IEEE P802.11
Wireless LANs

|  |
| --- |
| What are the requirements for a TGbh “private identifier”? |
| Date: 2021-09-15 |
| Author(s): |
| Name | Affiliation | Address | Phone | email |
| Dan Harkins | HPE |  |  |  |
|  |  |  |  |  |

Abstract

This submission elaborates on a post made to the 802.11bh mailing list asking what the requirements are for a “private identifier” that could be used in lieu of a MAC address.

Meta question: is this identifier used as an address in 802.11 frames or is it a blob that is put into a frame? What are we expecting?

A:

Further questions to solicit requirements on the identifier (whatever it is, address or blob):

1. Is a private address/identifier dynamic or is it just a different static address/identifier? How often does/should it change?

A: depends on the use case, for home it might be static or rarely changing, or a hotspot case might provide a semi-persistant identifier. Depends on trust/use case.

A: could be static per ESS, different for different ESS. STA provides info per ESS.

A: user decides whether static or dynamic, time frame for changing. For some networks it could be static or rarely changing. Identifier should be assigned by user.

A: user should be in control, decide whether device’s identifier will be static or not. Differs from a random MAC address because binding is only between STA and AP/network/ESS, 3rd party won’t be able to track.

A: different tracking tools can be used (e.g. location) and it’s important for user to be in control to decide when to change identifier.

A: this should not be a “session identifier” it could span multiple sessions.

1. Is it invertible such that the "real" address/identifier can be determined from a private address/identifier? Or is it pseudononymous and any binding between it and the “real” address/identifier is through some other means?

A: again, depends on use case. TGbh doesn’t really have a requirement for a mapping but TGbi may require it.

A: there are 2 types of problems to solve: 1) need to maintain some identity for some period which may not map back to a “real” identity (hotel); 2) you may want to randomize MAC address for <reasons> and still need a mappable identity back to a “real” identity that helps scale to enterprise networks.

A: needs to be bound to some “real” identity (address or whatever) for the connection.

A: there should not be any way to resolve a “real” identity from this private thing. Not invertible.

A: again, depends on what the user wants.

1. Do we need to prevent a 3rd party from knowing whether private identifiers are used? 3rd parties can already know whether a STA is using a random MAC address, would knowledge that a STA is (also) using a private address/identifier expose PII/PCI?

A: Yes, it does. Behavioral aspects of a user are exposed.

A: Not a significant exposure.

A: Yes, it does. No one should know whether private identifiers are used except the two parties using them.

A: It could expose PCI depending on how many private identifiers are in use at a particular time.

A: It *might* expose PCI but not to a major extent and we have other things to worry about.

1. Is it assumed that only certain entities can make a binding/track someone? If so, who is in the "in crowd" and how is that enforced? What is the work factor for someone not in the “in crowd” to make a binding/track someone? By “track” it is assumed that PII is built/gathered.

A: the non-AP STA and the AP is the full list, through a robust cryptographic protocol. Work factor should be roughly equivalent to the security protecting the data exchange.

A: it’s between the ESS (multiple APs) and “the guy you’re talking with”

1. Is the private address/identifier bound to a secure connection or is unencrypted (poss. unassociated) use of this functionality required? Would non-private 1st use and private after that be acceptable?

A: Need to avoid exposing PII on 1st use. Don’t want perfect to be enemy of the good™.

A: Should be protected at 1st use.

A: assume RSN; secure only. Non-private 1st use is not acceptable.

A: assume mutual authentication in network—i.e. RSN.

1. What are the assumptions on forgery of such an address/identifier? How hard does it need to be for someone to fake one? Do we even care about forgery?

A: It should be hard to forge.

A: Depends on what the identifier is used for, use case dependent.

A: if this is in an RSN then it forgery should not be an issue.

A: might depend on how the identifier is constructed, might be different rules for different use cases.

1. Are there any requirements to force STAs to do a scheme like this? Is co-existence (with other schemes, or no scheme) necessary?

A: depends, should be opt-in. As long as the STA consents.

A: certain network requirements may force STAs to consent in order to obtain service, should be part of the exchange so STA has informed consent.

A: opt-in on both sides.

A: co-existence is valuable where you might get some good info from, say, EAP, but need another mechanism for other non-EAP users.

1. Are there any collision resistance requirements? What's the probability of collision of private addresses/identifiers with 10,000 associated STAs? 20,000 STAs? What is acceptable?

A:

In addition:

1. What about protecting client identities from the network?

A: If the STA is providing the private address/identifier in its messages then isn’t control in the hands of the STA? If it doesn’t want the network to know its “real” identity then it won’t use one that is resolvable. Of course, the network may refuse a connection but that’s fine. The decision is still in the hands of the STA.

A: network needs to say what it wants for client to make an informed consent decision.

A: the advertisement of what you might need to be protected to.

A: similar to MAC randomization.

1. What other requirements do we have on usage of this address/identifier (aside from “private”)?

A: A cut-and-paste attack, substituting one address/identifier for another, must be prevented. Impersonation, attacker using someone elses address/identifier, must be prevented. Traffic analysis must not be enabled, the the greatest extent possible. Solution must not enable DOS or CPU exhaustion attacks on either AP or STA.

Another question: need informed consent.

**References:**