|  |
| --- |
| Proposed Resolution for Some Security CIDs |
| Date: 2014-03-19 |
| 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 discusses some security-related LB#198 comments related to D1.0 of the TGai specification.

**Summary sheet: Suggested resolution of a selection of comments from 13/1076r30:**

**DETAILS: Suggested resolution of a selection of comments from 13/1076r30:**

**CID #2986:** (Michael Montemurro) 11.11.2.3, p. 103, l. 31:

Circular reference "...shall be used in exactly the same way as same-named keys of IEEE 802.11-2012 (but now derived as specified above)."

Point to the specific clauses in IEEE 802.11-2012 that this sentence references.

Suggested resolution: Revised.

Note: this has been addressed, pursuant to adoption of 14/341r5.

**CID #3259:** (Rob Sun) 11.11.2.3, p. 103, l. 12:

How and where to store KCK2/KEK2 which should be transient and only for FILS key confirmation? It needs to define when to destroy the KCK2/KEK2. The assumption is PMKSA which is lack of definition in elements for FILS would store the KCK2/KEK2 which may not be ideal

Please clarify

Suggested resolution: Revised.

Motivation: the keys KEK2/KCK2 have been removed, pursuant to adoption of 14/341r5.

**CID #3243:** (Santosh Ghanshyam Pandey) 11.11.2.3, p. 103, l. 27:

The reference for encrypt-and-authentication should be 11.11.2.6, and decrypt-and-verify should be 11.11.2.7.

Change as per the comment

Suggested resolution: Revised.

Motivation: Editorial glitch. BTW – these clauses have been removed, pursuant to adoption of 14/341r5.

**CID #2987:** (Michael Montemurro) 11.11.2.3, p. 103, l. 13:

Where is the description of how the keys are derived from the KDF output.

Eiher explicity show the Key derivations from the KDF output or point ot the existing sub-clauses where these are defined.

Suggested resolution: Reject.

Motivation: The keys are specified as substrings, in order, of the corresponding kdf-output and uniquely defined by their length.

**CID #2495:** (George Cherian) 11.11.2.4, p. 103, l. 40:

Change sentence: "Key confirmation for FILS authentication is carried in an Association Request followed by ...."

as in comment

Suggested resolution: Revised.

Suggested to change this line to “Key confirmation for FILS Authentication is implemented by an Association Request followed by and Association Response.

Note: this has not been addressed by adoption of 14/341r5.

**CID #2494:** (George Cherian) 11.11.2.4, p. 103, l. 6:

Acronym overload. TK is already defined as temporal key. This paragraph redefines it to be Traffic Key. I believe the intention is still Temporal Key, if not, pick a different acronym

Amend acronym

Suggested resolution: Accept.

Note: this has been addressed via adoption of 14/341r5.

**CID #2195:** (Dan Harkins) 11.11.2.3, p. 103, l. 14:

FILS needs to define how to generate a PMKID

A PMK is derived but there is no PMK identifier. Define one. And don't hash the PMK either. It should not be based on the PMK but, instead, based on data that uniquely generates the PMK (like the diffie-hellman exponentials)

Suggested resolution: Revised.

Note: this has been implemented by adoption of 14/341r5.

**CID #2199:** (Dan Harkins) 11.11.2.3, p. 103, l. 8:

The length of keys should depend on the AKM and not be hardcoded to 128 (or 256, depending on the key). This allows for security levels to be set and to use consistent cryptographic primitives.

Make the length of the keys derived, and therefore used (like the KEK and KCK) be based on the security level afforded by the AKM.

Suggested resolution: Revised.

Implemented with adoption of 14/341r5.

**CID #2205:** (Dan Harkins) 11.11.2.3, p. 103, l. 32:

Imposed requirements cannot be unactionable and vague

what does "used in exactly the same way as same-named keys" mean? What does this refer to? What does "(but now derived as specified above)" mean? If this is "but now" then what happens later? Entire sentence is vague and needs to be properly rewritten.

Suggested resolution: Revised.

Implemented with adoption of 14/341r5.

**CID #2971:** (Michael Montemurro) 11.11, p. 99, l. 3:

Where's the GTKSA or STKSA?

If this is a protocol for intfrastructure connections, it requires a GTKSA. Furthermore if it supports other types of conneections it requires support for a STKSA as well.

Suggested resolution: Revised.

With Infrastructure BSS, the GTKSA is used by the AP to encrypt group-addressed MPDUs (see 802.11-2012, Clause 11.5.1.8.8). In that case, it would indeed be beneficial to pass the GTKSA, as part of key confirmation from the AP to STA. However, this is already facilitated (see Table 11-6 of Clause 11.6.2 of 802.11-2012). As to STKSA: FILS authentication results in a secure and authentic channel between STA and AP. Since STKSA results from the set-up of a secure and authentic channel between two STAs connected to the same AP (see 802.11-2012, Clause 11.6.8), this is not part of FILS. Apart from GTKSA, one also should consider the IGTKSA, if appropriate.

Instructions to the Editor:

When incorporating <http://www.google.com.hk/url?sa=t&rct=j&q=11-14-0341-05-00ai-resolution-of-cids-11-2-3-to-7> into the draft, change the last sentence of the last para ofClause 11.11.2.4.2 as follows (new text underlined):

The STA installs the GTK and ~~sets~~ the ~~key~~ corresponding RSC. If management protection is negotiated, the STA installs the IGTK and the corresponding RSC. The STA and the AP establish GTKSA and IGTKSA. GTK and IGTK rekeying shall be performed as described in 11.6.7 (Group Key Handshake).