Draft MADINAS Use Cases document

Jerome Henry

Mar 2024

v 01

Draft Update

Since draft madinas use cases 01:

- Draft 01 addressed all comments received since previous F2F
- Draft 02 starts examining possible existing solutions to the requirements
- Draft 03 adds more solutions, and fixes typos – procedural mishap that needs addressing
- Draft 04 implements more comments from previous F2F
- Draft 05 reduces the requirements section
- Draft 06 mitigates the IPv6 gap (and still finds typos!)
- Draft 07 implements the comments made in Nov F2F
- Draft 08 implements comments received in list (remove requirements)
- Draft 09 implements further comments (add annex, + next slides)

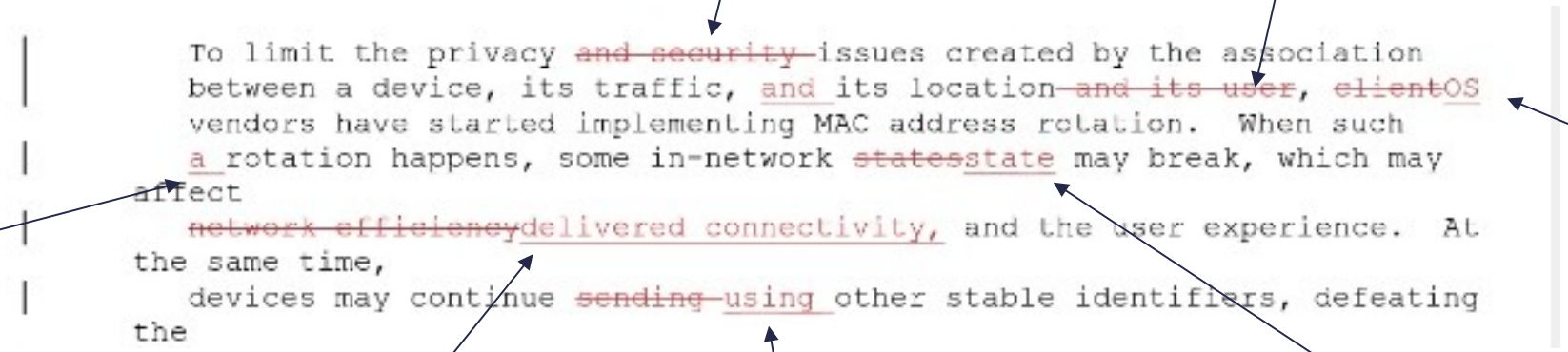
Document seems to be stable now and seems ready for adoption. Continued input and feedback are welcome

https://datatracker.ietf.org/doc/draft-ietf-madinas-use-cases/.

Draft Update

This was discussed in earlier versions, PII exposure might make some devices attack targets, thus ‘security’ was added

User is the key target of PII exposure, needed



To limit the privacy ~~and security~~ issues created by the association between a device, its traffic, and its location ~~and its user~~, ~~client~~OS vendors have started implementing MAC address rotation. When such a rotation happens, some in-network ~~states~~state may break, which may affect ~~network efficiency~~delivered connectivity, and the user experience. At the same time, devices may continue ~~sending~~ using other stable identifiers, defeating the

Changed to client and OS

changed

It is more than connectivity, and the overhead due to renewing elements like IP/802.1X etc.

changed

It is a countable noun, and there are more than one possible state -> plural is required

Draft Update

See later slide (functional is needed)

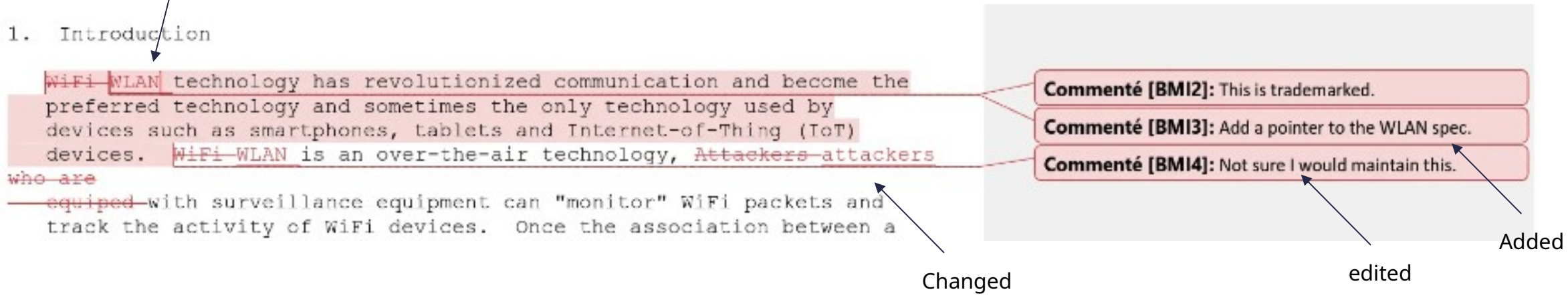
This document lists various network environments and a set of ~~functional~~ network services that may be affected by such rotation. This document then examines settings where the user experience may be affected by in-network state disruption, and settings where other machine identifiers may help re-identify the user or recover the identity of the user, and locate the device and its associated user. Last, this document examines solutions to maintain user privacy while preserving user quality of experience and network operation efficiency.

Commenté [BMI1]: Double check if user is meant here ore device

User indeed (target of PII exposure)

Draft Update

Changed to 802.11 (Wi-Fi), following the model of RFC 9119, to avoid the confusion that WLAN may cause with HiperLAN, HomeRF and others. We note that many RFCs just use Wi-Fi (RFC 7458, 9450, 8110, 9330…)



Draft Update

Needed, otherwise the distinction between personal device and shared service device is lost, but clarified

Added clarification text

To reduce the risks of correlation between a device activity and its owner, multiple vendors have started to implement Randomized and Changing MAC addresses (RCM). With this scheme, ~~an end-~~a device implements a different RCM over time when exchanging traffic over a wireless network. By randomizing the MAC address, the persistent association between a given traffic flow and a single device is made more difficult, assuming no other visible unique identifiers or stable patterns are in use.

However, such address change may affect the user experience and the efficiency of legitimate network operations. For a long time, network designers and implementers relied upon the assumption that a given machine, in a network implementing IEEE 802 technologies, would be represented by a unique network MAC address that would not change

Commenté [BMI5]: How the mac address is used for that?

Commenté [BMI6]: Not sure the causality effect is true here.

I would simply reword this to focus on "tracking device activity"

Commenté [BMI7]: I suggest to add a sentence that says that "device" is a device used by an end user to connect to a network.

Commenté [BMI8]: Not all wireless network uses MAC addresses

Changed

edited

Draft Update

The end device may be initiating, but it is not always the one establishing the session

Edited (in transit)

Services may be beyond the access

No, this may be an 802.11 stack function, not necessarily an OS function

example, sessions established ~~between the~~by the ~~-~~ ~~end~~-device ~~and~~ to access network
services may be ~~lost~~ disrupted and packets in translation may suddenly be
without clear source or destination. If multiple clients implement fast-paced RCM rotations with or without any coordination to prepare the migration, network services may be over-solicited by a small number of stations that appear as many clients.

At the same time, some network services rely upon the client station providing an identifier, which can be ~~the~~ a MAC address or another value. If the client implements MAC rotation but continues sending the same static identifier, then the association between a stable identifier and the station continues despite the RCM scheme. There may be environments where such continued association is desirable, but others where the user privacy has more value than any continuity

Commenté [BMI10]: ??

Commenté [BMI11]: Oses?

Commenté [BMI12]: I would delete this part as the main argument here is overload.

Why "small number"? This depends on how many endpoints have that behavior.

Commenté [BMI13]: To be defined.

deleted

Edited

Edited further

Draft Update

Needed, a network functional entity provides resources or services to the network, without necessarily being a network device (e.g. DHCP server)

3.1. Network ~~Functional~~ Entities

Network communications based on IEEE 802 technologies commonly rely on station identifiers based on a MAC address. This MAC address is utilized by several types of network ~~functional entitities~~entities.

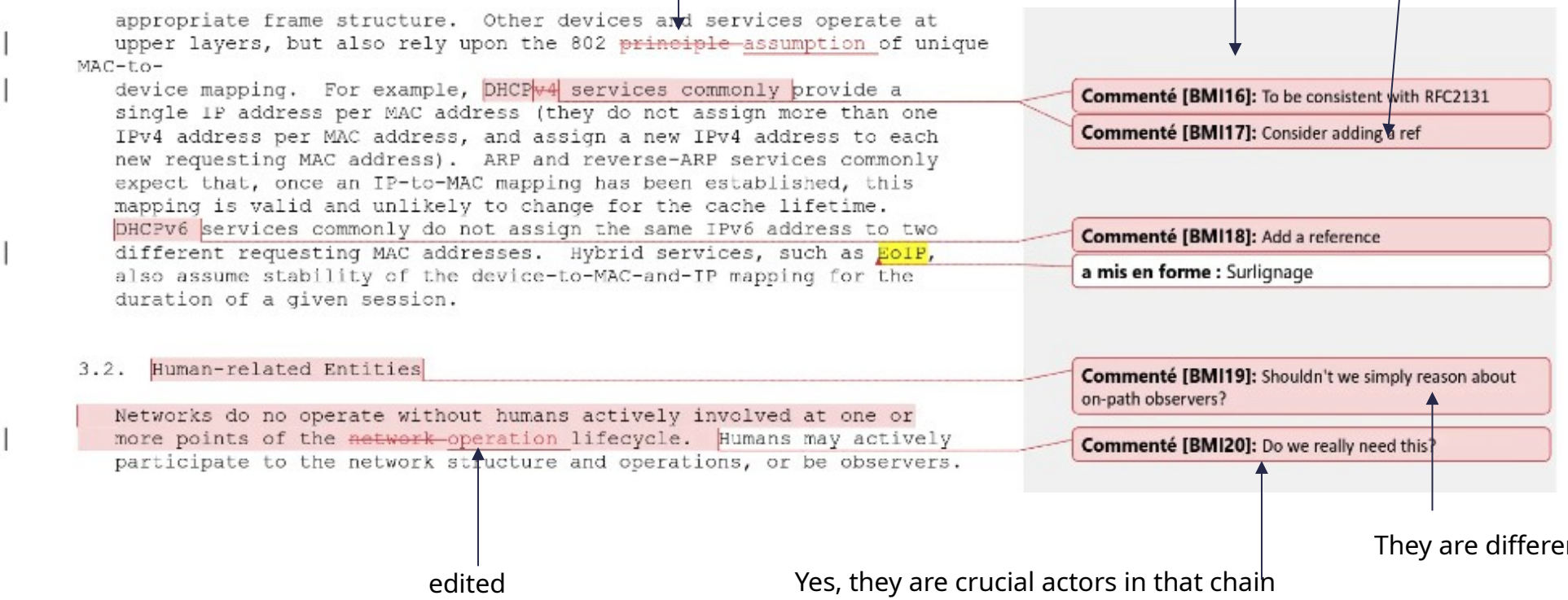
Wireless access network infrastructure devices (e.g., WLAN access points or controllers): these devices participate in IEEE 802 LAN operations. As such, they need to identify each machine as a source or destination so as to successfully continue exchanging frames. Part of the identification includes recording, and adapting to, devices communication capabilities (e.g., support for specific protocols). As a device changes its network attachment (roams) from one access point to another, the access points can exchange contextual information (e.g., device MAC, keying material) allowing the device session to continue seamlessly. These access points can

Draft Update

This would be in the BCP, if we add a reference here, we need a reference for any technical service mentioned in the doc, and it becomes heavy

Edited

It is not an assumption, it is an explicit principle



They are different entities

edited

Yes, they are crucial actors in that chain

Draft Update

for example, for IT support operations. However, it is difficult to control if another actor also monitors the same station with the goal of obtaining PII or PCI.

Wireless access network operators: some wireless access networks are only ~~offered to users or~~provided to devices matching specific requirements, such as device type (e.g., IoT-only networks, factory operational

edited

Draft Update

The surface of PII exposures that can drive MAC address randomization depends on (1) the environment where the device operates, ~~on~~ (2) the presence and nature of other devices in the environment, and ~~on~~ (3) the type of network the device is communicating through. Therefore, a device can ~~express an~~reveal an ~~identity~~identifier (such as a MAC address) that can persist over time if trust with the environment is established, or that can be temporal if an identity is required for a service in an environment where trust has not been established. ~~Trust is not a binary currency. Thus i~~It is useful to distinguish what trust a ~~personal~~ device may establish with the different entities at play in a ~~L2~~Layer 2 domain:

1. Full trust: there are environments where a personal device establishes a trust relationship and can share a persistent device identity with the access network devices (e.g., access point and WLC), the services beyond the access point in the L2 broadcast domain (e.g., DHCP, AAA), without fear that observers or network actors may access PII that would not be shared

Commenté [BMI21]: I'm afraid this is not specific to L2.

a mis en forme : Surlignage

edited

Draft Update

3. Zero trust: In other environments, ~~the~~ a device may not be willing to share any persistent identity with any local entity reachable through the AP, and may express a temporal identity to each of them. That temporal identity may or not be the same for different services.

5. Environments

~~This~~ The trust relationship ~~naturally~~ depends on the relationship between the user of ~~the~~ a ~~personal~~ device and the operator of the service. ~~Thus, it is useful to observe the~~The following lists ~~-~~typical trust structure of common environments:

A. Residential settings under the control of the user: this is typical of a home network with Wi-Fi in the LAN and Internet ~~connection~~connectivity. In this environment, traffic over the Internet does not expose the MAC ~~address~~addresses of internal devices if it is not copied to another field

Commenté [BMI22]: Why naturally?

This may be beyond the control of the user. It does not event know/control what is leaked/revealed when a device attaches to a network.

Commenté [BMI23]: Which service? Does this include the infrastructure?

Commenté [BMI24]: Still, even in this case, some devices may not be trusted. Think about guest SSIDs out there to isolate them.

edited

Draft Update

6. Network Services

Different network environments provide different levels of network services, from simple to complex. At its simplest level, a network can provide to a wireless connecting device basic address allocation service (DHCP) and an ability to connect to the Internet (~~i.e.~~e.g., ~~-~~ DNS service or relay, and ~~routing~~ forwarding in and out through a local gateway). The network can also offer more advanced services, such as file storage, printing or local web service. Larger and more complex networks can also incorporate a multiplicity of more advanced services, from authentication (AAA), to quality of experience (QoE) monitoring and management. These services are ~~often~~ accompanied with network performance management services. Different levels of services may call for different relationships with the device, or its user, identity. For example, there is usually no need to identify the device or its user for a public network to provide a DHCP-sourced IP address to a connecting station, or accept a station using its self-generated IP address (e.g., using SLAAC [RFC4862]). However, there

edited

Draft Update

generated IP address (e.g., using SLAAC [RFC4862]). However, there may be a need, in an enterprise private network, to identify devices in order to provide adapted quality of services (e.g., to prioritize identified voice traffic coming from a smartphone over keepalive data coming from an IoT endpoint). The same type of network may have a need to limit the effect of IP address spoofing and invalid reuse through mechanisms like SAVI [RFC6620].

6.1. ~~The Purpose of~~ Device Identification and Associated Problems

Many network functional devices offering a service to a ~~personal~~ device use the device's MAC address to maintain service continuity.

Commenté [BMI25]: What is a functional device?

Wireless access points and controllers use the MAC address to validate the device connection context, including protocol capabilities, confirmation that authentication was completed, QoS or security profiles, encryption key material. Some advanced access points and controllers also include upper layer functions which purpose is covered below. A device changing its MAC address, without another recorded device identity, would cause the access point and the controller to lose these parameters. As such, the Layer 2

edited

Draft Update

address is released.

Network devices using self-assigned IPv6 addresses (e.g., with SLAAC defined in [RFC6620]) use mechanisms like DAD to and ND to establish the association between a target IP address and a MAC address, and may cache this association in memory. Changing the MAC address, even through a disconnection-reconnection phase, without changing the IP address, may disrupt the stability of these mappings, if the change occurs within the caching period.

Routers keep track of which MAC address is on which interface. MAC rotation can cause MAC address cache exhaustion, but also the need for frequent ARP and inverse ARP exchanges.

In residential settings (environments type A in Section 5), policies can be in
place to control the traffic of some devices (e.g., parental control, or block-list ~~devices~~filters). These policies are often based on the device

edited

Draft Update

This section describes the requirements for Randomized and Changing MAC-addresses:

REQ1 The network must not make any assumption about client MAC address persistence. MAC address change must happen while allowing for service continuity. If a service is interrupted during the RCM process, there must be a formal mechanism for the client and the network to exchange about the interruption.

REQ2 During duration of the services, the device should not change its identity. Any change of identity may result in re-authentication and interruption of the current network services.

REQ3 Different use cases may result in different constraints, and therefore different solutions.

7. Considerations

7.1. IANA Considerations

Commenté [BMI26]: Can be injected into the use case discussion

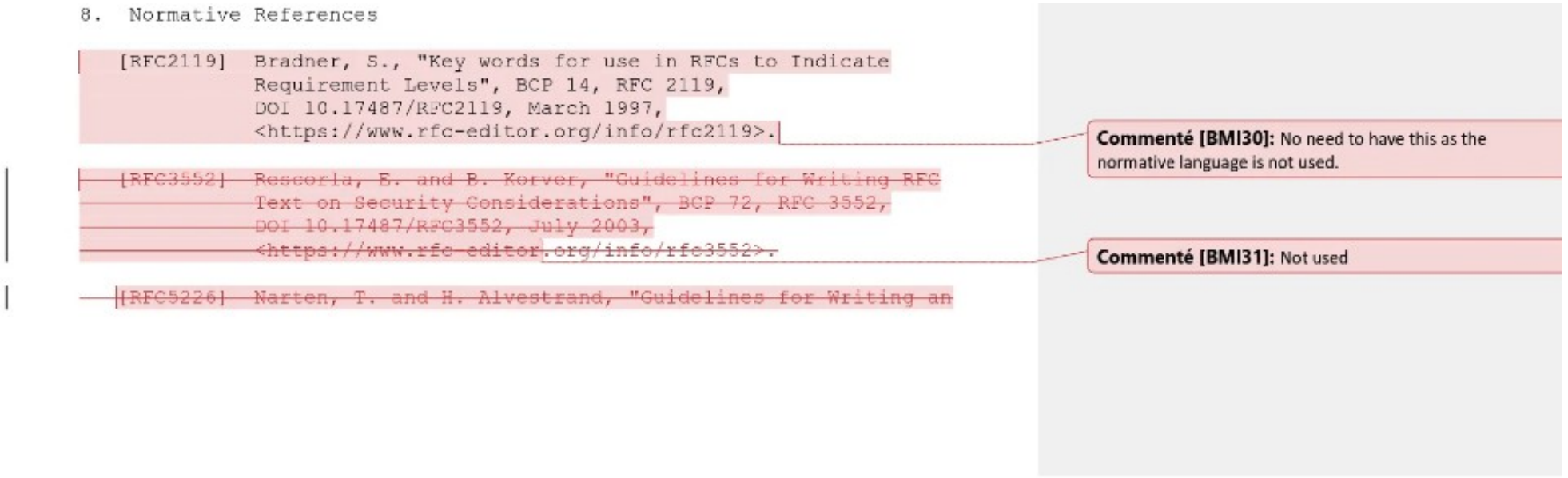
Commenté [BMI27]: ?

Commenté [BMI28]: This depends on the service implem. For example, @ migration can be coordinated with some services/CPEs/Aps/etc.

Commenté [BMI29]: I don' think this is useful as a requirement.

edited

Draft Update



edited

Use Cases

Use cases	Trust Degree	Network Admin	Network Services	Network Support Expectation
Home	Medium	User	Medium	Low
Managed residential	Medium	IT	Medium	Medium
Campus (BYOD)	Medium	IT	Complex	Medium
Enterprise (MDM)	High	IT	Complex	High
Hospitality	Low	IT	Simple	Medium
Public Wi-Fi	Low	ISP	Simple	Low

Draft Update

- 6.3. Use Cases and Requirements
- This section describes the requirements for Randomized and Changing MAC-addresses:
  - REQ1 The network must not make any assumption about client MAC address persistence. MAC address change must happen while allowing for service continuity. If a service is interrupted during the RCM process, there must be a formal mechanism for the client and the network to exchange about the interruption.
  - REQ2 During duration of the services, the device should not change its identity. Any change of identity may result in re-authentication and interruption of the current network services.
  - REQ3 Different use cases may result in different identity requirements.

Section 7, Existing solutions, was removed. Needs to be re-added as annex.

Should we go for WGLC?