IEEE P802.11
Wireless LANs

|  |
| --- |
| PDT Secure Communication - General |
| Date: 2025-10-13 |
| Author(s): |
| Name | Affiliation | Address | Phone | email |
| Hui Luo | Infineon |  |  | Hui.Luo@infineon.com |
|  |  |  |  |  |
|  |  |  |  |  |
|  |  |  |  |  |
|  |  |  |  |  |
|  |  |  |  |  |

Abstract

This document contains Proposed Draft Text (PDT) for secure communication - general of the proposed TGbp (AMP, Ambient Power) amendment to the 802.11 standard.

Rev 0: Initial version

# Introduction

Interpretation of a Motion to Adopt

A motion to approve this submission means that the editing instructions and any changed or added material are actioned in the TGbp Draft. The abstract, revision information, introduction, explanation of the proposed changes and references sections are not part of the adopted material.

***Editing instructions formatted like this are intended to be copied into the TGbp Draft (i.e. they are instructions to the 802.11 editor on how to merge the text with the baseline documents).***

## Explanation of the proposed changes:

The proposed changes to the 802.11 TGbp draft within this document are based on the following motions adopted by the TGbp task group:

### Relevant motions [1]:

[Motion #26]

* 11bp defines a mechanism to support secure communications for 802.11bp clients.

[Motion #44]

* IEEE 802.11bp will specify secure data communication methods that do not require maintaining security associations.
* Note:
	+ The methods are based on existing 802.11 security protocols.
	+ The security for backscattering AMP devices are TBD.
	+ The details are TBD.

[Motion #64]

* 802.11bp defines a mechanism to generate a transient key for an AMP non-AP STA that supports secure communication, where:
	+ An AMP AP transmits a downlink frame containing an ANonce.
	+ After receiving the downlink AMP frame from the AMP AP that contains an ANonce, an AMP non-AP STA generates an SNonce.
	+ The AMP non-AP STA generates a transient key using the ANonce, the SNonce, the Authenticator Address (AA), the Supplicant Address (SA), and a Pairwise Master Key (PMK) between the AP and the client.
	+ Note—Whether to include backscatter non-AP STAs in this procedure is TBD.

[Motion #65]

* 802.11bp defines a mechanism to generate a transient key for an AMP AP that supports secure communication, where:
	+ In response to the DL AMP frame from the AMP AP that contains an ANonce, the AMP AP receives an UL AMP frame from an AMP non-AP STA that carries the SNonce and a MIC.
		- The AMP non-AP STA generates the MIC using the derived transient key at the AMP non-AP STA.
		- If the uplink AMP frame is carrying any UL data, the data payload portion of the uplink AMP frame may be encrypted using the transient key generated at the AMP non-AP STA.
	+ If the MIC is verified:
		- The AP uses the ANonce it transmitted in the previous downlink AMP frame, the SNonce, the Authenticator Address (AA), the Supplicant Address (SA), and the PMK to generate the transient key.
		- Using the generated transient key, the AMP AP decrypts the UL data payload (if the payload was encrypted).
	+ Note—Whether to include backscatter non-AP STAs in this procedure is TBD.

[Motion #66]

* The transient key generation at the AP and the AMP client in 802.11bp may occur concurrently with AMP downlink and uplink data communication:
	+ The downlink AMP frame from the AP carries ANonce along with downlink data from the AP (e.g., AMP trigger).
	+ The uplink AMP frame from the AMP client carries SNonce and MIC along with the UL data (e.g., UL response to the AMP trigger).
		- The UL data may be encrypted using the transient key generated at the AMP non-AP STA.
	+ Note—Whether to include backscatter non-AP STAs in this procedure is TBD.

[Motion #113]

* 11bp shall specify a low-complexity secure method to generate and update a PMK for secure AMP communication between an AMP AP and an AMP non-AP STA?
	+ Note:
	+ The secure AMP communication method is defined in Motion 64, 65, 66.
	+ Whether to include backscatter non-AP STAs in this method is TBD.

**Text to be adopted begins here:**

***TGbp editor: Please add the following text in subclause 4.3.35 Ambient Power (AMP) AP and non-AP AMP STA of the 802.11bp draft D0.1:***

3. AMP MAC

3.5 Secure communication

3.5.1 General

An AMP AP can communicate with a non-AP AMP STA with security assurance, except that backscatter non-AP AMP STAs may not use the security method described in this specification.

Security assurance for AMP communication between an AMP AP and a non-AP AMP STA is achieved by mutual authentication and authenticated or encrypted data exchanges. Mutual authentication is based on the principle of 4-way handshake using a PMK known to the AMP AP and the non-AP AMP STA. The keys used for authenticated or encrypted data exchanges are derived from a PTK generated from the PMK, ANonce, SNonce, the AMP AP’s address, and the non-AP AMP STA’s address during mutual authentication.

Since a non-AP AMP STA may have extremely limited energy supply, it may not be able to maintain security association data (such as PTK, KCK, TK, and nonces for encryption algorithm) generated during mutual authentication in volatile memory after it exhausts the energy, or it may lack the energy to write such data in non-volatile memory, or it may exhaust the energy prematurely in the middle of secure communications. Therefore, a non-AP AMP STA is not required to maintain security association with an AMP AP. Instead, a non-AP AMP STA shall go through mutual authentication and key derivation every time after it is powered on for secure communication with an AMP AP.

The PMK between an AMP AP and a non-AP AMP STA can be generated and updated using a secure method.

**Text to be adopted ends here.**

**References:**

1. <https://mentor.ieee.org/802.11/dcn/24/11-24-1613-13-00bp-specification-framework-for-tgbp.docx>, Yinan Qi (OPPO)