IEEE P802.11
Wireless LANs

|  |
| --- |
| Proposed Resolution for Assigned Security CIDs |
| Date: 2013-05-13 |
| Author(s): |
| Name | Affiliation | Address | Phone | email |
| René Struik | Struik Security Consultancy | Toronto ON | +1 415 690-7363+1 647 867-5658Skype: rstruik | rstruik.ext@gmail.com |

Abstract

This document presents suggested text to implement “large objects” with TGai, as indicated in 13/201r6. Suggested text is relative to 802.11-2012 and TGai/D0.4.

**3.1 Definitions**

***Insert the following new definition:***

**Conceptual object:** octet string that may have syntax or semantics that are only partially specified with 802.11 (e.g., higher-layer information). This conceptual object is only conveyed between a STA and AP, after representing this as an ordered sequence of information elements, whereas the receiving entity may only act on this object after converting this back to the corresponding conceptual object.

**8.4 Management frame body components**

***Replace section 8.4.2.186 by the following section:***

**8.4.2.186 Conceptual objects**

***Replace section 8.4.2.186.1 by the following section:***

**8.4.2.186.1 General**

A conceptual object is an octet string that may have syntax or semantics that are only partially specified with 802.11 (e.g., higher-layer information). This conceptual object is only conveyed between a STA and AP, after representing this as an ordered sequence of information elements (8.4.2.186.1.1a.1), whereas the receiving entity may only act on this object after converting this back to the corresponding conceptual object (8.4.2.186.1.1a.2).

To facilitate description of the mapping from conceptual objects to sequences of information elements (8.4.2.186.1.1a.1) and the corresponding inverse mapping (8.4.2.186.1.1a.2), conceptual objects are described as “generalized information elements”, as follows.

Conceptual objects are defined to have a common general format consisting of a 1-octet Object ID field and a variable-length object ID-specific Information field. Each element is assigned a unique Object ID as defined in this standard. The format of the Conceptual Object is shown in Fig. 8.4.1a-1.

|  |  |  |  |
| --- | --- | --- | --- |
|  | Object ID | Length | Conceptual Object Value |
| Octets: | 1 | 2 | Variable |
|  | **Figure 8.4.2.186.1a – Conceptual object format(11s)** |  |  |

The set of valid object Ids is defined in Table 8.4.1a-2.

|  |  |  |
| --- | --- | --- |
| **Conceptual Object** | **Object Id** | **Description** |
| FILS HLP Wrapped Data TLV | 0 | (see 8.4.2.186.1.1) |
| IP Address Request Element | 1 | (see 8.4.2.186.1.2) |
| FILS IP Address Assignment TLV | 2 | (see 8.4.2.186.1.3) |
| FILS DNS Information TLV | 3 | (see 8.4.2.186.1.4) |
| FILS Public Key Element | 4 | (see 8.4.2.186.1.5) |
|  | 5-255 | Reserved |

***Insert the following section at the end of section 8.4.2.186.1:***

**8.4.2.186.1.a1 Conversion scheme**

**8.4.2.186.1.a1.1 Representation of Conceptual Objects**

This involves the transformation of the Conceptual Object field to an ordered sequence of information elements, according to the following stipulations:

* The Element Id of each such information element shall be set to the “Conceptual Object Segment IE”, as specified in Table 8-54;
* The Length field of each such information element shall have a value between 0 and 255 (inclusive);
* The right-concatenation of all Information Fields in the resulting ordered sequence of information elements shall be equal to the Conceptual Object field;
* The rightmost (last) information element in the resulting ordered sequence of information elements shall have its Length field set to zero.
* The representation of an ordered sequence of Conceptual Object fields shall be defined as the ordered sequence of the outcomes of the transformation of each single Conceptual object in this sequence, using this original ordering.

The procedure by which the partitioning of the Conceptual Object field over the Conceptual Object Segment information elements is determined is out of scope of this specification.

**8.4.2.186.1.a1.2 The Inverse Mapping**

This involves the transformation of an ordered sequence of information elements to an ordered sequence of Conceptual Object fields, according to the following stipulations:

* The transformation shall fail if not all information elements have their Element Id set to the “Conceptual Object Segment IE”, as specified in Table 8-54;
* The transformation shall partition the ordered sequence of information elements into ordered subsequences of information elements, where the rightmost (last) information element in each such ordered subsequence has a Length field set to zero and where each other information element in this subsequence has a Length field set to a nonzero value. If this partitioning is not possible, the transformation shall fail.
* The transformation shall convert each subsequence into a Conceptual Object field which is equal to the right-concatenation of all Information Fields in the ordered subsequence; the ordered sequence of Conceptual Object fields shall be defined as the result of ordering the Conceptual Object fields reconstructed from each subsequence, according to the partitioning order by which these subsequences were previously derived.

Note: It is easy to see that the composition of these two conversion function results in the original sequence of Conceptual Object fields (if one ignores empty octet strings).

***Insert the following section:***

**8.4.2.186.1.5 FILS Public Key Element TLV**

The FILS Public Key element is used to communicate the device's (certified) public-key for use with the

FILS authentication exchange and can be used as an alternative to the FILS Public Key Element of section 8.4.2.183 or when that FILS Public Key Element cannot be used, due to size restrictions of information elements.

The format of the FILS Public Key element is shown in Figure 8.4.2.186.1.5a.

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
|  | Object ID | Length | Key Type | FILS Public Key |
| Octets: | 1 | 2 | 1 | variable |

**Figure 8.4.2.186.1.5a — FILS Public Key element format**

The Key Type subfield is as specified in Section 8.4.2.183.

***Insert the following row/Information Elements to Table 8-54:***

|  |  |  |  |
| --- | --- | --- | --- |
| **Element** | **Element ID** | **Length of indicated element (in octets)**  | **Extensible** |
| Conceptual Object Segment (see x.x.x) | <ANA> | 2-257 | Representation of a segment of a conceptual object (if the length field of this element is set to a positive value), respectively representation of a separator between conceptual objects (if the length field of this element is set to zero)  |
| Encryption length indicator (see x.x.x) | <ANA> | 4 | Indicator of the octet length of the frame segment directly following it that is encrypted |

***Editorial note – the Element Id for the Encryption Indicator should be set to the smallest available number no already specified in 802.11-2012.***

***Insert the following subclause:***

**8.4.2.188 Encryption Length Indicator**

The encryption length indicator is used to uniquely indicate the frame segment that is encrypted. The format of the Encryption Length Indicator element is shown in Fig. 8.4.2.188-a1.

|  |  |  |  |
| --- | --- | --- | --- |
|  | Element Id | Length | Length Encrypted Data |
| Octets: | 1 | 1 | 2 |

The Element Id shall be set to the “Encryption Length Indicator IE”, as specified in Table 8-54.

***Modify section D0.5/11.11.2.4 as indicated:***

**11.11.2.4 Key confirmation with FILS authentication**

Key confirmation for FILS Authentication is an Associate Request followed by an Associate Response. The

Association Request and Association Response shall be protected using the KEK2 according to 11.11.2.5 and 11.11.2.6.

Upon the completion of key establishment (11.11.2.2) and key derivation (11.11.2.3) the STA shall construct an 802.11 associate request frame indicating its selected ciphersuite and the FILS AKM, and the FILS Key Confirmation element. The content of the Key Auth field of the Key Confirmation element depends on the type of FILS authentication.

The AP transfers any necessary KDEs to the STA in the Association Response frame. The AP may include one or more KDEs using the FILS KDE container. The format and the rules for transferring the KDE shall follow 11.6.2 (EAPOL Key Frames).

For FILS Authentication using a trusted third party, the Key Auth field of the Key Confirmation element of the Association Request shall be:

Key-Auth = HMAC-SHA256(KCK2, NSTA | NAP | STA-MAC | AP-BSSID).

For FILS Authentication without a trusted third party, the Key Auth field of the Key Confirmation element in the Association Request shall contain a digital signature using the STA's private key, the specific construction of the digital signature depends on the crypto-system of the public/private key pair:

Key-Auth = Sig-STA(gSTA | gAP | NSTA | NAP | STA-MAC | AP-BSSID).

Where Sig-STA indicates a digital signature using the STA's private key, gSTA is the octet-string representation

of the STA's public Diffie-Hellman value, gAP is the octet-string representation of the AP's public

Diffie-Hellman value, NSTA is the nonce selected by the STA, and NAP is the nonce selected by the AP.

The 802.11 Association Request frame shall be secured as follows:

* The input key shall be the KEK2
* The plaintext indicator shall be a set of information elements contained in the Association Request frame that follow the FILS Session element. The procedure by which STA selects this set of information elements is outside scope of the specification. (We assume that the indicator does not “break” conceptual objects (8.4.1a))
* The first input string shall be set to the right-concatenation of the following fields:
* The STA MAC
* The AP BSSID
* The STA's nonce
* The AP's nonce
* The second input string shall be set to the entire frame body of the Association Request frame
* The input key, the plaintext indicator, and the first and second input string shall be passed to the encrypt-and-authenticate operation specified in 11.11.2.6.
* The frame body of the Association Request frame shall be set to the transformed second input string resulting from 11.11.2.6.

The resulting 802.11 Association Request frame shall be transmitted to the AP.

The received 802.11 Association Request frame shall be processed as follows:

* The input key shall be the KEK2
* The first input string shall be set to the right-concatenation of the following fields:
1. The STA MAC
2. The AP BSSID
3. The STA's nonce
4. The AP's nonce
* The second input string shall be set to the entire frame body of the Association Request frame
* The input key and the first and second input strings shall be passed to the decrypt-and-verify operation specified in 11.11.2.7.
* If the output from 11.11.2.7 returns a failure, authentication shall be deemed a failure. Otherwise, the frame body of the Association Request frame shall be set to the transformed second input string resulting from 11.11.2.7.

The Key-Auth from the decrypted Association frame shall be checked. If it is incorrect, authentication shall be deemed a failure. If authentication is deemed a failure, the KCK2, KEK2, KCK, KEK, and TK shall be irretrievably destroyed. If authentication is not deemed a failure, the AP shall check the Key-Auth field in the Key Confirmation element.

For FILS Authentication using a trusted third party, the AP shall construct a verifier as follows:

Key-Auth' = HMAC-SHA256(KCK, NSTA | NAP | STA-MAC | AP-BSSID)

If Key-Auth' differs from the Key-Auth field in the Key Confirmation element, authentication shall be deemed a failure.

For FILS Authentication without a trusted third party, the AP shall use the STA's (certified) public key from the FILS Public Key element in the Association frame to verify the contents of the Key-Auth field of the Key Confirmation element. The specific technique for verification depends on the crypto-system used by the public key. If verification fails, authentication shall be deemed a failure.

If authentication is a failure, the KCK2, KEK2, KCK, KEK, and TK shall be irretrievably destroyed. Otherwise, the AP shall then construct an 802.11 associate response frame confirming the selected ciphersuite and the FILS AKM, and containing the FILS KDE Container, and its own Key-Auth.

For FILS authentication using a trusted third party, the Key Auth field of the Key Confirmation element in the Association Response shall be:

Key-Auth = HMAC-SHA256(KCK2, NAP | NSTA | AP-BSSID | STA-MAC).

For FILS Authentication without a trusted third party, the Key Auth field of the Key Confirmation element in the Association Response shall contain a digital signature using the AP's private key, the specific construction of the digital signature depends on the crypto-system of the public/private keypair:

Key-Auth = Sig-AP(gAP | gSTA | NAP | NSTA | AP-BSSID | STA-MAC ).

Where Sig-AP indicates a digital signature using the AP's private key, and where gSTA, gAP, NSTA, and NAP are the same as in the construction of the Association Request.

The 802.11 Association Response frame shall be protected as follows:

* The input key shall be the KEK2
* The plaintext indicator shall be a set of information elements contained in the Association Request frame that follow the FILS Session element. The procedure by which AP selects this set of information elements is outside scope of the specification. (We assume that the indicator does not “break” conceptual objects (8.4.1a))
* The first input string shall be set to the right-concatenation of the following fields:
1. The AP BSSID
2. The STA MAC
3. The AP's nonce
4. The STA's nonce
* The second input string shall be set to the entire frame body of the Association Response frame
* The input key, the plaintext indicator, and the first and second input string shall be passed to the encrypt-and- authentication operation specified in 11.11.2.6
* The frame body of the Association Response frame shall be set to the transformed second input string resulting from 11.11.2.6.

The resulting 802.11 Association Response frame shall be transmitted to the STA.

The STA shall process the received 802.11 Association Response frame as follows:

* The input key shall be the KEK2
* The first input string shall be set to the right-concatenation of the following fields:
1. The AP BSSID
2. The STA MAC
3. The AP's nonce
4. The STA's nonce
* The second input string shall be set to the entire frame body of the Association Response frame
* The input key and the first and second input string shall be passed to the decrypt-and-verify operation specified in 11.11.2.7.
* If the output from 11.11.2.7 returns failure, authentication shall be deemed a failure. Otherwise, the frame body of the Association Response frame shall be set to the transformed second input string resulting from 11.11.2.7.

The Key-Auth from the decrypted Authentication frame shall be checked. If it is incorrect, authentication shall be deemed a failure. If authentication is deemed a failure, the KCK2, KEK2, KCK, KEK, and TK shall be irretrievably destroyed. If authentication is not deemed a failure, the AP shall check the Key-Auth field in the Key Confirmation element.

For FILS Authentication using a trusted third party, the STA shall construct a verifier as follows:

Key-Auth' = HMAC-SHA256(KCK2, NAP | NSTA | AP-BSSID | STA-MAC).

If Key-Auth' differs from the Key-Auth field in the Key Confirmation element, authentication shall be deemed a failure .

For FILS Authentication without a trusted third party, the STA shall use the AP's (certified) public key from the FILS Public Key element in the Association frame to verify the contents of the Key-Auth field of the Key Confirmation element. The specific technique for verification depends on the crypto-system used by the public key. If verification fails, authentication shall be deemed a failure.

If authentication is a failure, the KCK2, KEK2, KCK, KEK, PMK, and TK shall be irretrievably destroyed.

Otherwise authentication succeeds. In that case, STA and AP shall irretrievably destroy the temporary keys

KCK2 and KEK2 and both shall use the TK with the cipher indicated by the negotiated. The KCK, KEK, and PMK shall be used for subsequent key management as specified in clause 11.5. The STA and AP shall set the lifetime of the PMKSA to the value dot11RSNAConfigPMKLifetime.

***Modify section D0.5/11.11.2.6 as indicated:***

**11.11.2.6 Encrypt and authenticate operation for FILS association frames**

**11.11.2.6.1 Input Transformation (Massage Plaintext if Applicable)**

* Determine the total octet length of the plaintext from the plaintext indicator and set the Information field of the Encryption Length Indicator element to this value.
* Partition the second input string into two string segments, viz. the plaintext *P* indicated by the plaintext indicator and the remainder *A* of the second input string (thereby not reordering IEs with the same Element ID).

NOTE: if one always encrypts the entire second input string, this transformation simply sets *P* to this string and *A* to the empty string. Similarly, if the to-be-authenticated string is always “at the back” of the second input string, the strings *P* and *A* are simply the left and right parts of the second input string, where the “dividing line” is determined by information on the length of plaintext. Thus, if one uses simple security policies as to which data elements are to be encrypted and authenticated and which only to be authenticated, one can implement this step in a trivial manner. A special case is where one encrypts the entire string, except possibly for a small portion at the end (e.g., the vendor-specific information).

**11.11.2.6.2 Encrypt and authenticate operation**

The AEAD scheme of 11.11.2.5 shall be used with the 802.11 Associate Request frame (for enciphering by

STA) or with the 802.11 Associate Response frame (for enciphering by AP), with the following instantiation:

* The key *K* shall be set to KEK2;
* The associated data string shall be set to the right-concatenation of the first input string and the string *A* determined in 11.11.2.6.1;
* The string *P* shall be set to the string *P* determined in 11.11.2.6.1;
* The nonce *N* shall be set to
1. For processing by STA: use the 13-octet all-zero string;
2. For processing by AP: use the 13-octet all-one string.

If the encryption-authentication process is unsuccessful, output a failure; otherwise, output the string *C* || *A*.

NOTE: if one always encrypts the entire second input string, the associate data string and plaintext string are always equal to the first and the second input string, respectively.

**11.11.2.6.3 Output Transformation (Indicate the Associated Data and Ciphertext)**

* Substitute the second input string by the string *LBL* || *C* || *A* (which contains all visible IEs in ascending order). Here, *LBL* is equal to the Encryption Length Indicator Element determined in 11.11.2.6.1.

***Modify section D0.5/11.11.2.7 as indicated:***

**11.11.2.7 Decrypt and verify operation for FILS association frames**

**11.11.2.7.1 Input Transformation (Determining the Associated Data and Ciphertext)**

* Determine the leftmost information element of the second input string. If this information element is not found or if this does not indicate an Encryption Length Indicator Element, the procedure shall output a failure.
* Remove the Encryption Length Indicator Element from the second input string.
* Partition the resulting second input string as *C* || *A*, where the octet string *C* has as length the value contained in the Encryption Length Indicator Information field of the Security Indicator Element. If this partitioning is not possible, the procedure shall output a failure.

**11.11.2.7.2 Decrypt and Verify Operation**

The AEAD scheme of 11.11.2.5 shall be used with the 802.11 Associate Request frame (for deciphering by

STA) or with the 802.11 Associate Response frame (for deciphering by AP), with the following instantiation:

* The key K shall be set to KEK2;
* The associated data string shall be set to the right-concatenation of the first input string and the string *A* determined in 11.11.2.7.1;
* The string *C* shall be set to the string *C* determined in 11.11.2.7.1;
* The nonce *N* shall be set to
1. For processing by AP: use the 13-octet all-zero string.
2. For processing by STA: use the 13-octet all-one string;

The function shall output the string *P* || *A* if the decryption/verification process is successful and shall output a failure otherwise.

**11.11.2.7.3 Output Transformation (Massage Plaintext if Applicable)**

* Parse the output string *P* || *A* and re-order IEs that are out of order (thereby not reordering IEs with the same Element ID).
* Substitute the second input string by the result of this transformation (which contains all IEs in ascending order).

NOTE: If subsequent processing of unsecured incoming frames in an existing implementation does not assume ordering of IEs (i.e., it considers the frame body as a set of IEs, rather than an ordered sequence of IEs), this step does not need to be implemented (since the implementation does not care about ordering anyway). Similarly, if the originator of the AEAD-secured data always has the to-be-authenticated string “at the back” of the second input string, this step is not required (since the output string *P* || *A* then always is already in order). A special case is where one encrypts the entire string, except possibly for a small portion at the end (e.g., the vendor-specific information).