## Proposed Changes to IEEE802.11d1

1. Section 1.4, References: Add; IEEE Std 802.10f-1993, Secure Data Exchange (SDE) Sublayer Management (Subclause 2.8).

2. Section 2.4.3.1, Authentication: Under examples of a C/R exchange for a password based system, add to the challenge a timestamp and have the response be a "hash" of the timestamp and the password. Rational: In a wireless system passwords must not be sent unprotected, any promiscuous listener could obtain the password and use it to become authenticated. Adding a timestamp will prevent replay attacks against the system. This may also be accomplished by encrypting the response using the Wire Equivalent Privacy (WEP) algorithm described in section 5.4.

3. Section 3.1.1.3, Security services:

**Replace existing Figure 3-1 with the figure below.** This is a updated figure provided by 802.10 which I believe is easier to understand and more accurate.

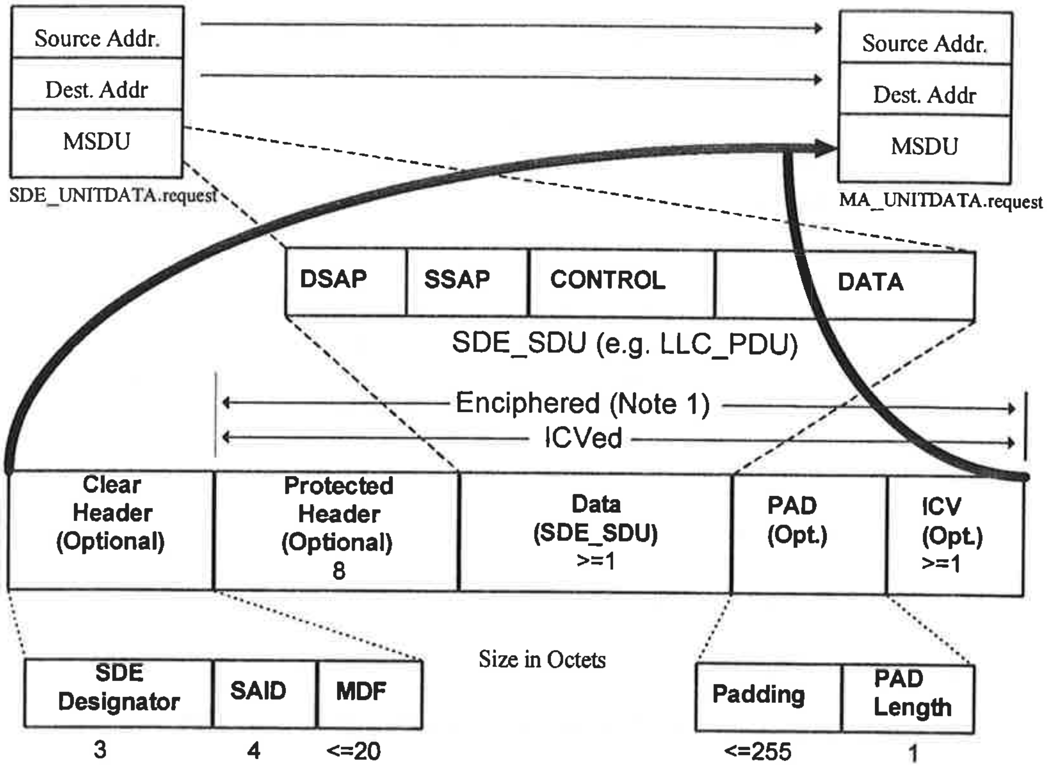


**Figure 3.1 - Construction of the SDE_PDU**

**Add the following paragraph at the end of paragraph 3.1.1.3:**

The Layer 2 security services provided by the SDE rely on information from non-Layer 2 management or system entities. Management entities communicate the information to the SDE entity through a Security Management Information Base (SMIB). The implementation of the SMIB is a local issue; however, IEEE 802.10f, SDE Sublayer Management, provides information on the managed object classes and attributes. The SMIB provides the interface between the local System Management Application Entity (SMAE) and the LM of the protocol stack. This is illustrated in Figure 3-2 (will require renumbering of the section 3 figures):

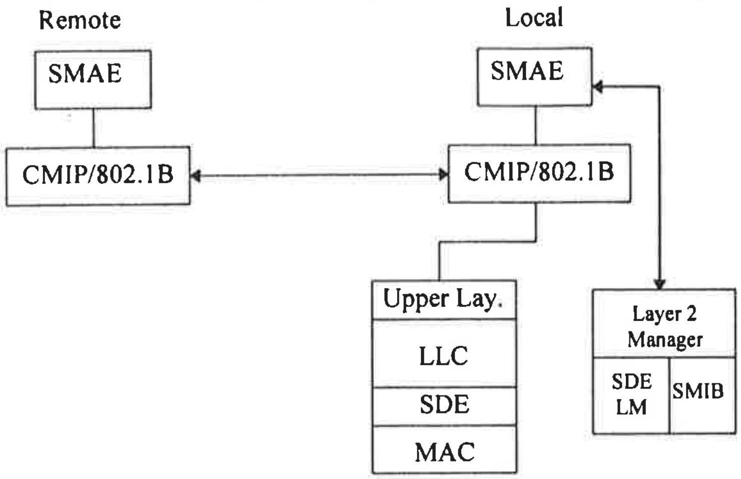


**Figure 3-2: SDE management architecture**

4. Section 5.4, The Wired Equivalent Privacy Algorithm (WEP): It is recommended that this section be moved to a normative annex.

5.4.1, Introduction: Add a sentence to the end of the first paragraph. "The WEP can also be used to provide implicit authentication. The commonly held key can be used to encrypt challenges from the access point or another station."

Change second paragraph to read;

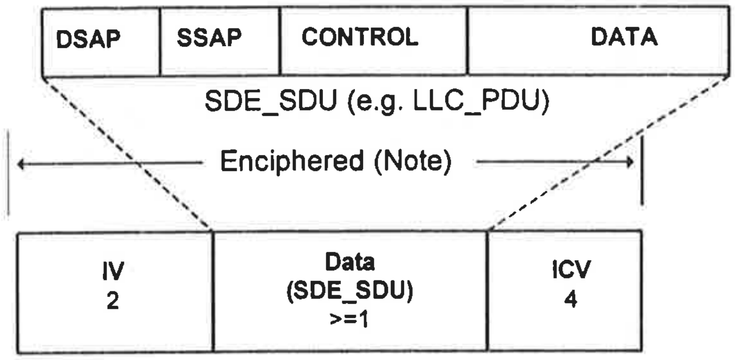
Data confidentiality depends on an external key management service to authenticate users and distribute data enciphering/deciphering keys. P802.11 specifically recommends against running an 802.11 with *confidentiality*~~privacy~~ but without authentication. While this combination is possible, it leaves the system open to significant security threats.

5.4.2, Properties of the WEP Algorithm: Add the property of **Implicit Authentication**, using language similar to above. "A commonly held key can be used to provide implicit authentication without the need for a separate authentication mechanism."

Add section 5.4.5, Relationship of WEP to IEEE 802.10, SDE:

**5.4.5, Relationship of WEP to IEEE 802.10, Secure Data Exchange (SDE):**

The WEP uses a subset of the IEEE 802.10 SDE shown in Figure 3-1 of section 3.1.1.3. Figure 5-24 (will require renumbering of section 5 figures) shows the SDE_PDU as constructed by the WEP.



Size in Octets

Note: The encryption process has expanded the PDU by 6 Octets, 2 for the Initialization Vector (IV) and 4 for the Integrity Check Value (ICV)

**Figure 5-24: Construction of WEP SDE_PDU**

5. Section 7.4, Management Information Definitions:

The following changes are recommended to harmonize the draft 802.11 standard with the approved IEEE 802.10 standard. These changes consisted of changing the word privacy to confidentiality, replacing Privacy with Confid in the MIB parameter list, and replacing Algorithm(s) with Alg_ID(s). These changes make the proposed 802.11 standard consistent terminology wise with the approved IEEE 802.10 standard. A separate file with these changes and their revisions marks is available from the author.

It is recommended that the entries regarding minimum authentication and confidentiality be removed from section 7.4. These are not Layer 2 functions. They are upper layer management functions.

# 0.1. Management Information Definitions

## 0.1.1. MIB Summary

The following sections summarize the 802.11 Management Information Base (MIB). Each group, attribute, action and notification is listed. This summary is for information purposes only. If any errors exist, the formal definitions have precedence. *This section also includes references to the SDE MIB (SMIB) found in IEEE 802.10f-1993, Secure Data Exchange (SDE) Sublayer Management. Attempts have been made to harmonize this standard with the approved IEEE 802.10 standard where ever practical. It is suggested that all developers of 802.11 products review the appropriate IEEE 802.10 standard for applicability.*

### 0.1.1.1. Station Management Attributes

#### 0.1.1.1.1. agStation_Config_grp

aActing_as_AP_Status,
aAssociated_State,
aBeacon_Period,
aPower_Mgt_State,
aPower_Mgt_Capability;

#### 0.1.1.1.2. agAuthentication_grp

aAuthentication_Algortihms,
aSelected_Authentication_Alg_ID,
aAuthentication_Handshake_State,
aAuthentication_State,
~~aMin_Authentication_Required;~~

#### 0.1.1.1.3. agConfid_grp

aConfid_Algortihms,
aSelected_Confid_Alg_ID,
aConfid_Handshake_State,
aConfid_State,
~~aMin_Confid_Required;~~

#### 0.1.1.1.4. Not Grouped

aStation_ID
aCurrent_BSS_ID
aCurrent_ESS_ID
aKnown_APs

### 0.1.1.2. MAC Attributes

#### 0.1.1.2.1. agAddress_grp

aMAC_Address,
aGroup_Addresses;

#### 0.1.1.2.2. agOperation_grp

aNAV,
aNAV_max,
aRate_Factor,
aHandshake_Overhead,
aSIFS,
aPIFS,
aDIFS,
aRTS_Threshold,
aSlot_Time,
aCW_max,
aCW_min,
aCTS_Time,
aACK_Time,
aRetry_max,
aMax_Frame_Length,
aFragmentation_Threshold;

#### 0.1.1.2.3. agCounters_grp

aTransmitted_Frame_Count,
aOctets_Transmitted_Count,
aMulticast_Transmitted_Frame_Count,
aBroadcast_Transmitted_Frame_Count,
aFailed_Count,
aCollision_Count,
aSingle_Collision_Count,
aMultiple_Collision_Count,
aReceived_Frame_Count,
aOctets_Received_Count,
aMulticast_Received_Count,
aBroadcast_Received_Count,
aError_Count,
aFCS_Error,Count,
aLength_Mismatch_Count,
aFrame_Too_Long_Count,
aTotal_Backoff_Time;

#### 0.1.1.2.4. agStatus_grp

aMAC_Enable_Status,
aTransmit_Enable_Status,
aPromiscuous_Status;

#### 0.1.1.2.5. Not Grouped

aManufacturer_ID
aProduct_ID

### 0.1.1.3. ResourceTypeID Attributes

#### 0.1.1.3.1. Not Grouped

aResourceTypeIDName
aResourceInfo

### 0.1.1.4. Actions

#### 0.1.1.4.1. SMT Actions

acStation_init
acStation_reset

#### 0.1.1.4.2. MAC Actions

acMAC_init
acMAC_reset

#### 0.1.1.4.3. PHY Actions

acPHY_init
acPHY_reset

### 0.1.1.5. Notifications

#### 0.1.1.5.1. SMT Notifications

nAssociate
nDissociate

#### 0.1.1.5.2. MAC Notifications

nFrame_Error_Rate_Exceeded

## 0.1.2. Managed Object Class Templates

### 0.1.2.1. SMT Object Class

#### 0.1.2.1.1. oSMT

```
SMT MANAGED OBJECT CLASS
DERIVED FROM "ISO/IEC 10165-2":top;
CHARACTERIZED BY
    pSMT_base                                  PACKAGE
        BEHAVIOUR
            bSMT_base BEHAVIOUR
                DEFINED AS "The SMT object class provides the necessary support at the station to
                manage the processes in the station such that the station may work cooperatively as a
                part of an 802.11 network.";
            ATTRIBUTES
                aStation_ID                            GET,
                aActing_as_AP_Status                   GET,
                aCurrent_BSS_ID                        GET,
                aCurrent_ESS_ID                        GET-REPLACE,
                aKnown_APs                             GET, (1 to N deep)
            aAuthentication_Alg_IDs                 GET,
            aConfid_Alg_IDs                         GET,
            aSelected_Authentication_Alg_ID         GET,
            aSelected_Confid_Alg_ID                 GET,
            aAuthentication_Handshake_State         GET,
            aConfid_Handshake_State                 GET,
            aAuthentication_State                   GET,
            aConfid_State                           GET,
            ~~aMin_Authentication_Required          GET,~~
            ~~aMin_Confid_Required                  GET,~~
            aAssociated_State                       GET,
            aBeacon_Period                          GET-REPLACE,
            aPower_Mgt_State                        GET-REPLACE,
            aPower_Mgt_Capability                   GET;
        ATTRIBUTE GROUPS
            agStation_Config_grp,
            agAuthentication_grp,
            agConfid_grp;
        ACTIONS
            acSMT_init,
            acSMT_reset;
REGISTERED AS { iso(1) member-body(2) us(840) ieee802dot11(xxxx) smt(0) };
```

### 0.1.2.2. MAC Object Class

#### 0.1.2.2.1. oMAC

```
MAC MANAGED OBJECT CLASS
DERIVED FROM "ISO/IEC 10165-2":top;
CHARACTERIZED BY
    pMAC_base                               PACKAGE
        BEHAVIOUR
            bMAC_base BEHAVIOUR
                DEFINED AS "The MAC object class provides the necessary support for the access
                control, generation and verification of frame check sequences, and proper delivery of
                valid data to upper layers.";
            ATTRIBUTES
                aMAC_Address                            GET,
                aGroup_Addresses                        GET-REPLACE,
                aPromiscuous_Status                     GET,
                aTransmitted_Frame_Count                GET-REPLACE,
                aOctets_Transmitted_Count               GET-REPLACE,
                aMulticast_Transmitted_Frame_Count      GET-REPLACE,
                aBroadcast_Frame_Count                  GET-REPLACE,
                aFailed_Count                           GET-REPLACE,
                aFrame_Exchange_Error_Count             GET-REPLACE,
                aSingle_Frame_Exchange_Error_Count      GET-REPLACE,
                aMultiple_Frame_Exchange_Error_Count GET-REPLACE,
                aReceived_Frame_Count                   GET-REPLACE,
                aOctets_Received_Count                  GET-REPLACE,
                aMulticast_Received_Frame_Count         GET-REPLACE,
                aBroadcast_Received_Frame_Count         GET-REPLACE,
                aReceived_Frame_Error_Count             GET-REPLACE,
                aFCS_Error_Count                        GET-REPLACE,
                aFrame_Too_Long_Count                 GET-REPLACE,
                aFrame_With_Protocol_Error_Count      GET-REPLACE,
                aMAC_Enable_Status                    GET,
                aRate_Factor                          GET,
                aHandshake_Overhead                   GET,
                aSIFS                                 GET,
                aPIFS                                 GET,
                aDIFS                                 GET,
                aRTS_Threshold                        GET-REPLACE,
                aTotal_Accumulated_Backoff_Time       GET-REPLACE,
                aSlot_Time                            GET,
                CW_max                                GET-REPLACE,
                aCW_min                               GET-REPLACE,
                aCTS_Time                             GET,
                aACK_Time                             GET,
                aRTS_Retry_max                        GET-REPLACE,
                aDATA_Retry_max                       GET-REPLACE
                aMax_Frame_Length                     GET,
                aFragmentation_Threshold              GET-REPLACE,
                aManufacturer_ID                      GET,
                aProduct_ID                           GET;
            ATTRIBUTE GROUPS
                agCapabilities_grp,
                agConfig_grp,
                agAddress_grp,
                agOperation_grp,
                agCounters_grp,
                agFrame_Error_Condition_grp,
                agStatus_grp;
            ACTIONS
                acMAC_init,
                acMAC_reset;
            NOTIFICATIONS
                nFrame_Error_Rate_Exceeded;
REGISTERED AS { iso(1) member-body(2) us(840) ieee802dot11(xxxx) mac(1) };
```

### 0.1.2.3. Resource Type Object Class

#### 0.1.2.3.1. oResourceTypeID

```
ResourceTypeID MANAGED OBJECT CLASS
DERIVED FROM IEEE802CommonDefinitions.oResourceTypeID;
CHARACTERIZED BY
    pResourceTypeID                           PACKAGE
            ATTRIBUTES
                aResourceTypeIDName                   GET,
                aResourceInfo                         GET;
REGISTERED AS { iso(1) member-body(2) us(840) ieee802dot11(xxxx) resourcetypeid(3) };
```

### 0.1.3. Attribute Group Templates

### 0.1.3.1. Station Management Attribute Group Templates

### 0.1.3.1.1. agStation_Config_grp

Station_Config_grp ATTRIBUTE GROUP
GROUP ELEMENTS
aActing_as_AP_Status,
aAssociated_State,
aBeacon_Period,
aPower_Mgt_State,
aPower_Mgt_Capability;
REGISTERED AS { iso(1) member-body(2) us(840) ieee802dot11(xxxx) smt(0) station_config_grp(0) };

### 0.1.3.1.2. agAuthentication_grp

Authentication_grp ATTRIBUTE GROUP
GROUP ELEMENTS
aAuthentication_Algortihms,
aSelected_Authentication_Alg_ID,
aAuthentication_Handshake_State,
aAuthentication_State,
~~aMin_Authentication_Required;~~
REGISTERED AS { iso(1) member-body(2) us(840) ieee802dot11(xxxx) smt(0) authentication_grp(1) };

### 0.1.3.1.3. agConfid_grp

Confid_grp ATTRIBUTE GROUP
GROUP ELEMENTS
aConfid_Algortihms,
aSelected_Confid_Alg_ID,
aConfid_Handshake_State,
aConfid_State,
~~aMin_Confid_Required;~~
REGISTERED AS { iso(1) member-body(2) us(840) ieee802dot11(xxxx) smt(0) Confid_grp(2) };

### 0.1.3.2. MAC Attribute Group Templates

### 0.1.3.2.1. agAddress_grp

Address_grp ATTRIBUTE GROUP
GROUP ELEMENTS
aMAC_Address,
aGroup_Addresses;
REGISTERED AS { iso(1) member-body(2) us(840) ieee802dot11(xxxx) mac(0) address_grp(0) };

### 0.1.3.2.2. agOperation_grp

Operation_grp ATTRIBUTE GROUP
GROUP ELEMENTS
aNAV,
aNAV_max,
aRate_Factor,
aHandshake_Overhead,
aSIFS,
aPIFS,
aDIFS,

```
        aRTS_Threshold,
        aSlot_Time,
        aCW_max,
        aCW_min,
        aCTS_Time,
        aACK_Time,
        aRetry_max,
        aMax_Frame_Length,
        aFragmentation_Threshold;
REGISTERED AS { iso(1) member-body(2) us(840) ieee802dot11(xxxx) mac(0) operation_grp(1) };
```

#### 0.1.3.2.3. agCounters_grp

```
Counters_grp ATTRIBUTE GROUP
    GROUP ELEMENTS
        aTransmitted_Frame_Count,
        aOctets_Transmitted_Count,
        aMulticast_Transmitted_Frame_Count,
        aBroadcast_Transmitted_Frame_Count,
        aFailed_Count,
        aCollision_Count,
        aSingle_Collision_Count,
        aMultiple_Collision_Count,
        aReceived_Frame_Count,
        aOctets_Received_Count,
        aMulticast_Received_Count,
        aBroadcast_Received_Count,
        aError_Count,
        aFCS_Error,Count,
        aLength_Mismatch_Count,
        aFrame_Too_Long_Count,
        aTotal_Backoff_Time;
REGISTERED AS { iso(1) member-body(2) us(840) ieee802dot11(xxxx) mac(0) counters_grp(2) };
```

#### 0.1.3.2.4. agStatus_grp

```
Status_grp ATTRIBUTE GROUP
    GROUP ELEMENTS
        aMAC_Enable_Status,
        aTransmit_Enable_Status,
        aPromiscuous_Status;
REGISTERED AS { iso(1) member-body(2) us(840) ieee802dot11(xxxx) mac(0) status_grp(3) };
```

### 0.1.4. Attribute Templates

#### 0.1.4.1. SMT Attribute Templates

#### 0.1.4.1.1. aStation_ID

```
Station_ID ATTRIBUTE
DERIVED FROM
    IEEE802CommonDefinitions.MACAddress;
REGISTERED AS
    { iso(1) member-body(2) us(840) ieee802dot11(xxxx) SMT(0) attribute(7) station_id(0) };
```

### 0.1.4.1.2. aActing_as_AP_Status

Acting_as_AP_Status ATTRIBUTE
WITH APPROPRIATE SYNTAX
boolean;
BEHAVIOUR DEFINED AS
"True if this station is acting as an access point, false otherwise.";
REGISTERED AS
{ iso(1) member-body(2) us(840) ieee802dot11(xxxx) SMT(0) attribute(7) acting_as_ap_status(4) };

### 0.1.4.1.3. aCurrent_AP_MAC_Address

Current_AP_MAC_Address ATTRIBUTE
DERIVED FROM
IEEE802CommonDefinitions.MACAddress;
REGISTERED AS
{ iso(1) member-body(2) us(840) ieee802dot11(xxxx) SMT(0) attribute(7) ap_address(5) };

### 0.1.4.1.4. aCurrent_BSS_ID

Current_BSS_ID ATTRIBUTE
WITH APPROPRIATE SYNTAX
integer;
BEHAVIOUR DEFINED AS
"This attribute shall identify the basic service set (BSS) with which the station is currently associated.";
REGISTERED AS
{ iso(1) member-body(2) us(840) ieee802dot11(xxxx) SMT(0) attribute(7) current_bss_id(6) };

### 0.1.4.1.5. aCurrent_ESS_ID

Current_ESS_ID ATTRIBUTE
WITH APPROPRIATE SYNTAX
integer;
BEHAVIOUR DEFINED AS
"This attribute shall identify the extended service set (ESS) with which the station is associated, if any.";
REGISTERED AS
{ iso(1) member-body(2) us(840) ieee802dot11(xxxx) SMT(0) attribute(7) current_ess_id(7) };

### 0.1.4.1.6. aKnown_APs

Known_APs ATTRIBUTE
WITH APPROPRIATE SYNTAX
set-of AP_ID.type;
BEHAVIOUR DEFINED AS
"This attribute shall be a set of the identities of the most recently known Access Points. The Access Point with which the station is currently associated, if any, shall always be the first element of the set. Access Points may be included in this list even if the station did not associate with them.";
REGISTERED AS
{ iso(1) member-body(2) us(840) ieee802dot11(xxxx) SMT(0) attribute(7) known_aps(8) };

### 0.1.4.1.7. aAuthentication_Alg_IDs

Authentication_Alg_IDs ATTRIBUTE
WITH APPROPRIATE SYNTAX
set-of integer;
BEHAVIOUR DEFINED AS

"This attribute shall be a set of all the authentication algorithms supported by the stations. The values of the numbers in the list are as defined in IEEE Standard 802.10.";
REGISTERED AS
{ iso(1) member-body(2) us(840) ieee802dot11(xxxx) SMT(0) attribute(7) authentication_Alg_IDs(9) };

### 0.1.4.1.8. aConfid_Alg_IDs

Confid_Alg_IDs ATTRIBUTE
WITH APPROPRIATE SYNTAX
set-of integer;
BEHAVIOUR DEFINED AS
"This attribute shall be a set all of the confidentiality algorithms supported by the stations. The values of the numbers in the list are as defined in IEEE Standard 802.10.";
REGISTERED AS
{ iso(1) member-body(2) us(840) ieee802dot11(xxxx) SMT(0) attribute(7) Confid_Alg_IDs(10) };

### 0.1.4.1.9. aSelected_Authentication_Alg_ID

Selected_Authentication_Alg_ID ATTRIBUTE
WITH APPROPRIATE SYNTAX
integer;
BEHAVIOUR DEFINED AS
"This attribute shall indicate the authentication algorithm identifer selected during the authentication negotiation. The value of this attribute shall be selected from the set in the aAuthentication_Alg_IDs attribute. The value of this attribute shall reference one of the authentication algorithm identifiers defined in IEEE Standard 802.10.";
REGISTERED AS
{ iso(1) member-body(2) us(840) ieee802dot11(xxxx) SMT(0) attribute(7) selected_authentication_Alg_ID(11) };

### 0.1.4.1.10. aSelected_Confid_Alg_ID

Selected_Confid_Alg_ID ATTRIBUTE
WITH APPOPRIATE SYNTAX
integer;
BEHAVIOUR DEFINED AS
"This attribute shall indicate the confidentiality algorithm identifer selected during the confidentiality negotiation. The value of this attribute shall be selected from the set in the aConfid_Alg_IDs attribute. The value of this attribute shall reference one of the confidentiality algorithm identifiers defined in IEEE Standard 802.10.";
REGISTERED AS
{ iso(1) member-body(2) us(840) ieee802dot11(xxxx) SMT(0) attribute(7) selected_Confid_Alg_ID(12) };

### 0.1.4.1.11. aAuthentication_Handshake_State

Authentication_Handshake_State ATTRIBUTE
WITH APPROPRIATE SYNTAX
authentication_handshake.type
BEHAVIOUR DEFINED AS
"This attribute shall identify the current state of the station in the authentication process.";
REGISTERED AS
{ iso(1) member-body(2) us(840) ieee802dot11(xxxx) SMT(0) attribute(7) authentication_handshake_state(13) };

### 0.1.4.1.12. aConfid_Handshake_State

Confid_Handshake_State ATTRIBUTE

```
WITH APPROPRIATE SYNTAX
    Confid_hanshake.type;
BEHAVIOUR DEFINED AS
    "This attribute shall identify the current state of the station in the confidentiality negotiation
    process.";
REGISTERED AS
    { iso(1) member-body(2) us(840) ieee802dot11(xxxx) SMT(0) attribute(7)
    Confid_handshake_state(14) };
```

### 0.1.4.1.13. aAuthentication_State

```
Authentication_State ATTRIBUTE
WITH APPROPRIATE SYNTAX
    authentication_state.type;
BEHAVIOUR DEFINED AS
    "This attribute shall indicate the authentication state.";
REGISTERED AS
    { iso(1) member-body(2) us(840) ieee802dot11(xxxx) SMT(0) attribute(7) authentication_state(15)
    };
```

### 0.1.4.1.14. aConfid_State

```
Confid_State ATTRIBUTE
WITH APPROPRIATE SYNTAX
    Confid_state.type;
BEHAVIOUR DEFINED AS
    "This attribute shall indicate the current confidentiality state.";
REGISTERED AS
    { iso(1) member-body(2) us(840) ieee802dot11(xxxx) SMT(0) attribute(7) Confid_state(16) };
```

### 0.1.4.1.15. ~~aMin_Authentication_Required~~ *(delete section)*

```
Min_Authentication_Required ATTRIBUTE
WITH APPROPRIATE SYNTAX
    Authentication_Required.type;
BEHAVIOUR DEFINED AS

    ;
REGISTERED AS
    { iso(1) member-body(2) us(840) ieee802dot11(xxxx) SMT(0) attribute(7)
    min_authentication_required(17) };
```

### 0.1.4.1.16. ~~aMin_Confid_Required~~ *(delete section)*

```
Min_Confid_Required ATTRIBUTE
WITH APPROPRIATE SYNTAX
    Confid_Required.type;
BEHAVIOUR DEFINED AS

    ;
REGISTERED AS
{ iso(1) member-body(2) us(840) ieee802dot11(xxxx) SMT(0) attribute(7)
min_Confid_required(18) };
```