::= { wmanIf2SsPkmAuthorizationEntry 3 }
31
32      wmanIf2SsPkmAuthKeySequenceNumber OBJECT-TYPE
33          SYNTAX      Integer32 (0 .. 15)
34          MAX-ACCESS  read-only
35          STATUS      current
36          DESCRIPTION
37              "This object provides the most recent authorization key
38             sequence number in the Auth Reply message for an SS."
39          REFERENCE
40              "Table 29 in IEEE Std 802.16-2004"
41          ::= { wmanIf2SsPkmAuthorizationEntry 4 }
42
43      wmanIf2SsPkmAuthKeyLifetime OBJECT-TYPE
44          SYNTAX      Integer32 (86400..6048000)
45          UNITS       "seconds"
46          MAX-ACCESS  read-only
47          STATUS      current
48          DESCRIPTION
49              "This object defines the lifetime of an authorization
50             key (AK) the BS assigns to a SS."
51          REFERENCE
52              "Table 343 in IEEE Std 802.16-2004"
53          ::= { wmanIf2SsPkmAuthorizationEntry 5 }
54
55      wmanIf2SsPkmAuthRejectError OBJECT-TYPE
56          SYNTAX      WmanIf2PkmErrorCode
57          MAX-ACCESS  read-only
58          STATUS      current
59          DESCRIPTION
60              "The Error Code in most recent Authorization Reject message
61             received from the BS.
62
63             The valid codes are:
64             0 - no failure

```

```

1           1 - unauthorized SS
2           2 - unauthorized SAID
3           6..11 - permanent authorization failure"
4 REFERENCE
5           "Table 371, Subclause 11.9.10, in IEEE Std 802.16-2004"
6 ::= { wmanIf2SsPkmAuthorizationEntry 6 }
7
8 wmanIf2SsPkmAuthInvalidError OBJECT-TYPE
9 SYNTAX      WmanIf2PkmErrorCode
10 MAX-ACCESS  read-only
11 STATUS      current
12 DESCRIPTION
13     "The Error Code in most recent Authorization Invalid message
14     received from the BS.
15
16     The valid codes are:
17     0 - no failure
18     1 - unauthorized SS
19     3 - unsolicited
20     4 - invalid key sequence
21     5 - key request authentication failure"
22
23 REFERENCE
24     "Table 371, Subclause 11.9.10, in IEEE Std 802.16-2004"
25 ::= { wmanIf2SsPkmAuthorizationEntry 7 }
26
27 wmanIf2SsPkmLastAkExpireTime OBJECT-TYPE
28 SYNTAX      DateAndTime
29 MAX-ACCESS  read-only
30 STATUS      current
31 DESCRIPTION
32     "This object is the time when the last AK expires.
33     wmanIf2SsPkmLastAkExpireTime = Time(last AK[Auth Reply])
34     + AK lifetime
35     If this FSM has only one authorization key, then
36     wmanIf2SsPkmLastAkExpireTime = the activation of FSM."
37 ::= { wmanIf2SsPkmAuthorizationEntry 8 }
38
39 wmanIf2SsPkmLatestAkExpireTime OBJECT-TYPE
40 SYNTAX      DateAndTime
41 MAX-ACCESS  read-only
42 STATUS      current
43 DESCRIPTION
44     "This object is the time when the latest AK expires."
45 ::= { wmanIf2SsPkmAuthorizationEntry 9 }
46
47 wmanIf2SsPkmAuthReset OBJECT-TYPE
48 SYNTAX      TruthValue
49 MAX-ACCESS  read-write
50 STATUS      current
51 DESCRIPTION
52     "Setting this object to TRUE generates a Reauthorize event
53     in the authorization FSM. Reading this object always
54     returns FALSE."
55 ::= { wmanIf2SsPkmAuthorizationEntry 10 }
56
57 --
58 -- Table wmanIf2SsPkmSecurityCapabilityTable
59 --
60 wmanIf2SsPkmSecurityCapabilityTable OBJECT-TYPE
61 SYNTAX      SEQUENCE OF WmanIf2SsPkmSecurityCapabilityEntry
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 ::= { wmanIf2SsPkmV1Objects 3 }
7
8 wmanIf2SsPkmSecurityCapabilityEntry OBJECT-TYPE
9 SYNTAX      WmanIf2SsPkmSecurityCapabilityEntry
10 MAX-ACCESS not-accessible
11 STATUS      current
12 DESCRIPTION
13      "This table is indexed by wmanIf2SsSecurityCapIndex."
14 INDEX       { wmanIf2SsPkmSecurityCapIndex }
15 ::= { wmanIf2SsPkmSecurityCapabilityTable 1 }
16
17 WmanIf2SsPkmSecurityCapabilityEntry ::= SEQUENCE {
18     wmanIf2SsPkmSecurityCapIndex      INTEGER,
19     wmanIf2SsPkmScDataEncryptAlgorithm WmanIf2DataEncryptAlgId,
20     wmanIf2SsPkmScDataAuthentAlgorithm WmanIf2DataAuthAlgId,
21     wmanIf2SsPkmScEncryptAlgorithm    WmanIf2TekEncryptAlgId}
22
23 wmanIf2SsPkmSecurityCapIndex OBJECT-TYPE
24 SYNTAX      INTEGER (1 .. 65535)
25 MAX-ACCESS not-accessible
26 STATUS      current
27 DESCRIPTION
28      "The index value which uniquely identifies an entry
29      in the wmanIf2SsPkmSecurityCapabilityTable"
30 ::= { wmanIf2SsPkmSecurityCapabilityEntry 1 }
31
32 wmanIf2SsPkmScDataEncryptAlgorithm OBJECT-TYPE
33 SYNTAX      WmanIf2DataEncryptAlgId
34 MAX-ACCESS read-only
35 STATUS      current
36 DESCRIPTION
37      "The value of this object is the data encryption algorithm
38      being utilized."
39 REFERENCE
40      "Table 375, IEEE Std 802.16-2004"
41 ::= { wmanIf2SsPkmSecurityCapabilityEntry 2 }
42
43 wmanIf2SsPkmScDataAuthentAlgorithm OBJECT-TYPE
44 SYNTAX      WmanIf2DataAuthAlgId
45 MAX-ACCESS read-only
46 STATUS      current
47 DESCRIPTION
48      "The value of this object is the data authentication
49      algorithm being utilized."
50 REFERENCE
51      "Table 376, IEEE Std 802.16-2004"
52 ::= { wmanIf2SsPkmSecurityCapabilityEntry 3 }
53
54 wmanIf2SsPkmScEncryptAlgorithm OBJECT-TYPE
55 SYNTAX      WmanIf2TekEncryptAlgId
56 MAX-ACCESS read-only
57 STATUS      current
58 DESCRIPTION
59      "The value of this object is the TEK key encryption
60      algorithm being utilized."
61 REFERENCE
62      "Table 377, IEEE Std 802.16-2004"
63 ::= { wmanIf2SsPkmSecurityCapabilityEntry 4 }
64

```

```

1  --
2  -- Table wmanIf2SsPkmTekTable
3  --
4  wmanIf2SsPkmTekTable OBJECT-TYPE
5      SYNTAX      SEQUENCE OF WmanIf2SsPkmTekEntry
6      MAX-ACCESS  not-accessible
7      STATUS      current
8      DESCRIPTION
9          "This table contains the TEK attributes that are associated
10         with each SAID."
11         ::= { wmanIf2SsPkmV1Objects 4 }
12
13  wmanIf2SsPkmTekEntry OBJECT-TYPE
14      SYNTAX      WmanIf2SsPkmTekEntry
15      MAX-ACCESS  not-accessible
16      STATUS      current
17      DESCRIPTION
18          "This table is double indexed by ifIndex and
19         wmanIf2SsSaidIndex."
20      INDEX       { ifIndex, wmanIf2SsPkmSaidIndex }
21      ::= { wmanIf2SsPkmTekTable 1 }
22
23  WmanIf2SsPkmTekEntry ::= SEQUENCE {
24      wmanIf2SsPkmSaidIndex          INTEGER,
25      wmanIf2SsPkmSaType             WmanIf2SaType,
26      wmanIf2SsPkmTekDataEncryptAlgorithm WmanIf2DataEncryptAlgId,
27      wmanIf2SsPkmTekDataAuthentAlgorithm WmanIf2DataAuthAlgId,
28      wmanIf2SsPkmTekEncryptAlgorithm  WmanIf2TekEncryptAlgId,
29      wmanIf2SsPkmOlderTekSequenceNumber Integer32,
30      wmanIf2SsPkmOlderTekLifetime     Integer32,
31      wmanIf2SsPkmNewerTekSequenceNumber Integer32,
32      wmanIf2SsPkmNewerTekLifetime     Integer32,
33      wmanIf2SsPkmKeyRejectError       WmanIf2PkmErrorCode,
34      wmanIf2SsPkmTekInvalidError      WmanIf2PkmErrorCode,
35      wmanIf2SsPkmLastTekExpireTime    DateAndTime,
36      wmanIf2SsPkmLatestTekExpireTime  DateAndTime,
37      wmanIf2SsPkmTekState             WmanIf2TekState}
38
39  wmanIf2SsPkmSaidIndex OBJECT-TYPE
40      SYNTAX      INTEGER (0 .. 65535)
41      MAX-ACCESS  not-accessible
42      STATUS      current
43      DESCRIPTION
44          "SAID index to the wmanIf2SsPkmSaDescriptorTable."
45      ::= { wmanIf2SsPkmTekEntry 1 }
46
47  wmanIf2SsPkmSaType OBJECT-TYPE
48      SYNTAX      WmanIf2SaType
49      MAX-ACCESS  read-only
50      STATUS      current
51      DESCRIPTION
52          "SA Type attribute that is included in the Auth Reply
53         message."
54      ::= { wmanIf2SsPkmTekEntry 2 }
55
56  wmanIf2SsPkmTekDataEncryptAlgorithm OBJECT-TYPE
57      SYNTAX      WmanIf2DataEncryptAlgId
58      MAX-ACCESS  read-only
59      STATUS      current
60      DESCRIPTION
61          "The data encryption algorithm attribute that is included
62         in the Auth Reply message."
63      REFERENCE
64          "Table 375, IEEE Std 802.16-2004"

```

```

1      ::= { wmanIf2SsPkmTekEntry 3 }
2
3      wmanIf2SsPkmTekDataAuthentAlgorithm OBJECT-TYPE
4          SYNTAX      WmanIf2DataAuthAlgId
5          MAX-ACCESS  read-only
6          STATUS      current
7          DESCRIPTION
8              "The data authentication algorithm attribute that is
9              included in the Auth Reply message."
10         REFERENCE
11             "Table 376, IEEE Std 802.16-2004"
12         ::= { wmanIf2SsPkmTekEntry 4 }
13
14         wmanIf2SsPkmTekEncryptAlgorithm OBJECT-TYPE
15             SYNTAX      WmanIf2TekEncryptAlgId
16             MAX-ACCESS  read-only
17             STATUS      current
18             DESCRIPTION
19                 "The TEK key encryption algorithm attribute that is
20                 included in the Auth Reply message."
21             REFERENCE
22                 "Table 377, IEEE Std 802.16-2004"
23             ::= { wmanIf2SsPkmTekEntry 5 }
24
25         wmanIf2SsPkmOlderTekSequenceNumber OBJECT-TYPE
26             SYNTAX      Integer32 (0 .. 3)
27             MAX-ACCESS  read-only
28             STATUS      current
29             DESCRIPTION
30                 "At all times the BS maintains two sets of active
31                 generations of keying material per SAID. One set
32                 corresponds to the 'older' generation of keying material,
33                 the second set corresponds to the 'newer' generation of
34                 keying material. The newer generation has a key sequence
35                 number one greater than (modulo 4) that of the older
36                 generation. This object provides the older TEK sequence
37                 number in the Key Reply message for an SS."
38             REFERENCE
39                 "Subclause 11.9.8 in IEEE Std 802.16-2004"
40             ::= { wmanIf2SsPkmTekEntry 6 }
41
42         wmanIf2SsPkmOlderTekLifetime OBJECT-TYPE
43             SYNTAX      Integer32 (1800 .. 604800)
44             UNITS      "seconds"
45             MAX-ACCESS  read-only
46             STATUS      current
47             DESCRIPTION
48                 "This object provides the older TEK Remaining Lifetime."
49             REFERENCE
50                 "Subclause 11.9.8 in IEEE Std 802.16-2004"
51             ::= { wmanIf2SsPkmTekEntry 7 }
52
53         wmanIf2SsPkmNewerTekSequenceNumber OBJECT-TYPE
54             SYNTAX      Integer32 (0 .. 3)
55             MAX-ACCESS  read-only
56             STATUS      current
57             DESCRIPTION
58                 "This object provides the newer TEK sequence
59                 number in the Key Reply message for an SS."
60             REFERENCE
61                 "Subclause 11.9.8 in IEEE Std 802.16-2004"
62             ::= { wmanIf2SsPkmTekEntry 8 }
63
64         wmanIf2SsPkmNewerTekLifetime OBJECT-TYPE

```

```

1      SYNTAX      Integer32 (1800 .. 604800)
2      UNITS       "seconds"
3      MAX-ACCESS  read-only
4      STATUS      current
5      DESCRIPTION
6          "This object provides the newer TEK Remaining Lifetime."
7      REFERENCE
8          "Subclause 11.9.8 in IEEE Std 802.16-2004"
9      ::= { wmanIf2SsPkmTekEntry 9 }
10
11     wmanIf2SsPkmKeyRejectError OBJECT-TYPE
12         SYNTAX      WmanIf2PkmErrorCode
13         MAX-ACCESS  read-only
14         STATUS      current
15         DESCRIPTION
16             "The Error Code in the most recent Key Reject message
17             received from the BS.
18
19             The valid error codes are:
20                 0 - no failure
21                 2 - unauthorized SAID"
22         REFERENCE
23             "IEEE Std 802.16-2004; Table 371"
24         ::= { wmanIf2SsPkmTekEntry 10 }
25
26     wmanIf2SsPkmTekInvalidError OBJECT-TYPE
27         SYNTAX      WmanIf2PkmErrorCode
28         MAX-ACCESS  read-only
29         STATUS      current
30         DESCRIPTION
31             "The Error Code in the most recent TEK Invalid message
32             received from the BS.
33
34             The valid error codes are:
35                 0 - no failure
36                 4 - invalid key sequence"
37         REFERENCE
38             "IEEE Std 802.16-2004; Table 371"
39         ::= { wmanIf2SsPkmTekEntry 11 }
40
41     wmanIf2SsPkmLastTekExpireTime OBJECT-TYPE
42         SYNTAX      DateAndTime
43         MAX-ACCESS  read-only
44         STATUS      current
45         DESCRIPTION
46             "This object is the time when the last TEK expires.
47             wmanIf2SsPkmLastTekExpireTime = Time(last TEK[Key Reply])
48             + TEK lifetime
49             If this FSM has only one authorization key, then
50             wmanIf2SsPkmLastTekExpireTime = the activation of FSM."
51         ::= { wmanIf2SsPkmTekEntry 12 }
52
53     wmanIf2SsPkmLatestTekExpireTime OBJECT-TYPE
54         SYNTAX      DateAndTime
55         MAX-ACCESS  read-only
56         STATUS      current
57         DESCRIPTION
58             "This object is the time when the latest TEK expires."
59         ::= { wmanIf2SsPkmTekEntry 13 }
60
61     wmanIf2SsPkmTekState OBJECT-TYPE
62         SYNTAX      WmanIf2TekState
63         MAX-ACCESS  read-only
64         STATUS      current

```

```
1      DESCRIPTION
2          "The value of this object is the state of the indicated TEK
3          FSM. The start(1) state indicates that FSM is in its
4          initial state."
5      ::= { wmanIf2SsPkmTekEntry 14 }
6
```


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 wmanIf2SsPkmV2AttributeTable
11 --
12 wmanIf2SsPkmV2AttributeTable OBJECT-TYPE
13     SYNTAX      SEQUENCE OF WmanIf2SsPkmV2AttributeEntry
14     MAX-ACCESS  not-accessible
15     STATUS      current
16     DESCRIPTION
17         "This table contains the PKM attributes that are needed
18         to PKM operation."
19     REFERENCE
20         "Table 343 in IEEE Std 802.16-2004 and 802.16e-2005"
21     ::= { wmanIf2SsPkmV2Objects 1 }
22
23 wmanIf2SsPkmV2AttributeEntry OBJECT-TYPE
24     SYNTAX      WmanIf2SsPkmV2AttributeEntry
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     ::= { wmanIf2SsPkmV2AttributeTable 1 }
33
34 WmanIf2SsPkmV2AttributeEntry ::= 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     ::= { wmanIf2SsPkmV2AttributeEntry 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           ::= { wmanIf2SsPkmV2AttributeEntry 2 }
7
```

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          ::= { wmanIf2SsPkmV2AttributeEntry 3 }
20
```

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          ::= { wmanIf2SsPkmV2AttributeEntry 4 }
32
```

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          ::= { wmanIf2SsPkmV2AttributeEntry 5 }
45
```

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          ::= { wmanIf2SsPkmV2AttributeEntry 6 }
57
```

```

58          --
59          -- Table wmanIf2SsPkmV2RsaAuthTable
60          --
```

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       WmanIf2PkmErrorCode,
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      WmanIf2PkmErrorCode
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      REFERENCE
3          "Subclause 11.9.10 in IEEE Std 802.16-2004"
4      ::= { wmanIf2SsPkmV2RsaAuthEntry 8 }
5
6  wmanIf2SsPkmV2LastAkExpireTime OBJECT-TYPE
7      SYNTAX      DateAndTime
8      MAX-ACCESS  read-only
9      STATUS      current
10     DESCRIPTION
11         "This object is the time when the last AK expires.
12         wmanIf2SsPkmV2LastAkExpireTime = Time(last AK[RSA-Reply])
13         + AK lifetime
14         If this FSM has only one authorization key, then
15         wmanIf2SsPkmV2LastAkExpireTime = the activation of FSM."
16     ::= { wmanIf2SsPkmV2RsaAuthEntry 9 }
17
18  wmanIf2SsPkmV2LatestAkExpireTime OBJECT-TYPE
19      SYNTAX      DateAndTime
20      MAX-ACCESS  read-only
21      STATUS      current
22      DESCRIPTION
23         "This object is the time when the latest AK expires."
24     ::= { wmanIf2SsPkmV2RsaAuthEntry 10 }
25
26  --
27  -- Table wmanIf2SsPkmV2TekTable
28  --
29  wmanIf2SsPkmV2TekTable OBJECT-TYPE
30      SYNTAX      SEQUENCE OF WmanIf2SsPkmV2TekEntry
31      MAX-ACCESS  not-accessible
32      STATUS      current
33      DESCRIPTION
34         "This table contains the TEK attributes that are associated
35         with each SAID."
36     ::= { wmanIf2SsPkmV2Objects 3 }
37
38  wmanIf2SsPkmV2TekEntry OBJECT-TYPE
39      SYNTAX      WmanIf2SsPkmV2TekEntry
40      MAX-ACCESS  not-accessible
41      STATUS      current
42      DESCRIPTION
43         "This table is double indexed by ifIndex and
44         wmanIf2SsPkmSaidIndex."
45      INDEX      { ifIndex,
46                 wmanIf2SsPkmV2SaidIndex }
47     ::= { wmanIf2SsPkmV2TekTable 1 }
48
49  WmanIf2SsPkmV2TekEntry ::= SEQUENCE {
50      wmanIf2SsPkmV2SaidIndex          INTEGER,
51      wmanIf2SsPkmV2SaType             WmanIf2SaType,
52      wmanIf2SsPkmV2OlderTekSequenceNumber Integer32,
53      wmanIf2SsPkmV2OlderTekLifetime   Integer32,
54      wmanIf2SsPkmV2NewerTekSequenceNumber Integer32,
55      wmanIf2SsPkmV2NewerTekLifetime   Integer32,
56      wmanIf2SsPkmV2AuthInvalidError   WmanIf2PkmErrorCode,
57      wmanIf2SsPkmV2LastTekExpireTime  DateAndTime,
58      wmanIf2SsPkmV2LatestTekExpireTime DateAndTime}
59
60  wmanIf2SsPkmV2SaidIndex OBJECT-TYPE
61      SYNTAX      INTEGER (0 .. 65535)
62      MAX-ACCESS  not-accessible
63      STATUS      current
64      DESCRIPTION

```

```

1         "SAID index to the wmanIf2SsPkmV2TekTable."
2         ::= { wmanIf2SsPkmV2TekEntry 1 }
3
4 wmanIf2SsPkmV2SaType OBJECT-TYPE
5     SYNTAX      WmanIf2SaType
6     MAX-ACCESS  read-only
7     STATUS      current
8     DESCRIPTION
9         "SA Type attribute that is included in the Auth Reply
10        message."
11        ::= { wmanIf2SsPkmV2TekEntry 2 }
12
13 wmanIf2SsPkmV2OlderTekSequenceNumber OBJECT-TYPE
14     SYNTAX      Integer32 (0 .. 3)
15     MAX-ACCESS  read-only
16     STATUS      current
17     DESCRIPTION
18         "At all times the BS maintains two sets of active
19        generations of keying material per SAID. One set
20        corresponds to the 'older' generation of keying material,
21        the second set corresponds to the 'newer' generation of
22        keying material. The newer generation has a key sequence
23        number one greater than (modulo 4) that of the older
24        generation. This object provides the older TEK sequence
25        number in the Key Reply message for an SS."
26     REFERENCE
27         "Subclause 11.9.8 in IEEE Std 802.16-2004"
28     ::= { wmanIf2SsPkmV2TekEntry 3 }
29
30 wmanIf2SsPkmV2OlderTekLifetime OBJECT-TYPE
31     SYNTAX      Integer32 (1800 .. 604800)
32     UNITS       "seconds"
33     MAX-ACCESS  read-only
34     STATUS      current
35     DESCRIPTION
36         "This object provides the older TEK Remaining Lifetime."
37     REFERENCE
38         "Subclause 11.9.8 in IEEE Std 802.16-2004"
39     ::= { wmanIf2SsPkmV2TekEntry 4 }
40
41 wmanIf2SsPkmV2NewerTekSequenceNumber OBJECT-TYPE
42     SYNTAX      Integer32 (0 .. 3)
43     MAX-ACCESS  read-only
44     STATUS      current
45     DESCRIPTION
46         "This object provides the newer TEK sequence
47        number in the Key Reply message for an SS."
48     REFERENCE
49         "Subclause 11.9.8 in IEEE Std 802.16-2004"
50     ::= { wmanIf2SsPkmV2TekEntry 5 }
51
52 wmanIf2SsPkmV2NewerTekLifetime OBJECT-TYPE
53     SYNTAX      Integer32 (1800 .. 604800)
54     UNITS       "seconds"
55     MAX-ACCESS  read-only
56     STATUS      current
57     DESCRIPTION
58         "This object provides the newer TEK Remaining Lifetime."
59     REFERENCE
60         "Subclause 11.9.8 in IEEE Std 802.16-2004"
61     ::= { wmanIf2SsPkmV2TekEntry 6 }
62
63 wmanIf2SsPkmV2AuthInvalidError OBJECT-TYPE
64     SYNTAX      WmanIf2PkmErrorCode

```

```

1         MAX-ACCESS  read-only
2         STATUS      current
3         DESCRIPTION
4             "BS returns Authorization Invalid message if an authorization
5             invlaid error is detected."
6         REFERENCE
7             "Subclause 11.9.10 in IEEE Std 802.16-2004"
8         ::= { wmanIf2SsPkmV2TekEntry 7 }
9
10        wmanIf2SsPkmV2LastTekExpireTime OBJECT-TYPE
11            SYNTAX      DateAndTime
12            MAX-ACCESS  read-only
13            STATUS      current
14            DESCRIPTION
15                "This object is the time when the last TEK expires.
16                 wmanIf2SsPkmV2LastTekExpireTime = Time(last TEK[Key Reply])
17                 + TEK lifetime
18                 If this FSM has only one authorization key, then
19                 wmanIf2SsPkmV2LastTekExpireTime = the activation of FSM."
20            ::= { wmanIf2SsPkmV2TekEntry 8 }
21
22        wmanIf2SsPkmV2LatestTekExpireTime OBJECT-TYPE
23            SYNTAX      DateAndTime
24            MAX-ACCESS  read-only
25            STATUS      current
26            DESCRIPTION
27                "This object is the time when the latest TEK expires."
28            ::= { wmanIf2SsPkmV2TekEntry 9 }
29
30
31
32
33
34
35
36
37
38
39
40

```

