|  |
| --- |
| CR for CIDs in PASN ID |
| Date: 2024-4-30 |
| Author(s): |
| Name | Affiliation | Address | Phone | email |
| Yan Li | ZTE Corporation |  |  | Yan.li16@zte.com.cn |
| Jay Yang | ZTE Corporation |  |  |  |
|  |  |  |  |  |

Abstract

This submission proposes resolutions for the following CIDs:

3003 and 3015

R0: initial CR document

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 D4.0 Draft. This introduction is not part of the adopted material.

***Editing instructions formatted like this are intended to be copied into the TGbh D4.0 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** | **Comment** | **Proposed Change** | **Resolution** |
| 3003 | Device ID has the long term property, but if the AP assign non-ap STA with a Device ID that is used in the PASN procedure, the long term property will be broken. Further, the Device ID in PASN is required to be encrypted, but there is no such limition in 4HS. Therefore the characteristic of Device ID in 4HS and PASN is still different. | Seperate Device ID in 4HS from PASN procedure, e.g. define PASN ID in PASN procedure. | Revised—As the Device ID works as a long-term identifier during association(i.e., FILS authentication and 4-way handshake) and works as a short-term one during PASN authentication. It’s necessary to divide the original Device ID into current Device ID(for association) and PASN ID(for PASN authentication)Additionally, both of Device ID and PASN ID should be provided when the initial connection case or ‘Not recognized’ case happens. TGbh editor to make the changes in 11-24/0789r0 |
| 3015 | When using PASN, the device ID must change every authentication. If the same network wanted to provide a permanent device ID to that non-AP STA, then it is in trouble. We should have a way such that a temporary ID can be used, that is seperate from the permanent ID. | As the ID used with PASN is a temporary ID, it is proposed to use a different term - PASN ID. A proposal will be presented. | Revised—As the Device ID works as a long-term identifier during association(i.e., FILS authentication and 4-way handshake) and works as a short-term one during PASN authentication. It’s necessary to divide the original Device ID into current Device ID(for association) and PASN ID(for PASN authentication)Additionally, both of Device ID and PASN ID should be provided when the initial connection case or ‘Not recognized’ case happens.TGbh editor to make the changes in 11-24/0789r0 |

**Discussion about PASN ID initiated by graham:**

***Effectively a new scheme has been introduced that use a temporary ID that is provided securely, but then used in the open for the next PASN authentication. The term “device ID’ however has still been used. The point of the comment is that if the STA will also ever connect to the same network (APs) then a device ID should be used and retained. Hence, we can easily use a temporary “PASN ID” and allow the device ID to be retained. Alternatively, as this is a temporary ID it would be better to rename it so as to save confusion. The following are the instructions to use the term “PASN ID”. It is simply that if using PASN then the Device ID field is interpreted as a “PASN ID”.***

**3. Definitions, acronyms, and abbreviations**

**3.2 Definitions specific to IEEE Std 802.11**

***change the following definitions as below:***

**device identification (ID): [device ID] An ID that a network can provide to a non-access point (non-AP)**

**station (STA) to allow the non-AP STA to identify itself to a known network during association at a future time.**

**identifiable random medium access control (MAC) address: [IRM] A MAC address that can be used by**

**a non-access point (non-AP) station (STA) to identify itself to a network.**

**measurement identifier (ID): [measurement ID] A transient device ID that a network can provide to a non-access point (non-AP) station (STA) to allow the non-AP STA to identify itself to another access point (AP) in the same network during a radio measurement procedure.**

**preassociation security negotiation identification (ID): [PASN ID] A device ID that a network can provide to a non-access point (non-AP) station (STA) to allow the non-AP STA to identify itself to a known network during PASN authentication at a future time.**

**4. General description**

**4.5 Overview of the services**

**4.5.4 Access control and data confidentiality services**

**4.5.4.10 MAC privacy enhancements**

***Change the last paragraph as follows.***

**To mitigate this sort of traffic analysis a STA can support the ability to periodically and randomly change its MAC addresses and reset counters and seeds prior to association. Such a STA, upon reconnecting to a network, can provide either a device ID or a PASN ID previously provided by the network or can use an identifiable random MAC address (IRM) the STA previously provided to the network or both. Either approach allows the network to recognize the STA while providing protection against third party tracking or traffic analysis. While discovering networks, a STA can refrain from gratuitously transmitting Probe Request frames containing SSIDs of favored BSS networks.**

**6.5 MLME SAP primitives**

**6.5.7 Associate**

**6.5.7.3 MLME-ASSOCIATE.confirm**

**6.5.7.3.2 Semantics of the service primitive**

***Change the primitive parameters list as follows (not all parameters are shown):***

**The primitive parameters are as follows:**

**MLME-ASSOCIATE.confirm(**

**...**

**Device ID,**

**IRM,**

**PASN ID,**

**VendorSpecificInfo**

**)**

***Add the following rows to the parameter description table before the VendorSpecificInfo row (header row***

***shown for convenience):***

|  |  |  |  |
| --- | --- | --- | --- |
| **Name** | **Type** | **Valid Range** | **Description** |
| **Device ID** | **Device ID element** | **As defined in 9.4.2.316 (Device ID element)** | **Specifies the device ID for the requesting STA. Optionally present if dot11FILSActivated is true and dot11DeviceIDActivated is true, otherwise not present.** |
| **IRM** | **IRM element** | **As defined in 9.4.2.317 (IRM element)** | **Specifies the IRM for the requesting** **STA. Optionally present if dot11FIL-****SActivated is true and dot11IRMActi-****vated is true, otherwise not present.** |
| **PASN ID** | **PASN ID element** | **As defined in 9.4.2.xxx (PASN ID element)** | **Specifies the PASN ID for the requesting STA. Optionally present if dot11FILSActivated is true and dot11DeviceIDActivated is true, otherwise not present.** |

**6.5.7.5 MLME-ASSOCIATE.response**

**6.5.7.5.2 Semantics of the service primitive**

***Change the primitive parameters list as follows (not all parameters are shown):***

**The primitive parameters are as follows:**

**MLME-ASSOCIATE.response(**

**...**

**Device ID,**

**IRM,**

**PASN ID,**

**VendorSpecificInfo**

**)**

***Add the following rows to the parameter description table before the VendorSpecificInfo row (header row***

***shown for convenience):***

|  |  |  |  |
| --- | --- | --- | --- |
| **Name** | **Type** | **Valid Range** | **Description** |
| **Device ID** | **Device ID element** | **As defined in 9.4.2.316 (Device ID element)** | **Specifies the device ID for the requesting STA. Optionally present if dot11FILSActivated is true and dot11DeviceIDActivated is true, otherwise not present.** |
| **IRM** | **IRM element** | **As defined in 9.4.2.317 (IRM element)** | **Specifies the IRM for the requesting** **STA. Optionally present if dot11FIL-****SActivated is true and dot11IRMActi-****vated is true, otherwise not present.** |
| **PASN ID** | **PASN ID element** | **As defined in 9.4.2.xxx (PASN ID element)** | **Specifies the PASN ID for the requesting STA. Optionally present if dot11FILSActivated is true and dot11DeviceIDActivated is true, otherwise not present.** |

**9. Frame formats**

**9.3.3 Format of (PV0) Management frames**

**9.3.3.6 Association Response frame format**

***Insert the following new rows before the Vendor Specific field of Table 9-65 (Association Response frame body) (header row shown for convenience.)***

**Table 9-65—Association Response frame body**

|  |  |  |
| --- | --- | --- |
| **Order** | **Information** | **Notes** |
| **78** | **Device ID** | **If dot11DeviceIDActivated is true and dot11FILSActivated is true, the Device ID element is optionally present when using FILS authentication; otherwise, it is not present.** |
| **79** | **IRM** | **If dot11IRMActivated is true and dot11FILSActivated is true, the IRM element is optionally present when using FILS authentication; otherwise, it is not present.** |
| **80** | **PASN ID** | **If dot11DeviceIDActivated is true and dot11FILSActivated is true, the PASN ID element is optionally present when using FILS authentication; otherwise, it is not present.** |

**9.4.2 Elements**

**9.4.2.1 General**

***Insert the following new rows in Table 9-130 (Element IDs) (header row shown for convenience) as***

***appropriate.***

**Table 9-130—Element IDs**

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **Element** | **Element ID** | **Element ID Extension** | **Extensible** | **Fragmentable** |
| **Device ID (see** **9.4.2.316 (Device** **ID element))** | **255** | **138** | **No** | **No** |
| **IRM (see** **9.4.2.317 (IRM** **element))** | **255** | **139** | **Yes** | **No** |
| **PASN Encrypted** **Data element (see** **9.4.2.319 (PASN** **Encrypted Data** **element))** | **255** | **140** | **Subelements** | **Yes** |
| **PASN ID (see** **9.4.2.xxx (PASN** **ID element))** | **255** | **141** | **No** | **No** |

**9.4.2.319 PASN Encrypted Data element**

***change the following table as below:***

**Table 9-417c—Subelement IDs for Encrypted Data field of the PASN Encrypted Data element**

|  |  |  |
| --- | --- | --- |
| **Subelement** | **Name** | **Extensible** |
| **0** | **Device ID** | **No** |
| **1** | **IRM** | **No** |
| **2** | **PASN ID** | **No** |
| **3-220** | **Reserved** |  |
| **221** | **Vendor Specific** | **Vendor Defined** |
| **222-255** | **Reserved** |  |

***add the following before the paragraph “The Vendor Specific subelements have the same format as their corresponding elements...”***

**The format of the PASN subelement is shown in Figure 9-zzz(****PASN ID subelement format)**

|  |  |  |  |
| --- | --- | --- | --- |
| **Subelement ID** | **Length** | **PASN ID Status** | **PASN ID** |

**Octets: 1 1 1 variable**

**Figure 9-zzz PASN ID subelement format**

**The Subelement ID field is defined in Table 9-417c (Subelement IDs for Encrypted Data field of the PASN**

**Encrypted Data element).**

**The Length field is defined in 9.4.3 (Subelements).**

**The PASN ID status field and the PASN ID field are defined in 9.4.2.xxx (PASN ID element).**

***add the following subclause after 9.4.2.319 PASN Encrypted Data element:***

**9.4.2.xxx PASN ID element**

**The PASN ID element contains a PASN ID. The format of the PASN ID element is shown in Figure 9-**

**xxx (PASN ID element format).**

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| **Element ID** | **Length** | **Element ID Extension** | **PASN ID Length** | **PASN ID Status** | **PASN ID** |

**Octets: 1 1 1 1 1 variable**

**Figure 9-XXX** PASN ID element format

**The Element ID, Length, and Element ID Extension fields are defined in 9.4.2.1 (General).**

**The PASN ID Length field is the length of the PASN ID field.**

**When sent from an AP to a non-AP STA, the PASN ID Status field contains one of the values shown in**

**Table 9-yyy (PASN ID Status field values)**

**Table 9-yyy—PASN ID Status field values**

|  |  |  |
| --- | --- | --- |
| **PASN ID Status** | **Name** | **Meaning** |
| **0** | **Recognized** | **Indicates that the PASN ID has been recognized.** |
| **1** | **Not Recognized** | **Indicates that the PASN ID has not been recognized.** |
| **2-255** | **Reserved** |  |

**The PASN ID field contains a PASN ID.**

**NOTE—Optionally the PASN ID might be constructed as an opaque identifier as described in 12.2.12.1 (Device ID mechanism) (see Annex AF).**

**When the PASN ID element is sent from a non-AP STA to an AP, the PASN ID Status field is reserved.**

**12.2.12.1 Device ID mechanism**

**A STA should not send a frame containing a device ID (sub)element or a PASN ID (sub)element to any STA unless the receiving STA sets the Device ID Active field to 1 in the Extended RSN Capabilities field.**

**If a non-AP STA has a device ID configured, then it shall provide a device ID using the procedures described below:**

**1) When using FILS authentication, in the Device ID element in the Association Request frame.**

**2) When not using PASN or FILS authentication, in the Device ID KDE in message 2 of the 4-way handshake.**

**If a non-AP STA has a PASN ID configured, then it shall provide a PASN ID in the PASN ID element in the first PASN frame, when using PASN authentication.**

**An AP shall provide a device ID using the procedures described below:**

**1) When using FILS authentication, in the Device ID element in the Association Response frame.**

**2) When not using PASN or FILS authentication, in the Device ID KDE in message 3 of the 4-way handshake.**

**An AP shall provide a PASN ID in the PASN ID element in the second PASN frame, when using PASN authentication.**

**When a non-AP STA performs an initial connection with an AP during association or PASN authentication, the AP shall provide both of a device ID and a PASN ID using the procedure described below:**

**1）When using PASN authentication, a device ID in the Device ID subelement and a PASN ID in the PASN ID element in the second PASN frame.**

**2）When using FILS authentication, a device ID in the Device ID element and a PASN ID in the PASN ID element in the Association Response frame.**

**3）When not using PASN or FILS authentication, a device ID in the Device ID KDE and a PASN ID in the PASN ID KDE in message 3 of the 4-way handshake.**

**A STA may delete either or both of a stored device ID and a stored PASN ID at any point in time for implementation specific reasons (for example, configuration changes have lost the device ID or the PASN ID, or some time has passed since the last association to the ESS).**

**When a non-AP STA sends a device ID or a PASN ID to an AP, it shall use the device ID or the PASN ID most recently received from any AP belonging to the same ESS.**

**When an AP with dot11DeviceIDActivated equal to true receives a frame containing a device ID from a**

**non-AP STA and the AP recognizes the received device ID, the AP shall perform one of the following**

**actions:**

**1) Set the Device ID Status field of the Device ID KDE or Device ID element to 0 to indicate**

**that the AP recognizes the non-AP STA and set the Device ID field to zero length (indicating the**

**current device ID is maintained).**

**2) Assign a new device ID value in the Device ID field and set the Device ID Status field of the**

**Device ID KDE or Device ID element to 0 in the appropriate frame.**

**When an AP with dot11DeviceIDActivated equal to true receives a first PASN frame containing a PASN ID that it recognizes, the AP shall assign a new PASN ID value to the non-AP STA and include this new PASN ID in a PASN ID subelement in the second PASN frame, setting the PASN ID Status field of the PASN ID subelement to 0 to indicate Recognized.**

**When a non-AP STA receives a frame that contains a Device ID Status field in the Device ID KDE or Device ID element equal to 0, or a PASN ID Status field in the PASN ID subelement equal to 0,indicating Recognized, it may proceed with the assumption that the shared identity state with the AP or ESS (as per the concepts of 12.2.12 (Identifying a non-AP STA with changing MAC address)) is now bound to the Address 2 field in the Association Request frame or the first PASN frame most recently transmitted by the non-AP STA.**

**If an AP sets Device ID element or Device ID KDE with the Device ID Status field set to 1, indicating Not Recognized, then the AP may also provide in that same Device ID element or Device ID KDE a new device ID and in a new PASN ID element or PASN ID KDE a new PASN ID, thus establishing a new shared identity. An AP may set a Device ID Status field to 1 indicating “Not Recognized” if the AP cannot unequivocally identify the non-AP STA shared identity state.**

**if an AP sets PASN ID subelement with the PASN ID Status field set to 1, indicating Not Recognized, then the AP may also provide in that same PASN ID subelement a new PASN ID and in a new Device ID subelement a new Device ID, thus establishing a new shared identity. An AP may set a PASN ID Status field to 1 indicating “Not Recognized” if the AP cannot unequivocally identify the non-AP STA shared identity state.**

**When a non-AP STA receives a frame that contains a Device ID Status field in a Device ID KDE or Device ID element equal to 1, or a PASN ID Status field in a PASN ID subelement equal to 1, indicating Not Recognized, it shall assume that no shared identity state exists with the AP or ESS (as per the concepts of 12.2.12 (Identifying a non-AP STA with changing MAC address)).**

**Figure 12-0a (Example of PASN ID exchanges in PASN [138]) shows an example of a PASN ID exchange in PASN. The example illustrates a non-AP STA performing PASN to establish FTM session(s) in an ESS containing AP1 and AP2. The non-AP STA with a MAC address of MAC1 first initiates the connection with AP1 by sending the first PASN frame with the Device ID Active field in the RSNXE set to 1. Upon receiving the first PASN frame, AP1 assigns Both of a device ID (devID1) and a PASN ID (PASN ID1), and sends it encrypted to the non-AP STA in the second PASN frame. The non-AP STA then continues to establish an FTM session with AP1. When the non-AP STA performs PASN with AP2 to establish another FTM session, now with a MAC address for MAC2 after the non-AP STA has changed its MAC address, the non-AP STA sends the previously assigned PASN ID (PASN ID1) to AP2 in the first PASN frame. [269, 270, 271, 139] Upon receiving the PASN ID (PASN ID1) in first PASN frame, AP2 assigns another PASN ID (PASN ID2) and sends it encrypted to the non-AP STA in the second PASN frame. The non-AP STA then proceeds to establish the FTM session. Similarly, when the non-AP STA**

**returns to AP1, now with a MAC address of MAC3, it sends the PASN ID (PASN ID2) most recently assigned to the non-AP STA and is assigned another encrypted PASN ID (PASN ID3) to be used in the subsequent PASN for another FTM session.**



Figure 12-0a—Example of PASN ID exchanges in PASN

**12.7.2 EAPOL-Key frames**

**Table 12-10—KDE selectors**

|  |  |  |
| --- | --- | --- |
| **OUI** | **Data Type** | **Meaning** |
| **00-0F-AC**  | **20** | **Device ID KDE** |
| **00-0F-AC**  | **21** | **IRM KDE** |
| **00-0F-AC**  | **22** | **PASN ID KDE** |
| **00-0F-AC**  | **23-255** | **Reserved** |

***add the following descriptions of the new KDEs at the end of 12.7.2***

**The format of the PASN ID KDE is shown in Figure 12-50c (PASN ID KDE format).**

|  |  |
| --- | --- |
| **PASN ID Status** | **PASN ID** |

**Octets: 1 variable**

**The PASN ID Status field is defined in 9.4.2.XXX (PASN ID element).**

**The PASN ID field contains a PASN ID.**

**12.7.4 EAPOL-Key PDU notation**

***Add the following text after OCI KDE (shown for reference).***

**OCI KDE is the OCI KDE**

**Device ID KDE is the Device ID KDE, described in 9.4.2.316 (Device ID element)**

**IRM KDE is the IRM KDE, described in 9.4.2.317 (IRM element)**

**PASN ID KDE is the PASN ID KDE, described in 9.4.2.XXX (PASN ID element).**

**12.7.6 4-way handshake**

**12.7.6.1 General**

***Modify the following text as shown.***

**RSNA defines a protocol using EAPOL-Key frames called the 4-way handshake. The handshake completes the IEEE 802.1X authentication process. The information flow of the 4-way handshake is as follows:**

**Message 1:Authenticator  Supplicant: EAPOL-Key(0,0,1,0,P,0,0,ANonce,0,{} or {PMKID})**

**Message 2:Supplicant  Authenticator: EAPOL-Key(0,1,0,0,P,0,0,SNonce,MIC,{RSNE} or {RSNE,**

**OCI KDE} or {RSNE, RSNXE} or {RSNE, OCI KDE, RSNXE} or {RSNE, Device ID KDE} or {RSNE, OCI KDE, Device ID KDE} or {RSNE, RSNXE, Device ID KDE} or {RSNE, OCI KDE, RSNXE, Device ID KDE})**

**Message 3:AuthenticatorSupplicant: EAPOL-Key(1,1,1,1,P,0,KeyRSC,ANonce,MIC,{RSNE,GTK[N]} or {RSNE, GTK[N], OCI KDE} or {RSNE, GTK[N], RSNXE} or {RSNE, GTK[N], OCI KDE, RSNXE} or {RSNE, GTK[N], Device ID KDE} or {RSNE, GTK[N], OCI KDE, Device ID KDE} or {RSNE, GTK[N], RSNXE, Device ID KDE} or {RSNE, GTK[N], OCI KDE, RSNXE, Device ID KDE} or {RSNE, GTK[N], IRM KDE} or {RSNE, GTK[N]. OCI KDE, IRM KDE} or {RSNE, GTK[N], RSNXE, IRM KDE} or {RSNE, GTK[N], OCI KDE, RSNXE, IRM KDE} or {RSNE, GTK[N], Device ID KDE, PASN ID KDE} or {RSNE, GTK[N], OCI KDE, Device ID KDE, PASN ID KDE} or {RSNE, GTK[N], RSNXE, Device ID KDE, PASN ID KDE} or {RSNE, GTK[N], OCI KDE, RSNXE, Device ID KDE, PASN ID KDE})**

**12.7.6.4 4-way handshake message 3**

***Add the following text as shown to the list beginning “Key Data =”.***

**Key Data =**

**— ...**

**— Additionally, contains an OCI KDE when dot11RSNAOperatingChannelValidationActivated is true on the Authenticator.**

**— Additionally, may include a Device ID KDE and optionally a PASN ID KDE subject to the conditions at 12.2.12.1 (Device ID mechanism).**

**— Additionally, may include an IRM KDE subject to the conditions in 12.2.12.2 (Identifiable**

**random MAC address (IRM) operation).[174]**

**— The RSNXE that the Authenticator sent in its Beacon or Probe Response frame, if this element is present in the Beacon or Probe Response frame that the Authenticator sent.**

**12.13.3 Key establishment with PASN authentication**

**12.13.3.2 PASN frame construction and processing**

***Add the following text as shown at the end of the list that begins: “The first PASN authentication frame (see 9.3.3.11) of the exchange is constructed as follows:”***

**— If dot11DeviceIDActivated is true, including a PASN ID element as defined in 9.4.2.xxx (PASN ID element), if required per the procedure in 12.2.12.1 (Device ID mechanism).**

***Add the following text as shown in the list that begins: “— Derives the PTKSA; see 12.13.7.”***

**— If dot11RSNAOperatingChannelValidationActivated is true, including an OCI Element containing an OCI element as defined in 9.4.2.236 (OCI element), if dot11RSNAOperatingChannelValidationActivated is true.**

**— If dot11DeviceIDActivated is true, including a PASN Encrypted Data element, a PASN ID subelement and optionally a Device ID subelement as defined in 9.4.2.xxx(PASN ID element) and 9.4.2.316 (Device ID element) in the PASN Encrypted Data element, if required per the procedure in 12.2.12.1 (Device ID mechanism). The PASN Encrypted Data element shall be encrypted as defined in 12.2.13 (Encryption of the Encrypted Data field in the PASN Encrypted Data element in PASN).**

**(informative) Example opaque device identifier scheme**

**AF.1 General**

**This annex provides an example opaque identifier generation scheme that may be used to generate an identifier suitable for use in the Device ID field of the Device ID element** **(see 9.4.2.316 (Device ID element)) or in the PASN ID field of the PASN ID element (see 9.4.2.xxx (PASN ID element))as used in the procedure defined in 12.2.12.1 (Device ID mechanism). [247] These procedures require that the identifier precludes tracking by third parties. In addition to satisfying this requirement, this scheme also provides for countermeasures to deal with traffic analysis, precludes cutting-and-pasting of identities into conversations, prevents the same identifier from being used on distinct ESSs, and has an acceptable security level based on the birthday paradox.[248] It uses symmetric cryptography for speed and DoS resistance. It imposes minimal overhead on each frame that contains either or both of a device ID and a PASN ID, imposes minimal state retention requirements on an ESS (a single secret), and establishes a binding of each unwrapped identity assigned to a STA and the current opaque device identifier provided to it.**