|  |
| --- |
| CR for CIDs relevant to device ID--part 2 |
| Date: 2023-7-10 |
| Author(s): |
| Name | Affiliation | Address | Phone | email |
| Jay Yang | ZTE Corporation |  |  | Yang.zhijie@zte.com.cn |
| Yan Li | ZTE Corporation |  |  |  |
|  |  |  |  |  |

Abstract

This submission proposes resolutions for the following CIDs:

1. 42，97，99, 124，125，126，127，146，181，

182，183，184，185，186，187, 188 ，227，265，281

R0: initial this draft.

R1: minor change according to off-line discussion.

R2: address the Editorial issue according to the comment from Jouni.

R3: update the resolution for CID181

R4: minor change according to the feedback during the call in 24th Oct.

R5: update based on the comment during the call in 31st Oct.

R6: update Figure 12-0a provided by Jose and the corresponding resolution

R7: update FIgure 12-0a and other comment resolution during the call in 16th Nov.

R8: update on CID227 according to the comment during the call in17th Nov.

Interpretation of a Motion to Adopt

A motion to approve this submission means that the editing instructions and any changed or added material are actioned in the TGbh D1.0 Draft. This introduction is not part of the adopted material.

***Editing instructions formatted like this are intended to be copied into the TGbh D1.0 Draft. (i.e. they are instructions to the 802.11 editor on how to merge the text with the baseline documents).***

***TGbh Editor: Editing instructions preceded by “TGbh Editor” are instructions to the TGbh editor to modify existing material in the TGbh draft. As a result of adopting the changes, the TGbh editor will execute the instructions rather than copy them to the TGbh Draft.***

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **CID** | **Page/line** | **Comment** | **Proposed Change** | **Resolution** |
| 12 | 30/40 | Clause 12.2.11 claims 'Exchanges of the device ID are protected from third parties'. However, if AEAD cipher mode for FILS is not used, message 2 of the 4 way handshake is not encrypted. Similar issue in the first PASN frame if PASN is used. | AP maintains a X509 public key certificate.Non-AP STA requests the AP's public key before authentication.Non-AP STA uses the AP's public key to encrypt the device ID in msg 2 of the 4-way and the first PASN frame. | Revised--For 4-way handshake message 2, it has a sentence to say “Encrypted Key Data = 1 when using an AEAD cipher or if the Device ID KDE is included”in 11bh draft0.1,but such sentence is missing in 11bh draft1.0, add it back to address such bug.For first PASN frame,the security rely on device ID that is different each time as the first PASN is not encrypted.TGbh editor to make the changes with the tag CID12 in 1353r4. |
| 97 | 32/32-35 | This statement is useless from a security point of view: "For the purposes of creating a Device ID without exposing the underlying device identification, the procedure in Annex AD, or any procedure (including nothing, if appropriate), can optionally be used by the AP to keep the Device ID content private ("opaque") from third parties." How can nothing be done while achieving the goal of not exposing the underlying device identification? You can do anything or nothing? This is not right. | Enumerate a list of security features that a compliant implementation MUST abide by in order to use device id. The text in AD.1 would be a good start. | Revised--change “(including nothing, if appropriate) to (including nothing if the Device ID is encrypted),”TGbh editor to make the changes with the tag CID97 in 1353r4. |
| 42 | 31/35 | Draft says: "(note that the encrypted form of devID1, i.e., "aa" is seen in the clear)."Saying that encrypted text is seen in the clear sounds like a contradiction.It's true that the encrypted data is visible on the medium, but "in the clear" is very much a synonym of "unencrypted".I assume the intention is to distinguish it from the case where opague ID is used, but wording should be improved. | Improve wording.See also Line 41 on page 31. | Revised--Agree in principle.Delete the text in the parentheses, and the same resolution in other instances.TGbh editor to make the changes with the tag CID42 in 1353r4 and replace Figure 12-0a with the Figure labeled by tag CID127 |
| 99 | 31/30-46 | The aa, bb, cc, dd stuff is pointless. | Get rid of the aa, bb, cc, dd stuff in the text and the figure. Saying "the encrypted form is seen in the clear" is also odd. Get rid of that sentence | Revised--Agree in principle.Delete the text in the parentheses, and the same resolution in other instances.TGbh editor to make the changes with the tag CID42 in 1353r4 and replace Figure 12-0a with the Figure labeled by tag CID127 |
| 124 | 31/36 | The sentence "note that the encrypted form of devID1, i.e., "aa" is seen in the clear" is self contradictory. How can something be encrypted and is also in the clear? | Delete the cited sentence. | Revised--Agree in principle.Delete the text in the parentheses, and the same resolution in other instances.TGbh editor to make the changes with the tag CID42 in 1353r4 and replace Figure 12-0a with the Figure labeled by tag CID127 |
| 125 | 31/36 | I'm not sure what "aa" is? I think it is the encrypted form of devID1 | Delete the cited sentence. | Revised--Agree in principle.Delete the text in the parentheses, and the same resolution in other instances.TGbh editor to make the changes with the tag CID42 in 1353r4 and replace Figure 12-0a with the Figure labeled by tag CID127 |
| 126 | 31/41 | There is no definition of "bb". I think it is the encrpted form of devID2. | Delete "bb" | Revised--Agree in principle.Delete the text in the parentheses, and the same resolution in other instances.TGbh editor to make the changes with the tag CID42 in 1353r4 and replace Figure 12-0a with the Figure labeled by tag CID127 |
| 127 | 32/1 | There are several issues with Figure 12-0a: 1) "DevID4" is not defined in the text and probably should be "devID4"; 2) "cc" and "dd" are not defined in the text; 3) "DevID1", "DevID2" and "DevID3" should be "devID1", "devID2" and "devID3"; 4) there are missing closing parentheses (x2) on the right hand side of the Figure. | Apply the changes in the comment to Figure 12-0a. | Revised--Agree in principle.TGbh editor to make the changes with the tag CID42 in 1353r4 and replace Figure 12-0a with the Figure labeled by tag CID127 |
| 187 | 32/29 | Missing closing parens on msg2 lines for bb and dd | As it says in the comment | Revised--Agree in principle.TGbh editor to make the changes with the tag CID42 in 1353r4 and replace Figure 12-0a with the Figure labeled by tag CID127 |
| 188 |  | Remove all the aa, bb, cc, dd stuff inc. in the figure, as it's just confusing | As it says in the comment | Revised--Agree in principle.TGbh editor to make the changes with the tag CID42 in 1353r4 and replace Figure 12-0a with the Figure labeled by tag CID127 |
| 265 | 32/8,9,18,19 | In Figure 12-0a the Auth Msg 1 and 2 between Non-AP-STA and AP-2, the device IDs (DevID1, DevID2, DevID3 and DevID3 should be lower case "devID1 ..... devID4" to align with draft text. | As commented | Revised--Agree in principle.TGbh editor to make the changes with the tag CID42 in 1353r4 and replace Figure 12-0a with the Figure labeled by tag CID127 |
| 281 | 32/1 | Clarify Figure 12-0a to make the timing of the "Next Connection" stuff more obvious, and the overlap (or lack thereof) of the Initial/Next Connection to AP-1 and AP-2 more clear. | As per comment | Revised--Agree in principle.Change “Next connection” to “return to the same ESS” in the figure.TGbh editor to make the changes with the tag CID42 in 1353r4 and replace Figure 12-0a with the Figure labeled by tag CID127 |
| 146 | 32/41 | Missing closing parentheses after (See 9.4.2.241 (RSNXE) | As in comment | Revised--Add the closing parentheses.TGbh editor to make the changes with the tag CID146 in 1353r4. |
| 181 | 31/30 | "with MAC1" not clear. "its MAC" not clear | Change to "with MAC address MAC1" and "its MAC address" respectively. Ditto "with MAC address MAC2" and "with MAC address MAC3" | Revised--Agree in principle.TGbh editor to make the changes with the tag CID181 in 1353r4. |
| 182 | 31/31 | "establish FTM session(s) with the ESS" -- FTM sessions are not established with ESSes | Change to "establish FTM session(s) in the ESS" | Accepted-- |
| 183 | 31/32 | "first PASNframe with device ID active" missing articles and not clear | Change to "the first PASNframe, indicating device ID is active" | Revised.Agree in principleRewording the sentence to “...the first PASN frame with Device ID Active field in the RSNXE set to 1”TGbh editor to make the changes with the tag CID183 in 1353r4  |
| 184 | 31/35 | "the encrypted form of devID1, i.e.,"aa" is seen in the clear" -- this is confusingly obvious | Change to "devID1 is encrypted". Simlarly "AP2 assigns another deviceID (devID2) encrypted to the non-AP STA in the second PASN frame ("bb" is seen in the clear)" -> "AP2 assigns another deviceID (devID2) and sends it encrypted in the second PASN frame", and "it sends the previously assigned device ID (devID2) and isassigned another device ID encrypted (devID3)" -> "it sends the previously assigned device ID (devID2) and isassigned another device ID (devID3), where both IDs are encrypted" | Revised. TGbh editor to make the changes with the tag CID184 in 1353r4. |
| 185 | 31/38 | "the encrypted form of devID1, i.e.,"aa" is seen in the clear" -- this is confusingly obvious | Change to "devID1 is encrypted". Simlarly "AP2 assigns another deviceID (devID2) encrypted to the non-AP STA in the second PASN frame ("bb" is seen in the clear)" -> "AP2 assigns another deviceID (devID2) and sends it encrypted in the second PASN frame", and "it sends the previously assigned device ID (devID2) and isassigned another device ID encrypted (devID3)" -> "it sends the previously assigned device ID (devID2) and isassigned another device ID (devID3), where both IDs are encrypted" | Revised. TGbh editor to make the changes with the tag CID184 in 1353r4. |
| 186 | 31/43 | "after deauthenticating from the ESS" -- you deauthenticate from BSSes, not ESSes | Delete "from the ESS" | Revised--TGbh editor please make the change labelled with CID186. |
| 227 | 31/30 | In the example of using PASN for FTM and Device ID, it is not clear why do you need to be identified in this specific use case. Is it for troubleshooting? better to explain the reason of the use case. | Provide explanation of why this use case makes sense for identification | Revised--In order to avoid the location issue based on MAC address by the 3rd party, the non-AP STA may use different MAC addresses in each FTM session. However, the non-AP STA may carry 11bh identifier when it’s desired to be located by the network.The is already insubcaluse 12.2.11(Changing MAC Address), no need extra clairification in this example. |

**CID 12.**

**TGbh editor: please replace the text with the following change( the same text in draft 0.1) in 12.7.6.3 4-way handshake message 2**

Message 2 uses the following values for each of the EAPOL-Key frame fields:

Descriptor Type = N - see 12.7.2 (EAPOL-Key frames)

Key Information:

Key Descriptor Version = 1 (ARC4 encryption with HMAC-MD5) or 2 (NIST AES key wrap

with HMAC-SHA-1-128) or 3 (NIST AES key wrap with AES-128-CMAC), in all other

cases 0 – same as message 1

Key Type = 1 (Pairwise) – same as message 1

Reserved = 0

Install = 0

Key Ack = 0

Key MIC = 0 when using an AEAD cipher or 1 otherwise

Secure = 0 – same as message 1

Error = 0 – same as message 1

Request = 0 – same as message 1

Encrypted Key Data = 1 when using an AEAD cipher or if the Device ID KDE is included, or 0

otherwise

Reserved = 0 – unused by this protocol version

Key Length = 0

Key Replay Counter = *n* – to let the Authenticator or initiator STA know to which message 1 this

corresponds

Key Nonce = SNonce

EAPOL-Key IV = 0

Key RSC = 0

Key MIC = Not present when using an AEAD cipher; otherwise, MIC(KCK, EAPOL) – MIC

computed over the body of this EAPOL-Key frame with the Key MIC field first initialized to 0

Key Data Length = length of Key Data field in octets

Key Data =

— included RSNE – the sending STA’s RSNE for PTK generation or peer RSNE for the current operating

band, and when this message 2 is part of a fast BSS transition initial mobility domain association

or an association started through the FT protocol, the PMKR1Name calculated by the S1KH according

to the procedures of 12.7.1.6.4 (PMK-R1) is included in the PMKID List field of the RSNE and

the FTE and MDE are also included, or

— The sending STA’s Multi-band element for PTK generation for a supported band other than the current

operating band if dot11MultibandImplemented is true, or

— The sending STA’s RSNE and Multi-band element(s) for generating a single PTK for all involved

bands, if dot11MultibandImplemented is true and both the Authenticator and the Supplicant use the

same MAC address in the current operating band and the other supported band(s); or

— The sending STA’s RSNE and Multi-band element(s) for generating a different PTK for each

involved band, if dot11MultibandImplemented is true and the Joint Multi-band RSNA subfield of

the RSN capabilities field is 1 for both the Authenticator and the Supplicant, and either the Authenticator

or the Supplicant uses different MAC addresses for different bands.

— Additionally, contains an OCI KDE when dot11RSNAOperatingChannelValidationActivated is true

on the Supplicant.

— Additionally, may include a Device ID KDE.

— The RSNXE that the Supplicant sent in its (Re)Association Request frame, if this element is present

in the (Re)Association Request frame that the Supplicant sent.

**12.2.11.1 Device ID indication**

**......**

To avoid being tracked by third parties, a non-AP STA may adopt a different MAC addresses in the different FTM sessions with multiple APs in the same ESS . The non-AP STA may use the device ID mechanism when it desires to be located by the network.(CID227)

Figure 12-0a (Example of device ID exchange in PASN) shows an example of a device ID exchange in PASN.

The example illustrates a non-AP STA performing PASN to establish FTM session(s) in the ESS containing AP1 and AP2. The non-AP STA with(CID181) a MAC address of MAC1 first initiates the connection with AP1 by sending the first PASN frame with Device ID Active field in the RSNXE set to 1(CID183). Upon receiving the first PASN frame, AP1 assigns a device ID (devID1) and sends it encrypted to the non-AP STA in the second PASN frame (CID42). The non-AP STA then continues to establish an FTM session with AP1. When the non-AP STA with (CID181) a MAC address of MAC2 (non-AP STA changing its (CID181)MAC address from MAC1 to MAC2) performs PASN with AP2 to establish another FTM session, the non-AP STA sends previously assigned device ID (devID1) to AP2 in the first PASN frame. Upon receiving the device ID (devID1) in first PASN frame, AP2 assigns another device ID (devID2) and sends it (CID184)encrypted to the non-AP STA in the second PASN frame(CID42). The non-AP STA then proceeds to establish the FTM session. Similarly, when the non-AP STA with(CID181) a MAC address of MAC3 returns to AP1(CID186), it sends the previously assigned device ID (devID2) and is assigned another encrypted device ID(CID184) (devID3) that will be used in the subsequent PASN for another FTM session.

CID 127





For purposes of creating a Device ID that can be sent over the air without exposing the underlying device

identification, the procedure in Annex AD, or any procedure (CID 97) (including nothing, if the Device ID is encrypted), can optionally

be used by the AP to keep the Device ID content private (“opaque”) from third parties.

CID 146

**12.2.11.2 Identifiable Random MAC address (IRM) operation**

A non-AP STA indicates activation of IRM for a particular ESS by setting the IRM Active field to 1 in the

Extended RSN Capabilities field (see 9.4.2.241 (RSNXE)) in (Re)Association Request frames sent to any AP in

the ESS. An