IEEE P802.11
Wireless LANs

|  |
| --- |
| Adding devID to Association |
| Date: 2024-01-11 |
| Author(s): |
| Name | Affiliation | Address | Phone | email |
| Dan Harkins | HPE |  |  |  |
|  |  |  |  |  |

Abstract

This submission addresses several comments from LB282 and proposes to add device ID to association frames even for non-FILS cases.

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| CID | Clause Number | Comment | Proposed Change | Resolution |
| 239 | 12.2.12.1 | providing a device ID in message 2 is too late | send the device ID in a (re)associate request when not doing PASN or FILS | Revised, see <this document> |
| 243 | 9.3.3.5 | send the device ID in a (re)associate request when not doing PASN or FILS | add device ID to an associate request and associate response even when FILS is not activated. If Annex AD is normative and required then the device ID will be opacified and it is safe to send it as part of the (unprotected) associate request. | Revised, see <this document> |
| 242 | Annex AD | make Annex AD normative and required | Move this opaque device identifier scheme into its own subsection in 12 and make it required along with device ID support. | Revised, see <this document> |
| 187 | Annex AD | "on distinct ESSs" not clear | Change to "in multiple ESSs" | Reject, you can’t know whether you have multiple objects unless you have a way of identifying distinct—i.e. recognizably different—instances of said object. |
| 188  | Annex AD | "It imposes minimal overhead on each frame" -- which frames are we talking about here? | Clarify | Revised, see <this document> |
| 189 | Annex AD | "It imposes minimal overhead on each frame and imposes minimal state retention requirements on an ESS (a single secret), and a binding of each unwrapped identity assigned to a STA and the current opaque device identifier provided to it." -- I can't work out what the bit after the comma means. Is this also something it imposes? Is imposing a binding desirable? | Clarify | Revised, see <this document> |
| 191 | Annex AD | How is n determined at both sides / negotiated? | Clarify | Reject, it does need to. The STA has no knowledge of the value of n. |
| 194 | Annex AD | "is embedded in the output ciphertext" -- how? Is this an action ("shall be embedded") or a statement of fact ("is to be found somewhere in") or what? | Clarify | Revised, see <this document> |
| 196 | Annex AD | "becomes part of the opaque device identifier" -- we don't want part of the identifier, we want all of it | Explain how the rest of the opaque DID is constructed | Revised, see <this document> |
| 198 | Annex AD | Is there any restriction on the pad length? Can it be 255? | Add a NOTE to clarify | Revised, see <this document> |

Discussion:

In draft 2 of TGbh we include the device ID in a PASN message in order to let the AP identify the device initiating the PASN connection. This can be the first message an AP gets and the AP is able to determine an identity of the sender. This same requirement exists for non-PASN connections. In fact, in 12.2.12 we even say, “The first mechanism, referred to as device ID, has the AP provide an identifier to the non-AP STA during association or PASN authentication that the non-AP STA can then report back to the AP during a future association or PASN authentication.” Yet we do not actually provide a way for the non-AP STA to “report back” on all non-PASN connections. Furthermore, device ID as written does not have as much utility as IRM because a non-AP STA can use a received IRM in its next association and the AP can identify it immediately (note: before the 4way HS), with device ID the AP will not know the identity of the non-AP STA until the conclusion of the 4way HS which is way too late.

To resolve this dichotomy, we need to add the device ID to all associate request frames. Since these frames do not have protection, the device ID that is provided in those frames needs to be of the opaque variety, that is, not the assigned long-term identity but and encrypted version of that that changes with each association. The existing informational annex provides a secure way of doing that so it makes sense to make the annex mandatory as part of this effort.

This will make use of device ID similar to IRM in that after the first association, the device will be known by an identifier received the previous association, and each association will generate a new identifier by which the non-AP STA can make itself known on the next association.

Since the Annex is moving, this is a perfect time to address some other comments it received.

*Instruct the editor to modify section 4.5.4.10 as indicated:*

**4.5.4.10 MAC privacy enhancements**

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, when reconnecting to a network, can provide a previously provided device ID or can use a previously provided MAC address (IRM), either of which allows the network to recognize the STA while mitigating the abilities of third parties to do tracking or traffic analysis. While discovering networks, a STA can refrain from gratuitously transmitting Probe Request frames containing SSIDs of favored BSS networks.

When using a device ID, the non-AP STA is identified by a long-term identifier, assigned by the AP during the initial association. This long-term identifier is encrypted each time the non-AP STA connects to the network such that the encrypted version is unique for each connection. The encrypted version obtained during an association is used to identify the non-AP STA in the next connetion. This ensures that encrypted device IDs cannot be used to track non-AP STAs or do traffic analysis.

*Instruct the editor to modify the identical text in 6.5.7.2, 6.5.7.3, 6.5.7.4, and 6.5.7.5 as indicated:*

|  |  |  |  |
| --- | --- | --- | --- |
| Name  | Type  | Valid Range  | Description  |
| Device ID  | Device ID element  | As defined in 9.4.2.311 (Device ID element)  | Specifies the device ID for the requesting STA. Optionally present if dot11DeviceIDActivated is true, oth- erwise not present.  |
| IRM  | IRM element  | As defined in 9.4.2.312 (IRM ele- ment)  | Specifies the IRM for the requesting STA. Optionally present if dot11FILSActivated is true and dot11IRMActivated is true, otherwise not present.  |

*Instruct the editor to modify section 9.3.3.5 and 9.3.3.6 as indicated:*

**9.3.3.5 Association Request frame format**

 **Table 9-64—Association Request frame body**

|  |  |  |
| --- | --- | --- |
| **Order**  | **Information**  |  **Notes**  |
| 60  | Device ID  | If dot11DeviceIDActivated is true, the Device ID element present ; otherwise, it is not present.  |
| 61  | IRM  | If dot11IRMActivated is true and dot11FILSActivated is true, the IRM element is optionally present when using FILS authentication; otherwise, it is not present.  |

**9.3.3.6 Associate Response frame format**

 **Table 9-65—Associate Respose frame body**

|  |  |  |
| --- | --- | --- |
| **Order**  | **Information**  |  **Notes**  |
| 78  | Device ID  | If dot11DeviceIDActivated is true, the Device ID element is present; 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.  |

*Instruct the editor to modify section 9.4.2.3.311 as indicated:*

**9.4.2.3.311 Device ID element**

The Device ID field contains a device ID generated by encrypting a long-term identifier (see 12.X.Y).

*Instruct the editor to modify section 12.2.12.1 as indicated:*

**12.2.12.1 Device ID mechanism**

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 and if the received frame does not contain a Device ID, generate a unique identifer to assign to this non-AP STA.
* include an Extended RSN Capabilities element in the second PASN frame with the Device ID Active field set to 1.

Correct operation of the device ID mechanism depends on all APs in the ESS being configured with dot11DeviceIDActivated set to true and a single symmetric key used for encrypting device IDs per 12.X.Y. Support of the device ID mechanism needs to be advertised by all APs in an ESS in Beacons and Probe Response frames.

A STA shall not send a frame containing a device ID element to any STA unless the receiving STA sets the Device ID Active field to 1 in the Extended RSN Capabilities field.

A non-AP STA shall provide a device ID when required by the procedures described below:

1. When using PASN authentication, in the Device ID element in the first PASN frame.
2. In the Device ID element in the Association Request frame.
3. When not using PASN or FILS authentication, in the Device ID KDE in message 2 of the 4 way handshake.

The AP shall decrypt a received device ID using the technique described in 12.X.Y. Failures of the procedure in 12.X.Y shall be treated as if the non-AP STA is an unrecognized device.

An AP shall provide a device ID when required by the procedures described below:

1. When using PASN authentication, in the Device ID element in the second PASN frame.
2. In the Device ID element in the Association Response frame.
3. When not using PASN or FILS authentication, in the Device ID KDE in message 3 of the 4 way handshake.

When an AP with dot11DeviceIDActivated equal to true receives an association request or a first PASN frame containing a device ID which is decrypted and recognized, the AP shall reencrypt the non-AP STA’s decrypted long term identity (per the technique of 12.X.Y) to generate a new device ID and assign that new device ID value to the non-AP STA, via setting a new device ID in the Device ID field with the Device ID Status field of the Device ID element set to 0 to indicate that the AP recognizes the non-AP STA in the second PASN frame.

*Instruct the editor to add a new subsection after 12.2.12.3, number it correctly, and modify all references in this document that refer to 12.X.Y to refer to this new subsection number:*

**12.2.12.3 Encryption of Device ID IE and IRM IE in PASN**

When using PASN authentication, the Device ID element shall be encrypted in PASN frame 2 (if present) and

then IRM element shall be encrypted in PASN frame 3 (if present) with the negotiated key wrap algorithm (see

Table 12-11-Integrity and key wrap algorithms).

To encrypt a Device ID element in PASN frame 2 or an IRM element in PASN frame 3, KEK shall be used, as

derived as part of PTK (see 12.13.7 (PTKSA derivation with PASN authentication)), with the negotiated key

wrap algorithm (see Table 12-11 (Integrity and key wrap algorithms)).

**12.X.Y Generation of device ID from long term identity**

**12.X.Y.1 General**

APs generate device IDs by encrypting a long-term identity used to identify a non-AP STA. This encrypted identity becomes the device ID field of the Device ID element (see 9.4.2.311 (Device ID element)) as used in the procedure defined in 12.2.12.1 (Device ID mechanism). This procedure prevents tracking of the identifier by third parties. This procedure 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. It uses symmetric cryptography for speed and DoS resistance. It imposes minimal overhead on each frame that contains a device ID, imposes minimal state retention requirements on an ESS (a single secret), and establishes a binding of the long-term identity assigned to a STA and the current device ID provided to it.

Device IDs are generated and processed by APs. To a non-AP STA they are indistinguishable from a

random string and have no significance.

**12.X.Y.2 Generation of opaque device identifiers**

The device ID generation scheme takes a unique identifier as input and uses AES-SIV in deterministic mode

to wrap the device ID to produce output. There is a single symmetric secret, *k*, shared by all APs in an ESS. The length of *k* is either 256 bits or 512 bits depending on whether AES-SIV-256 or AES-SIV-512 is used. There is also a shared value *n* which all APs in an ESS must share. It defines the size of a variable-length input into the generation of device IDs. The procedure is to prepend the identifier with a single octet indicating the number of random octets of padding that follow. For example, if there are 4 octets of padding added to mitigate traffic analysis, the identifier, *id*, might be padded as:

 *padded-id = 0x04 0xc8 0x34 0x9a 0x70 <id>*

The maximum amount of padding that can be added is determined by the size of identifier being padded and the value of n and is equal to 237 minus the sum of the length of the identifier and *n*. If there is no padding, a single octet of the value zero is prepended to the identifier.

The padded identifier is prepended with a variable-length input comprised of random octets called a tweak.

The length of the tweak is *n* in bits. This determines the baseline security of the scheme such that the probability of

a duplicate identifier being generated, assuming a worst case of no padding, would be 1/2(n/2). For example,

an 8 octet tweak would provide collision resistance of at least 1/232 (in addition to that provided by the

padding) and would be constructed as (assuming the values of the tweak are generated according to Annex

J.5):

 *tweaked-padded-id = 0x7e 0x17 0x54 0x82 0xf1 0xd0 0xaa 0x52 0x04 0xc8 0x34 0x9a 0x70 <id>*

The tweaked-padded-id is then passed to AES-SIV in deterministic mode as plaintext using *k* as a key to

produce the device ID.

**12.X.Y.3 Processing of opaque device identifiers**

All APs in an ESS use the same tweak length, *n*, for all device IDs which are generated and parsed.

APs that receive device IDs using the procedures described in 12.2.12 (Identifying a non-AP STA with changing MAC address), pass the device ID to AES-SIV with key *k*. If AES-SIV returns FAIL, the protocol using the device ID fails. If AES-SIV returns a plaintext, the (known-length) tweak is removed and the next octet, the pad length, is inspected to determine how many additional octets are removed to recover the original identifier, id. This identifier is checked to ensure that the non-AP STA’s identity uses the current opaque identity that was received. If so, the unwrapped long-term identity is passed up to the protocol using the scheme with an indication of success.

**12.X.Y.4 Using opaque device identifiers**

An AP that receives a device ID will extract the original identity and generate a new device ID for the STA. A new device ID should be generated with a pad length that differs from the pad length of the previous device ID.

The AP associates the new device ID with the non-AP STA’s identity.

**12.X.Y.5 Security of scheme**

The security guarantees of AES-SIV mean that it is computationally infeasible for an adversary to generate a

valid device ID that could be processed by an AP and it is computationally infeasible for an adversary to decrypt a valid device ID to determine the long-term identity.

Assuming the combination of tweak and pad are never repeated for a given identifier, the probability of a

given identity producing a device ID that has been used already is at least 1/2(n/2) where *n* is the number of bits of tweak. This probability can be lessened further by using different amounts of padding each time a new device ID is generated.

The overhead added to each frame that uses device IDs by this procedure is 16 octets of AES-SIV tag plus length of tweak plus one octet of padding indication plus padding.

*Instruct the editor to remove Annex AD*

**References:**