IEEE P802.11
Wireless LANs

|  |
| --- |
| Response to comments on IEEE 802.11ax-2021 in *60-day ballot* using the ISO/IEEE PSDO agreement |
| Date: 2021-10-29 |
| Author(s): |
| Name | Affiliation | email |
| Andrew Myles | Cisco | amyles@cisco.com |
| Dan Harkins | HPE |  |

Abstract

Five NBs provided comments during the *60-day ballot* on IEEE 802.11ax-2021 under the PSDO agreement between IEEE and ISO. This document proposes responses to those comments.

R2: updates after IEEE 802 JTC1 SC meeting on 14 Sep 2021, with suggested refinements to the text from multiple contributors, and particularly from IEEE SA staff.

R3: added reference to 802.11md liaison to SC6. This version was recommended to IEEE 802.11 WG for approval by the IEEE 802 EC. The IEEE 802 deferred a decision until 5 Nov 2021.

R4: Includes edits reflecting discussion in 802 EC on 5 Oct 2021, and subsequent edits to simplify the language and clarify the logic. IEEE SA staff have reviewed this revision. IEEE 802 EC members are asked to comment on this revision before it is considered by the IEEE 802 EC on 5 Nov 2021.

R5: proposed changes respond to comments made by various IEEE 802 EC members. It has been reviewed by IEEE SA staff (including Legal)

R6: All changes were accepted and comments removed. The response to the IPR related comments were removed, as directed by IEEE SA. This material will be liaised separately under the signature of the IEEE SA President

## This Liaison Statement responds to comments during *60-day ballot* on IEEE 802.11ax-2021

ISO/IEC JTC1/SC6 held a *60-day ballot*, closing on 10 August 2021, on IEEE 802.11ax-2021 as the first part of an approval process defined by the Partner Standards Development Organization (PSDO) Cooperation Agreement between IEEE and ISO. The results of the *60-day ballot* are documented in 6N17559.

The two questions asked both received majority support from those *National Bodies* (NBs) voting *yes* or *no*, and therefore the *60-day ballot* passed:

* *Do you support the need for an ISO International Standard on the subject?*
	+ Approved 10/0/9
* *Do you support the submission of this proposal for FDIS ballot?*
	+ Approved 6/4/9

Comments were received from the following five NBs:

* China NB
* Sweden NB
* Finland NB
* Germany NB
* Japan NB (associated with a *yes* vote on both questions)

This liaison statement from IEEE 802 LAN/MAN Standards Committee[[1]](#footnote-1) (IEEE 802) to ISO/IEC JTC1/SC6 provides responses to all the comments received during the *60-day ballot* on IEEE 802.11ax-2021.

## Response to comment CN1-003

### CN1-003 comment

*IEEE 802.11ax-2021 is an amendment to IEEE 802.11-2020. China voted against IEEE 802.11- 2020 with technical comments (see SC6N17516). At present, China's comments on IEEE 802.11-2020 have not been properly handled. For many of these comments also apply to IEEE 802.11ax, China disapprove IEEE 802.11ax submitting to the next stage*

### CN1-003 proposed change

*It is recommended to postpone the subsequent ballot on IEEE 802.11 and IEEE 802.11ax in ISO/IEC until the discovered design flaws are sufficiently resolved.*

### IEEE 802 response to CN1-003

*Reject*

As noted by the China NB, comment CN1 is essentially a reiteration of various comments submitted by the China NB during the *60-day ballot* on IEEE 802.11-2020, and documented in SC6N17516. IEEE 802 notes that responses to all these comments were provided in a previous *Liaison Statement* to ISO/IEC JTC1/SC6 (See N17600).

## Response to comment CN2-006

### CN2-006 comment

*In 2019, Mathy Vanhoef published a paper “Dragonblood: Analyzing the Dragonfly Handshake of WPA3 and EAP-pwd” in IEEE Symposium on Security and Privacy on 18-20 May 2020 in Oakland (San Francisco). (It’s free for downloading from the Internet.) This paper presents design flaws in the 802.11 standard. The design flaws can be divided in two categories. The first category consists of downgrade attacks against SAE-capable devices, and the second category consists of weaknesses in the Dragonfly handshake of recover the password of the WLAN network, launch resource consumption attacks, and force devices into using weaker security groups.*

### CN2-006 proposed change

*It is recommended to postpone the subsequent ballot on IEEE 802.11 and IEEE 802.11ax in ISO/IEC until the discovered design flaws are sufficiently resolved.*

### IEEE 802 response to CN2-006

*Reject*

Changes to the IEEE 802.11 standard were proposed in 2019 (see [11-19/1173r15](https://mentor.ieee.org/802.11/dcn/19/11-19-1173-15-000m-pwe-in-constant-time.docx) for more details) to produce a constant-time generation of the *secret* used in SAE as well as to prevent downgrade attacks. The changes resulting from that modification make SAE resistant to the *Dragonblood* attacks described in the referenced 2020 paper. These changes are already part of the IEEE 802.11-2020 standard and are therefore included the IEEE 802.11ax-2021 amendment considered in the *60-day ballot*. This comment is not a reason to delay balloting because the so called "design flaws" have already been addressed.

##  Response to comments SE-001/FI-002/JP1-004/DE-005

### Comments

Please refer to SE-001, FI-002, JP1-004 and DE-005 in SC6N17559 for the text of the comments from the Sweden, Finland, Japan and Germany NBs.

### Proposed changes

Please refer to SE-001, FI-002, JP1-004 and DE-005 in SC6N17559 for the text specifying the proposed changes from the Sweden, Finland, Japan and Germany NBs.

### IEEE 802 response

*Defer*

A response to the comments above will be provided to ISO/IEC JTC1/SC6 directly by the IEEE Standards Association.

1. This Liaison Statement solely represents the views of the IEEE 802 LAN/MAN Standards Committee, and does not necessarily represent a position of IEEE or IEEE Standards Association [↑](#footnote-ref-1)