IEEE P802.11  
Wireless LANs

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| RSNXE in PASN | | | | |
| Date: July 16, 2020 | | | | |
| Author(s): | | | | |
| Name | Affiliation | Address | Phone | email |
| Nehru Bhandaru | Broadcom | 250 Innovation Drive, San Jose CA | +1 408 391 2159 | [nehru.bhandaru@broadcom.com](mailto:nehru.bhandaru@broadcom.com) |

Abstract

RSN Extension Element (RSNXE) is being used to carry Secure LTF and other capabilities that are used for secure timing measurement defined in the current 11az Draft. RSNXE is confirmed as part of Security Association (SA) setup messages (e.g. 4-way handshake) when the SA is setup as part of or after 802.11 (re)association. This document presents a proposal for inclusion of RSNXE in PASN messages and its confirmation as part of validation procedure used in PASN. Proposed changes are relative 11az Draft 2.2 and 11md Draft 3.4.

**References**

[1] IEEE P802.11-REVmdTM/D3.4, July 2020

[2] IEEE P802.11az™/D2.2 April 2020

**Discussion**

RSN Extension Element (RSNXE) is being used to carry Secure LTF and other capabilities that are used for secure timing measurement defined in the current 11az Draft. RSNXE is confirmed as part of Security Association (SA) setup messages (e.g. 4-way handshake - 12.7.2 EAPOL-Key frames) when the SA is setup as part of or after 802.11 (re)association.

See 9.4.2.241 RSN Extension element (RSNXE), and Table 9-94 (Element ID 244) in [1]

11-20-0698r2 proposed moving Secure LTF supported and Range Negotiation requires Security policy to RSNXE.

RSNXE is also used to communicate and confirm other aspects of security negotiation e.g. SAE-hash-to-element.

It is necessary to include and confirm RSNXE in PASN messages.

RSNXE is present in Beacons and (re)association request/response messages – See Tables 9-34, 9-36, 9-37 in [1]. It is present if there the sender has \*any\* capability that is signaled in RSNXE.

RSNXE is validated and confirmed as part of PASN key derivation and MIC computation – just like RSNE. RSNXE from non-AP STA is confirmed in PASN message 3 from the non-AP STA that includes hash of M1 body. RSNXE from AP in the frame and the Beacons is confirmed in PASN message 2 from the AP.

This document proposes the corresponding changes to PASN related text in [2] summarized below.

* Update to MLME-authenticate primitives
* PASN authentication text (12.13)
* PASN figure 12-54a – to include RSNXE

**Proposed Changes**

**Tgaz Editor: replace the ‘Valid Range’ cell for ‘Content of PASN Authentication frame’ with the following in MLME primitives MLME-Authenticate.request (p25.1), MLME-Authenticate.confirm (p26.1), MLME-Authenticate.indication (p26.12), MLME-Authenticate.response (p27.11)**

As defined in 12.13.3.2 PASN Frame Construction and Processing. 9.4.2.24 (RSNE), 9.4.2.241 (RSNXE), 9.4.2.187 (Wrapped Data element), 9.4.2.301 (PASN Parameters element), 9.4.2.48 (Timeout Interval element)

**Tgaz Editor: Add the following line after the sentence ‘RSNE is present…’ in Table 9-43 (snapshot below) to include the conditions under which RSNXE is present in these frames in the first two rows (Authentication transaction sequence numbers 1 and 2)**

RSNXE is present if any subfield of the Extended RSN Capabilities field in this element, except the Field Length subfield, is nonzero.

**![A screenshot of a cell phone

Description automatically generated]()**

**Tgaz Editor: Change 12.13.1 General (p182.5) as follows to indicate downgrade protection also for RSNXE**

The security of PASN depends on assumptions similar to those for FILS and SAE authentication. In particular:

— It assumed that both the STAs have in common at least one cyclic group from the dot11RSNAConfigDLCGroupTable that is used to select the ephemeral key exchange parameters.

— Protection is provided against downgrade attacks that may alter security parameters (e.g. RSNE, RSNXE, Group, Hash Function) used in the negotiation.

— Denial of service protection is not guaranteed.

**Tgaz Editor: Change the construction of first PASN frame (p185.1)**

The first PASN Authentication frame (see 9.3.3.11 (Authentication frame format)) of the exchange is constructed as follows:

…

— Optionally including 9.4.2.48 (Timeout Interval element (TIE)) with Timeout Interval Value set to dot11RSNAConfigPASNPTKSATimeout and Timeout Interval Type set to 2 (key lifetime interval);

— Including RSNXE (9.4.2.241 RSN Extension Element (RSNXE)) if any subfield of the Extended RSN Capabilities field in this element, except the Field Length subfield, is nonzero

**Tgaz Editor: Change the construction of the second PASN frame as follows**

**(p186.19)**

Otherwise, if the validation is successful, the AP with the chosen finite cyclic group, generates an ephemeral (random) private key, and uses the selected group’s scalar operation with the private key to generate its ephemeral public key.

— Derives the PTKSA; see 12.13.7 (PTKSA derivation with PASN authentication)

— Constructs and includes in the second PASN frame

— An RSNE that contains

…

**(p187.9)**

— Optionally including 9.4.2.48 (Timeout Interval element (TIE)) with Timeout Interval Value set to dot11RSNAConfigPASNPTKSATimeout and Timeout Interval Type set to 2 8 (key lifetime interval).

— Including RSNXE (9.4.2.241 RSN Extension Element (RSNXE)) that is advertised in AP’s Beacon and Probe Response frames, if any subfield of the Extended RSN Capabilities field in this element, except the Field Length subfield, is nonzero.

…

**Tgaz Editor: Change the construction of the MIC for second PASN frame as follows**

**(P192.27)**

**12.13.8.1 MIC Computation for PASN second frame**

The MIC field of the MIC element in the PASN second frame is set by the AP to first MMM octets of

HMAC-HASH (KCK, BSSID||SPA||Beacon RSNE||Beacon RSNXE||Frame Data)

Where

…

**(P193.1)**

SPA is the MAC address of the non-AP STA, the transmitter of the first PASN frame.

Beacon RSNE is the RSN element sent in the Beacons transmitted by the AP.

Beacon RSNXE is the RSNXE sent in the Beacons transmitted by the AP.

Frame Data is the body of the PASN second frame including the MIC element with the Octets in the MIC field of the MIC element set to 0.

…

Beacon RSNE and Beacon RSNXE are ~~is~~ included in the MIC computation so that a downgrade attack with forged RSNE Beacons will result in a MIC mismatch and thus PASN authentication failure.

**Tgaz Editor: Replace Figure 12-54a PASN Authentication with the following – [RSNXE] is added to first and second messages.**

A screenshot of a cell phone

Description automatically generated