IEEE P802.11  
Wireless LANs

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| Rejected Groups in SAE redux | | | | |
| Date: 2021-07-10 | | | | |
| Author(s): | | | | |
| Name | Affiliation | Address | Phone | email |
| Mark RISON | Samsung Cambridge Solution Centre | SJH, CB4 0DS, U.K. | +44 1223 434600 | at samsung (a global commercial entity) I'm the letter emme then dot rison |
| Based on work in 21/0871 by: |  |  |  |  |
| 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 include 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)), an Anti-Clogging Token field shall be included (see 9.4.1.38 (Anti-Clogging Token field)). When the password element (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 PWE a Password Identifier element shall be included and the identifier shall be encoded as a UTF-8 string in the Identifier field (see 9.4.2.216 (Password Identifier element)).

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 included (see (9.4.2.246 Rejected Groups element)), otherwise it shall not be included.

nany

NOTE—is(see 9.4.1.42 (Finite Cyclic Group field))

**References:**