IEEE P802.11
Wireless LANs

|  |
| --- |
| Resolution of Annex AD Comments from LB282 |
| Date: 2024-01-16 |
| Author(s): |
| Name | Affiliation | Address | Phone | email |
| Dan Harkins | HPE |  |  |  |
|  |  |  |  |  |

Abstract

This submission addresses some comments received on Annex AD from LB282.

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| CID | Clause Number | Comment | Proposed Change | Resolution |
| 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. |
| 191 | Annex AD | How is n determined at both sides / negotiated? | Clarify | Reject, it does not need to be determined or negotiated at both sides. The STA has no knowledge of the value of n. |

Discussion: Reject

1. distinct is a necessary condition before knowing you have multiple anything. The term is fine.
2. Since opaque identifiers are indistinguishable from a random string their composition is not a concern of the non-AP STA.

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| CID | Clause Number | Comment | Proposed Change | Resolution |
| 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> |

Discussion: the sentence was poorly constructed. Instruct the editor to modify AD.1 as indicated:

**AD.1 General**

This annex provides an example for generating an identifier for 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). The requirements for using those procedures are that the identifier precludes tracking by third parties. In addition to satisfying those requirements, 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. 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 each unwrapped identity assigned to a STA and the current opaque device identifier provided to it.

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| CID | Clause Number | Comment | Proposed Change | Resolution |
| 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> |
| 195 | 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> |

Discussion: the makeup of ciphertext exported by SIV is irrelevant to this scheme. So just delete the sentence since it’s causing confusion. Instruct editor to modify section AD.2 as indicated:

**AD.2 Generation of opaque device identifiers**

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

produce the opaque device identifier.

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| CID | Clause Number | Comment | Proposed Change | Resolution |
| 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: Fine. Instruct the editor to modify section AD.2 as indicated:

**AD.2 Generation of opaque device identifiers**

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.

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| CID | Clause Number | Comment | Proposed Change | Resolution |
| 196 | Annex AD | "ensure that the non-AP STA's identity uses the current opaque identity that was received." -- not clear how an identity uses an identity that was received | Clarify | Revised, see <this document> |

Discussion: In AD.4 it notes that “The AP associates the new opaque identifier with the non-AP STA’s identity.” So the intention here is to check that the non-AP STA used the current opaque identifier associated with its identity.

Instruct the editor to modify section AD.3 as indicated:

**AD.3 Processing of opaque device identifiers**

APs that receive opaque device identifiers using the procedures described in 12.2.12 (Identifying a non-AP STA with changing MAC address), pass the opaque device identifier to AES-SIV with key k. If AES-SIV returns FAIL, the protocol using the opaque device identifier 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 opaque identity that was received is the current one associated with the identifier. If so, the unwrapped identity is passed up to the protocol using the scheme with an indication of success.

**References:**