IEEE P802.11
Wireless LANs

|  |
| --- |
| CSD Draft for the IEEE 802.11bi Privacy Amendment |
|  Date: 2020-11-04 |
| Author(s): |
| Name | Affiliation | Address | Phone | email |
| Carol Ansley | self |  |  | carol@ansley.com |
| Stephen McCann | Huawei | Southampton, UK |  | stephen.mccann@ieee.org |

1. IEEE 802 criteria for standards development (CSD)

The CSD documents an agreement between the WG and the Sponsor that provides a description of the project and the Sponsor's requirements more detailed than required in the PAR. The CSD consists of the project process requirements, [1.1](#bookmark), and the 5C requirements, [1.2](#bookmark1).

## 1.1 Project process requirements

### 1.1.1 Managed objects

Describe the plan for developing a definition of managed objects. The plan shall specify one of the following:

1. The definitions will be part of this project.

**Yes**

1. The definitions will be part of a different project and provide the plan for that project or anticipated future project.
2. The definitions will not be developed and explain why such definitions are not needed.

### 1.1.2 Coexistence

A WG proposing a wireless project shall prepare a Coexistence Assessment (CA) document unless it is not applicable.

1. Will the WG create a CA document as part of the WG balloting process as described in Clause 13?

**Yes**

1. If not, explain why the CA document is not applicable.

## 1.2 5C requirements

### 1.2.1 Broad Market Potential

Each proposed IEEE 802 LMSC standard shall have broad market potential. At a minimum, address the following areas:

f) Broad sets of applicability.

* User privacy is concerned with control of data that is or can be used to construct personally identifiable information (PII) and/or personally correlated information (PCI). A user of IEEE Std 802.11 compliant devices may generate PII and PCI. Retaining user control of the PII and PCI generated as a result of using such devices is a goal of this amendment.
* User privacy has also been an increasing area of focus in the wireless marketplace. Most smartphones, for example, have implemented at least randomly changing MAC addresses before associating with an access point. This trend is not confined to smartphones, other client devices such as laptops have also implemented this feature.
* The set of interested parties is not confined to client device manufacturers and users. At the same time, access points and the infrastructure that uses them have been increasing their capabilities to provide personalized services, as well as other tracking services, that are not necessarily compatible with privacy goals.

g) Multiple vendors and numerous users.

A wide variety of vendors currently build systems and products that impact privacy concerns for both the clients and access points. Based upon the variety of companies that participated in the RCM TIG and the RCM SG, it is anticipated that a substantial proportion of those vendors, and others, will participate in subsequent activities for improving privacy-related behaviors.

### 1.2.2 Compatibility

Each proposed IEEE 802 LMSC standard should be in conformance with IEEE Std 802, IEEE 802.1AC, and IEEE 802.1Q. If any variances in conformance emerge, they shall be thoroughly disclosed and reviewed with IEEE 802.1 WG prior to submitting a PAR to the Sponsor.

1. Will the proposed standard comply with IEEE Std 802, IEEE Std 802.1AC and IEEE Std 802.1Q?

Yes

1. If the answer to a) is no, supply the response from the IEEE 802.1 WG.

The review and response is not required if the proposed standard is an amendment or revision to an existing standard for which it has been previously determined that compliance with the above IEEE 802 standards is not possible. In this case, the CSD statement shall state that this is the case.

### 1.2.3 Distinct Identity

Each proposed IEEE 802 LMSC standard shall provide evidence of a distinct identity. Identify standards and standards projects with similar scopes and for each one, describe why the proposed project is substantially different.

This amendment defines modifications, additions and/or recommendations to the medium access control layer (MAC) to improve the privacy experienced by users in environments using IEEE Std 802.11 technology. These developments include a review of the recommendations of IEEE P802E.

There is no other WLAN standard focusing on enhancing the performance of IEEE Std 802.11 networks in regards to user privacy other than this amendment.

### 1.2.4 Technical Feasibility

Each proposed IEEE 802 LMSC standard shall provide evidence that the project is technically feasible within the time frame of the project. At a minimum, address the following items to demonstrate technical feasibility:

j) Demonstrated system feasibility.

There are already proprietary solutions available in the market to improve user privacy. However, there are a number of areas where standards support can enhance the overall performance of user privacy efforts.

The IEEE 802.11 Wireless Next Generation (WNG) Standing Committee (SC) and RCM Topic Interest Group (TIG)/Study Group (SG) have reviewed many presentations indicating that enhancements are technically feasible. These contributions outlined techniques related to privacy to enhance current use cases and enable new ones.

k) Proven similar technology via testing, modeling, simulation, etc.

IEEE Std. 802.11 technology is very mature and has a wide variety of legacy devices and a proven track record, with several billions of devices shipping each year. The principle of extending the IEEE 802.11 PHYs and MAC with new capabilities is also well established by previous amendments within IEEE 802.11.

The increased capabilities envisioned for the MAC necessary to implement the proposed amendment are in line with the current progress in technology and not expected to impinge testability.

### 1.2.5 Economic Feasibility

Each proposed IEEE 802 LMSC standard shall provide evidence of economic feasibility. Demonstrate, as far as can reasonably be estimated, the economic feasibility of the proposed project for its intended applications. Among the areas that may be addressed in the cost for performance analysis are the following:

l) Known cost factors.

Support of the proposed standard will likely require a manufacturer to develop modified firmware on AP STAs and non-AP STAs. The cost factors for these transitions are well known.

m) Balanced costs.

WLAN equipment is accepted as having balanced costs. The development of features to support RCM features in WLAN network deployments will not disrupt the established balance.

n) Consideration of installation costs.

The proposed amendment has no known impact on installation costs.

o) Consideration of operational costs (e.g., energy consumption).

This amendment is not expected to change today’s operation costs.

**References:**

[1] [11-19-0588-02-0rcm-summary-of-discussions-on-randomized-and-changing-mac-addresses-2014-2019.odt](https://mentor.ieee.org/802.11/dcn/19/11-19-0851-00-0rcm-p802-1cq-mac-address-assignment-requirements.pptx)

[2] [11-19-0851-00-0rcm-p802-1cq-mac-address-assignment-requirements.pptx](https://mentor.ieee.org/802.11/dcn/19/11-19-0851-00-0rcm-p802-1cq-mac-address-assignment-requirements.pptx)

[3] [11-19-0884-00-0rcm-temporary-addresses.pptx](https://mentor.ieee.org/802.11/dcn/19/11-19-0884-00-0rcm-temporary-addresses.pptx)

[4] [11-19-1027-01-0rcm-do-not-fear-random-macs.pptx](https://mentor.ieee.org/802.11/dcn/19/11-19-1027-01-0rcm-do-not-fear-random-macs.pptx)

[5] [11-19-1313-02-0rcm-pitfalls-with-address-randomization.pptx](https://mentor.ieee.org/802.11/dcn/19/11-19-1313-02-0rcm-pitfalls-with-address-randomization.pptx)

[6] [11-19-1314-02-0rcm-privacy-protection-in-wi-fi-analytics-systems.pptx](https://mentor.ieee.org/802.11/dcn/19/11-19-1314-02-0rcm-privacy-protection-in-wi-fi-analytics-systems.pptx)

[7] [11-19-1320-00-0rcm-assignment-of-temporary-addresses.pptx](https://mentor.ieee.org/802.11/dcn/19/11-19-1320-00-0rcm-assignment-of-temporary-addresses.pptx)

[8] 802.11-2016 - IEEE Standard for Information technology--Telecommunications and information exchange between systems Local and metropolitan area networks--Specific requirements - Part 11: Wireless LAN Medium Access Control (MAC) and Physical Layer (PHY) Specifications.

[9] 802.11aq-2018 - IEEE Standard for Information technology--Telecommunications and information exchange between systems Local and metropolitan area networks--Specific requirements Part 11: Wireless LAN Medium Access Control (MAC) and Physical Layer (PHY) Specifications Amendment 5: Preassociation Discovery.

[10] IEEE P802E: Recommended Practice for Privacy Considerations for IEEE 802 Technologies highlights techniques and concerns to improve privacy.