IEEE P802.11
Wireless LANs

|  |
| --- |
| Proposed Resolution for Assigned Security CIDs |
| Date: 2013-05-14 |
| 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. Suggested text is relative to 802.11-2012 and TGai/D0.5.

**8.4 Management frame body components**

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

**8.4.2.186 Jumbo-IE**

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

**8.4.2.186.1 General**

A jumbo element is an octet string that may have syntax or semantics that are only partially specified with 802.11 (e.g., higher-layer information) or that does not fit the length restrictions of an ordinary Information element. This jumbo IE 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 after re-assembling the corresponding Jumbo information element (8.4.2.186.1.1a.2).

Jumbo-elements are defined to have a common general format consisting of a 1-octet Element ID field, a variable-length Length field, and a variable-length element-specific Information field. Each element is assigned a unique Element ID as defined in this standard. The Length field specifies the number of octets in the Information field. See Figure 8.4.2.186.1a.

|  |  |  |  |
| --- | --- | --- | --- |
|  | Element ID | Length | Information |
| Octets: | 1 | Variable | Variable |
|  | **Figure 8.4.2.186.1a – Jumbo-Element format(11s)** |  |  |

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

|  |  |  |
| --- | --- | --- |
| **Jumbo Element** | **Element Id** | **Description** |
| FILS HLP Wrapped Data TLV | 1 | (see 8.4.2.186.1.1) |
| IP Address Request Element | 2 | (see 8.4.2.186.1.2) |
| FILS IP Address Assignment TLV | 3 | (see 8.4.2.186.1.3) |
| FILS DNS Information TLV | 4 | (see 8.4.2.186.1.4) |
| FILS Public Key Element | 5 | (see 8.4.2.186.1.5) |
|  | 6-255 | Reserved |

**Table 8.4.2.186.1b – Jumbo Elements IDs**

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

**8.4.2.186.1.a1 Representation and Re-Assembly Scheme**

**8.4.2.186.1.a1.1 Representing Jumbo elements as a sequence of Fragmentation elements**

A single Jumbo element is represented as an ordered sequence of Fragment elements, as follows:

* The length field (if present) shall be purged from the Jumbo element.
* The resulting Jumbo element shall be partitioned as the right-concatenation of non-empty chunks of size at most 255 octets. Here, all but the rightmost chunks shall have size 255 octets.
* The sequence of fragment elements shall be formed from these corresponding chunks, in order, with the length field set to the corresponding octet size of the chunk.
* A fragment element with Length field set to zero shall be added to the thus constructed ordered sequence of fragment elements, as rightmost fragment, in the event that the constructed sequence of fragment elements would otherwise only have fragment fields with 255 octets.

A sequence of Jumbo elements shall be represented by representing each single Jumbo element using the procedure described above and concatenating the result, using this original Jumbo element ordering.

**8.4.2.186.1.a1.2 Reassembling Jumbo elements from a sequence of Fragment elements**

Re-assemble of a Jumbo element (or an ordered set of Jumbo elements) from a sequence of Fragment elements proceeds as follows:

* Determine the largest consecutive sequence of fragment elements.
* Partition the sequence of fragment elements as an ordered set of subsequences of fragment elements, each subsequence ending with a fragment element with length field smaller than 255 octets and having only length 255 fragment elements otherwise. Each of these subsequences corresponds to precisely one single Jumbo element.
* Re-assemble each Jumbo element from the fragment elements as follows:
	+ Form the right-concatenation of the corresponding fragment fields.
	+ The Jumbo element ID shall be set to the leftmost octet of this string.
	+ The Jumbo information field shall be set to the remainder of this string.
	+ The length of the Jumbo element (if present) shall be set to the octet size of the Jumbo information field, according to the representation convention for the Jumbo element in question.

Note: It is easy to see that the composition of these two conversion function results in the original sequence of Jumbo information element fields.

***Insert the following section:***

**8.4.2.186.1.5 FILS Public Key Jumbo-Element**

The FILS Public Key Jumbo 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.

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
|  | Element 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 Element Id shall be set to the “FILS Public Key Jumbo element”, as specified in Table 8.4.2.186.1b.

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)**  | **Description** |
| Fragment (see 8.4.2.188) | <ANA> | 2-257 | Representation of a fragment of a Jumbo element (if the length field of this element is set to a positive value), respectively representation of a separator between Jumbo elements (if the length field of this element is set to zero)  |

***Instruct the editor to add section 8.4.2.188, and subsections, to the draft and replace <ANA-X> with an appropriate figure identifier:***

**8.4.2.188 Fragment Element**

The fragment element is used to indicate a fragment of the representation of a Jumbo element. The format of the fragment element is shown in Fig. 8.4.2.188-a1.

|  |  |  |  |
| --- | --- | --- | --- |
|  | Element Id | Length | Fragmented information |
| Octets: | 1 | 1 | variable |

**Figure <ANA-X>-- Fragment IE**

The Element ID shall be set to the “Fragment IE”, as specified in Table 8-54.