

A (very) quick update on RCM work at 802.11

Mark Hamilton, Carol Ansley
(Personal opinions, per IEEE SASB Op Manual)
July 2023

v01

IEEE 802.11 has 2 projects related to “RCM”

- TGBh: Randomized and Changing MAC addresses
 - Formed in response to “changing MAC addresses can have a wide range of repercussions impacting not only 802.11 networks, but also many related services.”
 - Developed scope and list of issues, based on use cases that have been identified as impacted by use of RCM, and then considering which were within IEEE 802.11 scope [1].
 - Draft 1.0 passed Initial WG Letter Ballot (92% approval) – more details on following slides
- TGbi: Enhanced Data Privacy
 - Much broader scope: “Protecting personal information such as location, movements, contacts and activities.” [2] Again, within 802.11 scope...
 - Longer schedule – 2026?
 - Also more details on later slide

IEEE 802.11 TGbh Draft 1.0 rough content

- “Device ID”
 - Infrastructure (network) allocates an identifier, and provides it to the client device, within secured communications (part of the security negotiation exchange)
 - Optional mechanism is provided to make the identifier “opaque” (self-encrypted), for cases where the identifier will/may be transmitted in unsecured frames.
 - Note: Device ID might also be “garbage” to a third-party (a local identifier only useful to the network), and could be transmitted visibly *_once_* without creating loss of privacy or tracking opportunities. So, for pre-association use (for example), which exposes the ID, it is rotated on every use.
- “IRM” (identifiable MAC address)
 - Allocated by client device (“randomized”), and used as source (TA) of transmissions.
 - Also communicated in security negotiation exchange, to allow the network to associate the MAC address with the client’s known/true identity.
 - Rotated frequently, at client’s discretion.
- Both schemes can be used to identify the client for the duration of an association, or can be used for pre-association interactions using the 802.11az “PASN” authentication

IEEE 802.11 TGbh Draft 1.0 status/schedule

- Draft 1.0 was completed at the May 802.11 F2F session. [3]
- 802.11 Working Group Letter Ballot, ran between May and July sessions. Passed with 92% approval.
- The draft is considered stable enough for public sharing. This sharing is typically only for IEEE members, but could also include liaison organizations.
 - Sharing with IETF is TBD, but should be considered (in my opinion).
 - Suggest we formalize/confirm a liaison between Madinas and 802.11, specifically on this topic.
- “SA Balloting” process targeted to start March 2024. Often, implementers find this point stable enough to get started.
- Final publication expected in Q3’24.

IEEE 802.11 TGbi scope/content

- TGbi is working to improve 802.11 user privacy by redesigning parts of the protocol to reduce the amount of information available to third party observers
- Recent topics of discussion include:
 - MAC address change while associated for Multi-Link Devices (MLD) and non-MLD STAs
 - Particularly how to address behavior in the transition between a first MAC address and a second MAC address
 - Associated parameters affected by MAC address change
 - Particularly parameters with limited number spaces, such as the Association ID
 - (re)Association message protection
 - Probe Request/Response message exchange with reduced parameters

IEEE 802.11 TGbi status/schedule

- TGbi's currently working to produce text for an early version that can be sent around within 802.11 in a comment collection similar to what TGbh did earlier this year.
- The goal for TGbi is a comment collection starting after the September Interim meeting of 802.11, but the exact date will be driven by the level of completion of the work topics.
- Final publication of TGbi's amendment is expected in 2026.

References

- [1] <https://mentor.ieee.org/802.11/dcn/21/11-21-0332-37-00bh-issues-tracking.docx>
- [2] <https://mentor.ieee.org/802.11/dcn/23/11-23-0892-02-00bi-requirements-and-issues-tracking.docx>
- [3] https://grouper.ieee.org/groups/802/11/Reports/802.11_Timelines.htm