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:

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:

1. Can a 3rd party determine whether an address/identifer is private or not? 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:

1. Is it assumed that only certain entities can figure out the "real" address/identifier? If so, who is in the "in crowd" and how is that enforced? What is the work factor to break it and find the “real” identifier?

A:

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:

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:

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:

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 identies 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.

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.

**References:**