IEEE P802.11  
Wireless LANs

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| CID 3015 Device ID and PASN | | | | |
| Date: 2024 - January | | | | |
| Author(s): | | | | |
| Name | Affiliation | Address | Phone | email |
| Graham SMITH | SR Technology | Sunrise, FL, USA. | 916 799 9563 | gsmith@srtrl.com |

Abstract

As the ID used with PASN is a temporary ID, it is proposed to use a different term and PASN ID is proposed.

**Background**

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| 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. | 31 | 12.2.12.1 | 41 | . |

The PASN device ID scheme uses a device ID that is provided securely, but then used in the open for the next PASN authentication. Hence, every authentication a new ID is required. So we have a problem, if this network wants to use a permanent device ID under the present scheme, IT MUST USE OPAQUE IDs.

An alternative is that we can easily use a temporary “PASN ID” and allow the device ID to be retained. In addition, 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”.

The proposed cheme is simply that if using PASN then the Device ID field is interpreted as a “PASN ID”.

***Instructions to use a PASN ID.***

**At P27.63 replace**

“The Device ID field contains a device ID.

NOTE—Optionally the device ID might be constructed as an opaque identifier as described in 12.2.12.1 (Device ID mechanism) (see Annex AD).[1]

With

“When a non-AP STA is associating with an AP, the Device ID field contains a device ID. When using PASN authentication, the Device ID field contains a PASN ID.”

NOTE—Optionally the Device ID field might contain an opaque identifier as described in 12.2.12.1 (Device ID mechanism) (see Annex AD).[1]

**Make following edits to clause 12.2.12.1:**

**12.2.12.1 Device ID mechanism**

An AP that has dot11DeviceIDActivated equal to true advertises activation of the device ID mechanism by setting the Device ID Active field to 1 in the Extended RSN Capabilities field (see 9.4.2.240 (RSNXE)) in Beacon and Probe Response frames.

A non-AP STA that has dot11DeviceIDActivated equal to true indicates the device ID mechanism is activated by setting the Device ID Active field to 1 in either the Extended RSN Capabilities field in (Re)Association Request frames or the first PASN frame that is sent to any AP that advertises activation of the device ID mechanism.

An AP that includes the PASN AKMP as part of the RSNE included in Beacon and Probe Response frames, i.e., when dot11PASNActivated is true, and has dot11DeviceIDActivated equal to true shall set dot11KEKPASNActivated to true.

A non-AP STA that has dot11DeviceIDActivated equal to true and intends to use PASN, i.e., when dot11PASNActivated is true, shall set dot11KEKPASNActivated to true.

An AP that has dot11DeviceIDActivated equal to true and that receives a (Re)Association Request frame or the first PASN frame that includes an Extended RSN Capabilities field with the Device ID Active field equal to 1 shall do one of the following:

— include an Extended RSN Capabilities element in the (Re)Association Response frame with the Device ID Active field set to 1.

— include an Extended RSN Capabilities element in the second PASN frame with the Device ID Active field set to 1.

To ensure correct operation of the device ID mechanism, all APs in the ESS need to have dot11DeviceIDActivated set to true.

NOTE—The criteria and mechanism to distribute device IDs throughout the ESS is out of scope for this standard. A STA should not send a frame containing a device 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 or PASN ID using the procedures described below

1) When using PASN authentication, provide a PASN ID in the Device ID element in the first PASN frame.

2) When using FILS authentication, provide a device ID in the Device ID element in the Association Request frame.

3) When not using PASN or FILS authentication, provide a device ID in the Device ID KDE in message 2 of the 4-way handshake.[263]

An AP shall provide a device ID or a PASN ID using the procedures described below:[58]

1) When using PASN authentication, provide a PASN ID in the Device ID subelement in the second PASN frame.[210]

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

3) When not using PASN or FILS authentication, provide a device ID in the Device ID KDE in message 3 of the 4-way handshake.[264]

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

When a non-AP STA sends a device ID or PASN ID to an AP, it shall use the device ID or PASN ID most recently received from the ESS of which the AP is a member.

When an AP with dot11DeviceIDActivated equal to true receives a frame containing a device ID or PASN 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 (sub)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 or PASN ID value in the Device ID field and set the Device ID Status field of the Device ID KDE or Device ID (sub)element to 0 in the appropriate frame.

When an AP with dot11DeviceIDActivated equal to true receives a first PASN frame containing a ~~device~~ PASN ID that it recognizes, the AP shall assign a new ~~device~~ PASN ID value to the non-AP STA and include this new ~~device~~ PASN ID in a Device ID element in the second PASN frame, setting the Device ID Status field of the Device 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 (sub)element 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 (sub)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 (sub)element or Device ID KDE a new device ID or 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.

When a non-AP STA receives a frame that contains a Device ID Status field in a Device ID KDE or Device ID (sub)element 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 device ID exchanges in PASN [138]) shows an example of a ~~device~~ 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 a ~~device~~ PASN ID (~~dev~~pasnID1) 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 ~~device~~ PASN ID (~~dev~~pasnID1) to AP2 in the first PASN frame. [269, 270, 271, 139] Upon receiving the ~~device~~ PASN ID (~~dev~~pasnID1) in first PASN frame, AP2 assigns another ~~device~~ PASN ID (~~dev~~pasnID2) 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 ~~device~~ PASN ID (~~dev~~pasnID2) most recently assigned to the non-AP STA and is assigned another encrypted ~~device~~ PASN ID (~~dev~~pasnID3) to be used in the subsequent PASN for another FTM session. [

**In Figure 12-0a**

replace

“(devID1)” with “(pasnID1)”

“(devID2)” with “(pasnID2)”

“(devID3)” with “(pasnID3)”