IEEE P802.11  
Wireless LANs

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| SAE password identifier update | | | | |
| Date: 2025-02-27 | | | | |
| Author(s): | | | | |
| Name | Affiliation | Address | Phone | email |
| Jouni Malinen | Qualcomm Technologies, Inc. |  |  | jouni@qca.qualcomm.com |
|  |  |  |  |  |

Abstract

This submission proposes a mechanism to meet the approved P802.11bi requirement 1 to prevent an eavesdropper distinguishing whether authentication exchanges between CPE Client and CPE AP use identical SAE credentials or distinct SAE credentials by changes in the SAE password identifier after each successful use. This is an alternative approach for addressing this requirement (the approach using HPKE to protect the password identifier without changing the actual identifier is described in described in 24-46r4).

r1: Extended delivery of a new password identifier to allow a list of one or more password identifiers to be deliveried.

r2: Updated for IEEE P802.11bi/D1.0. Added a note to describe how password sharing between multiple devices of a user could be enabled. Added a requirement for APs to not share the password identifiers with 3rd parties.

**Discussion**

TGbi has approved a document describing the requirements for the project:

<https://mentor.ieee.org/802.11/dcn/21/11-21-1848-16-00bi-requirements-document.docx>

This contribution proposes draft text changes to address Requirement 1:

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
|  | **Requirement** | **Issue / Use Case Reference** | **Status** | **Information** |
| 1 | 11bi shall define a mechanism to prevent an eavesdropper distinguishing whether authentication exchanges between CPE Clients and CPE AP use identical **SAE credentials** or distinct SAE credentials (where a CPE AP supports multiple SAE credentials). | I1, I5 | Approved | Proposed - 22/107r2  (9 March 2022)  To be motioned –agreed by unanimous consent 4/21/2022  **Approved** (Motion #13, 13 May 2022) |

|  |  |
| --- | --- |
|  | **Issues/Use Cases** |
| I1 | **Protecting password identifiers** |
| I5 | **Protecting authentication identifiers and key identifiers** |

This document proposes a mechanism that changes the SAE password identifier after each successful use to avoid tracking of a STA based on the otherwise persistent identifier. This addressed the requirements approved for the TGbi Requirement 1.

**P802.11bi/D1.0 LB288 CID ????**

Comment:

IEEE P802.11bi/D1.0 does not address the approved TGbi requirement 1 in 21-1848r16 ("11bi shall define a mechanism to prevent an eavesdropper distinguishing whether authentication exchanges between CPE Clients and CPE AP use identical SAE credentials or distinct SAE credentials (where a CPE AP supports multiple SAE credentials).")  
This needs to be addressed to allow the baseline functionality for multiple SAE passwords to be used in cases where the password identifier might contain identifiable information (e.g., a user's name).

Proposed Change:

Add privacy protection for SAE password identifiers by incorporating the proposed changes from https://mentor.ieee.org/802.11/dcn/25/11-25-0155-02-00bi-sae-password-identifier-update.docx.

Proposed Resolution:

REVISED. Allow the SAE password identifier to be changed to avoid persistent use of the same identifier by incorporating the proposed changes from <this document>.

**Proposed changes**

* RSNXE

*Insert following row at the end of Table 9-373 (Extended RSN Capabilities field) (P802.11bi/D1.0 P60 L53:*

|  |  |  |
| --- | --- | --- |
| Bit | Information | Notes |
| <ANA> | SAE Password Identifier Change Support | A non-AP STA that supports changing the SAE Password Identifier sets this to 1. Otherwise, this is set to 0. |

*Modify 12.4.3 (title and REVme/D7.0 P3002 L32) as indicated:*

**12.4.3 Representation of passwords and password identifiers**

...

In an infrastructure BSS for which an SAE AKM is indicated, the AP shall set the SAE Password Identifiers In Use subfield of the Extended Capabilities field of the Extended Capabilities element to 1 if any entry in the dot11RSNAConfigPasswordValueTable has a non-NULL dot11RSNAConfigPasswordIdentifier, and shall set it to 0 otherwise. Similarly, an AP shall set the SAE Password Identifiers Used Exclusively subfield of the Extended Capabilities field of the Extended Capabilities element to 1 if every entry in the dot11RSNAConfigPasswordValueTable has a non-NULL dot11RSNAConfigPasswordIdentifier and shall set it to 0 otherwise.

SAE password identifiers can expose information that a passive attacker could use to identify and track STAs that authenticate to a network. To provide privacy, the password identifier can be changed for each use. A list of new password identifiers can be provided in message 3 of the 4-way way handshake after a successful SAE authentication when the non-AP STA and the AP support the mechanism for updating SAE password identifiers. The non-AP STA indicates its support using the SAE Password Identifier Change Support bit in the RSNXE. The AP indicates its support by providing a list of new password identifiers in an SAE Password Identifiers KDE. When an AP in an ESS provides a list of password identifier, those new password identifiers can be used with all APs in the ESS and previously used password identifiers are deleted. The AP decision on when to update the password identifiers and how many active password identifiers to provide are outside the scope of this standard. However, an AP should update the list of password identifiers in a manner that prevents need for the non-AP STA to reuse the same identifier. The AP shall not share the list of password identifiers with third parties outside the set of APs in the ESS to avoid exposing information that might be used to track the STA.

NOTE—The list of active SAE password identifiers might also be updated using out-of-band mechanisms. Such mechanisms are outside the scope of this standard. An initially configured password identifier might be allowed to be used after password identifier updates if the identified password is allowed to be shared between multiple devices. This would allow such devices to receiver their unique set of password identifiers.

When a non-AP STA has more than one password identifier available for a password it uses for SAE authentication, the STA may use any of the password identifiers to identify the password. The STA should select which password identifier to use in a manner that avoids reuse of the same value.

* EAPOL-Key frames

*Modify 12.7.2 as shown (P802.11bi/D1.0 P115 L19):*

***Modify Table 12-10 (KDE selectors) (not all lines shown) as follows:***

* KDE selectors

|  |  |  |
| --- | --- | --- |
| OUI | Data type | Meaning |
| 00-0F-AC | 23 | PGTK KDE |
| 00-0F-AC | <ANA> | SAE Password Identifiers KDE |

***Insert the following at the end of 12.7.2 (EAPOL-Key frames):***

* Revme D7.0 up to Figure 12-50, 11be D7.0 up to Figure 12-50h

The format of the PGTK KDE is shown in Figure 12-50i (PGTK KDE format).

|  |  |  |
| --- | --- | --- |
|  | PGTK Switch Time Indication | PGTK |
| Octets: | 8 | 32 |
| * PGTK KDE format | | |

The PGTK Switch Time Indication field indicates the time at which the PGTK indicated in the Key field shall be applied to replace the PGTK in use by the EDP AP MLD and EDP non-AP MLDs. The 8 octet PGTK Switch Time Indication is set to the time at which the PGTK contained in the PGTK field shall be applied by the EDP AP MLD and the EDP non-AP MLDs using, as a time-base, the value of the TSF corresponding to the BSS identified by the BSSID of the frame containing the PGTK KDE.

The PGTK field contains the PGTK.

The format of the SAE Password Identifiers KDE is shown in Figure 12-50j (SAE Password Identifiers KDE format).

|  |  |
| --- | --- |
|  | SAE Password Identifier Tuples |
| Octets: | variable |
| Figure 12-50j—SAE Password Identifiers KDE format | | |

The SAE Password Identifier Tuples field contains one or more SAE Password Identifier Tuple fields.

The format of the SAE Password Identifiers Tuple field is shown in Figure 12-50k (SAE Password Identifier Tuples field format).

|  |  |  |  |
| --- | --- | --- | --- |
|  | SAE Password Identifier Length | | SAE Password Identifer |
| Octets: | 1 | | variable |
|  | | Figure 12-50k—SAE Password Identifier Tuple field format | | |

The SAE Password Identifier Length field indicates the length of the following SAE Password Identifier field.

The SAE Password Identifier field contains an SAE Password Identifier.

**12.7.6.4 4-way handshake message 3**

*Modify 12.7.6.4 (REVme/D7.0 P3113 L65) as indicated:*

Key Data =

…

— The RSNXE that the Authenticator sent in its Beacon or Probe Response frame, if this element is present in the Beacon or Probe Response frame that the Authenticator sent.

— The SSID element containing the SSID of the BSS when both the Authenticator and the Supplicant have indicated support for SSID protection in the RSNXE.

— When SAE was used with a password identifier and the non-AP STA indicated support for changing the SAE password identifiers, optionally contains the SAE Password Identifiers KDE.