Draft MADINAS Use Cases document

Jerome Henry

July 2022

v 01

Draft Update

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

Goal is to:

1. Help define use cases for RCM, by triaging contributing elements:

- User vs. devices, personal vs. shared service devices
- Who is “they”? actors involved in network operations
  - Network functional entities (802.11 entities [APs, WLCs], switches, routers, 802.1X/DHCP services and more)
  - Human-related entities (OTA observers, wireless network operators, network access providers, OTWi/OTWe observers)

Draft Update

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

Goal is to:

1. Help define use cases for RCM, by triaging contributing elements:

- "Trust" variable (full trust, vs. selective trust, vs. zero trust)
- Environments (individual residential settings, managed residential settings, public guest networks, enterprise, with BYOD or MDM)
- Network entities that track the MAC today (L2 infra, 802.1X/DHCP services, routers, policy engines)
- Current assumptions on RCM

2. Examine if existing techniques address the requirements derived from the use cases

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

Continued input and feedback is welcome

Requirements Recap

- REQ 1: 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.
- REQ 2: 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: Survey the current standards that use MAC address as a device identifier in the protocol. Make recommendation to the working groups to remove the dependency.
- REQ4: Work as liaison with external standard bodies such as IEEE, BBF and WBA to align with use cases and requirements.
- REQ5: Identify a secure mechanism to authenticate and exchange network identity to the device.

Requirements Recap

- REQ6 Identify a secure mechanism to inform the device about the type of network the device is connecting to (e.g. public Wi-Fi, enterprise, home), allowing the user to select the device identity (or identities) accordingly.
- REQ7 Identify a secure mechanism for the network to request device identity. Upon successful authentication, the network may provide the device a temporary network-based marker to use the network services.
- REQ8 Identify a secure mechanism for the device to notify the network prior to changing its MAC address.

Possible Existing Solutions

Some requirements cannot be met today (e.g. REQ 1 , no session continuity), but 802.11bi may address this requirement (-> not addressed yet in the draft)

Some requirements can be met:

e.g. REQ 5 and REQ 7, with 802.1X/WPA2/WPA3, however, low adoption outside of enterprise (this is an issue, especially in public Wi-Fi)

WBA OpenRoaming fills the gap (brings 802.1X/WPA2/3 to public Wi-Fi, allows user to stay anonymous to the venue, does not rely on the MAC address [thus it can change, although reauth is still needed])

Draft Update

Proposed steps :

- Continue surveying the current standards that use MAC address as a device identifier in the protocol.
  - What RFCs and protocols should we look into? DHCP, EAP, RADIUS, others?
  - Outside of IETF specifications? IEEE, WBA, WFA, others?
- Continue surveying standards that may enable RCM while enabling network services
- Make recommendation to the working groups to remove the dependency.