IEEE P802.11
Wireless LANs

|  |
| --- |
| Rejected Groups in SAE |
| Date: 2021-05-18 |
| Author(s): |
| Name | Affiliation | Address | Phone | email |
| Dan Harkins | HPE |  |  |  |
| Jouni Malinen | Qualcomm |  |  |  |

Abstract

There is an ambiguity in the SAE specification that needs clarification.

Discussion: There is an ambiguity in whether a Rejected Groups element is always part of an SAE Commit message and whether an element with no Rejected groups (basically just the element ID, length, and extension ID) is included when there have been no rejected groups. Therefore, it is necessary to be more explicit about this.

*Instruct the editor to modify section 9.4.2.246 as indicated:*

**9.4.2.246 Rejected Groups element**

The Rejected Groups field contains one or more Finite Cyclic Group fields indicating all of the finite cyclic groups that have been rejected by a peer in a previous authentication attempt.

*Instruct the editor to modify section 12.4.7.4 as indicated:*

**12.4.7.4 Encoding and decoding of SAE Commit messages**

An SAE Commit message shall consist of a Finite Cyclic Group field (9.4.1.42 (Finite Cyclic Group field)) indicating a group, a Scalar field (9.4.1.39 (Scalar field)) containing the scalar, and an FFE field containing the element (9.4.1.40 (FFE field)). If the SAE Commit message is in response to an Anti-Clogging Token field request (see 12.4.7.6 (Status codes)), the Anti-Clogging Token field is present (see 9.4.1.38 (Anti-Clogging Token field)). When the PWE is derived using the hash-to-element method, the Anti-Clogging Token field is encapsulated in an Anti-Clogging Token Container element; otherwise, the Anti-Clogging Token field is included in the frame outside of an element as described in Table 9-41 (Presence of fields and elements in Authentication frames). If a password identifier is used in generation of the password element (PWE) the Password identifier element shall be present and the identifier shall be encoded as a UTF-8 string in the Identifier portion of the element (see 9.4.2.216 (Password Identifier element)). If an SAE Commit message with status code set to SAE\_HASH\_TO\_ELEMENT is being sent in response to rejection of a previous SAE Commit message with status code set to UNSUPPORTED\_FINITE\_CYCLIC\_GROUP, the group that was rejected shall be appended, after the rejected groups from previous attempts if applicable, to the Rejected Groups field of the Rejected Groups element. Each rejected group shall be represented as an unsigned 16-bit integer using the bit ordering conventions of 9.2.2 (Conventions). If the status code of the SAE Commit message is SAE\_HASH\_TO\_ELEMENT and if any groups have been rejected during the current SAE session, the Rejected Groups element shall be present, otherwise it shall not be present.

**References:**