IEEE P802.11
Wireless LANs

|  |
| --- |
| SAE password identifier update |
| Date: 2025-01-13 |
| Author(s): |
| Name | Affiliation | Address | Phone | email |
| Jouni Malinen | Qualcomm Technologies, Inc. |  |  | jouni@qca.qualcomm.com |
|  |  |  |  |  |

Abstract

This submission proposes a mechanism to neet 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 TGbi CC49 CID 1097 (the approach using HPKE to protect the password identifier without changing the actual identifier is described in described in 24-1319r0).

**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.

**TGbi CC49 CID 1097**

Comment:

IEEE P802.11bi/D0.4 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/24/11-24-0046-01-00bi-privacy-protection-for-sae-credentials.docx.

Proposed Resolution:

REVISED. Allow the SAE password identifier to be changes 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):*

|  |  |  |
| --- | --- | --- |
| 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 after each use. A new password identifier is 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 provided a new password identifdier in a New SAE Password Identifier KDE. When an AP in an ESS provides a new password identifier, that new password identifier can be used with all APs in the ESS.

* EAPOL-Key frames(#1001)

*Modify 12.7.2 as shown:*

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

* KDE selectors

|  |  |  |
| --- | --- | --- |
| OUI | Data type | Meaning |
| 00-0F-AC | 23(#ANA) | PGTK KDE |
| 00-0F-AC | <ANA> | New SAE Password Identifier KDE |

***Insert the following at the end of 12.7.2 (EAPOL-Key frames(#1001)):***

* 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 New SAE Password Identifier KDE is shown in Figure 12-50j (New SAE Password Identifier KDE format).

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

The New SAE Password Identifier field indicates the next 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 New SAE Password Identifier KDE.