Chargeable-User-Identity specification and implementation notes

Karri Huhtanen (Radiator Software Oy)

Chargeable-User-Identity (RFC 4372)

- EAP-PEAP, EAP-TTLS, EAP-SIM, EAP-AKA anonymous outer EAP identities and IMSI Privacy Protection combined with MAC address randomization protect the user privacy, but there are still both business and security reasons to be able to distinguish user sessions from others and for example bind authentication to accounting.
- Chargeable-User-Identity is intended for that, but …

- “Providing a unique identity, Chargeable-User-Identity, is necessary to fulfill certain business needs. This should not undermine the anonymity of the user.”
- “When the home network assigns a value to the CUI, it asserts that this value represents a user in the home network. The assertion should be temporary -- long enough to be useful for the external applications and not too long such that it can be used to identify the user.”

– RFC 4372, Proposed Standard, January 2006

WBA OpenRoaming Wireless Federation draft

- RFC 4372 does not define the the time CUI must or should stay immutable as there are different business cases, roaming agreements etc.
- WBA OpenRoaming Wireless Federation Informational Internet-Draft by WBA members, B. Tomas, M. Grayson, N. Canpolat, B. A. Cockrell, S. Gundavelli (draft-tomas-open-roaming) has additional requirements and clarifications for the use of Chargeable-User-Identity in OpenRoaming, which affect the IdPs, ANPs, RADIUS server vendors and network equipment vendors (NAS devices, Wi-Fi controllers, APs)

7.2.3 Privacy Policies

The baseline privacy policy of OpenRoaming ensures the identities of end-users remain anonymous when using the service. The WBA WRIX specification specifies that **where supplicants use EAP methods that support user-name privacy, i.e., which are compatible with the "@realm" (or "anonymous@realm") (outer) EAP-Identifier, then the supplicant SHOULD use the anonymized outer EAP identifier.** Supplicants supporting other EAP methods SHOULD support EAP method specific techniques for masking the end-user's permanent identifier, for example pseudonym support in EAP-AKA/AKA' [RFC4187] and/or enhanced IMSI privacy protection [WBAEIPP]. **OpenRoaming IDPs SHOULD support and enable the corresponding server-side functionality to ensure end-user privacy is protected.**

7.2.3 Privacy Policies

The WBA WRIX specification also recognizes that the privacy of end-users can be unintentionally weakened by the use of correlation identifiers signalled using the Chargeable-User-Identity attribute (#89) [RFC4372] and/or the Class attribute (#25) [RFC2865] in the RADIUS Access-Accept packet. **The WBA WRIX Specification recommends that the default IDP policy SHOULD ensure that, when used, such correlation identifiers are unique for each combination of end-user/ ANP and that the keys and/or initialization vectors used in creating such correlation identifiers SHOULD be refreshed at least every 48 hours, but not more frequently than every 2 hours.**

7.2.3 Privacy Policies

The OpenRoaming IDP terms ensure **subscribers MUST explicitly give their permission before an immutable end-user identity is shared with a third party ANP**. When such permission has not been granted, an IDP MUST NOT set the PID field to "1" in any of the RCOIs in its end-user Passpoint profiles. When such permission has been granted, an IDP MAY configure multiple RCOIs in their end-users' Passpoint profile, including RCOIs with the PID field set to "0" and RCOIs with the PID field set to "1".

8.2. Chargeable-User-Identity

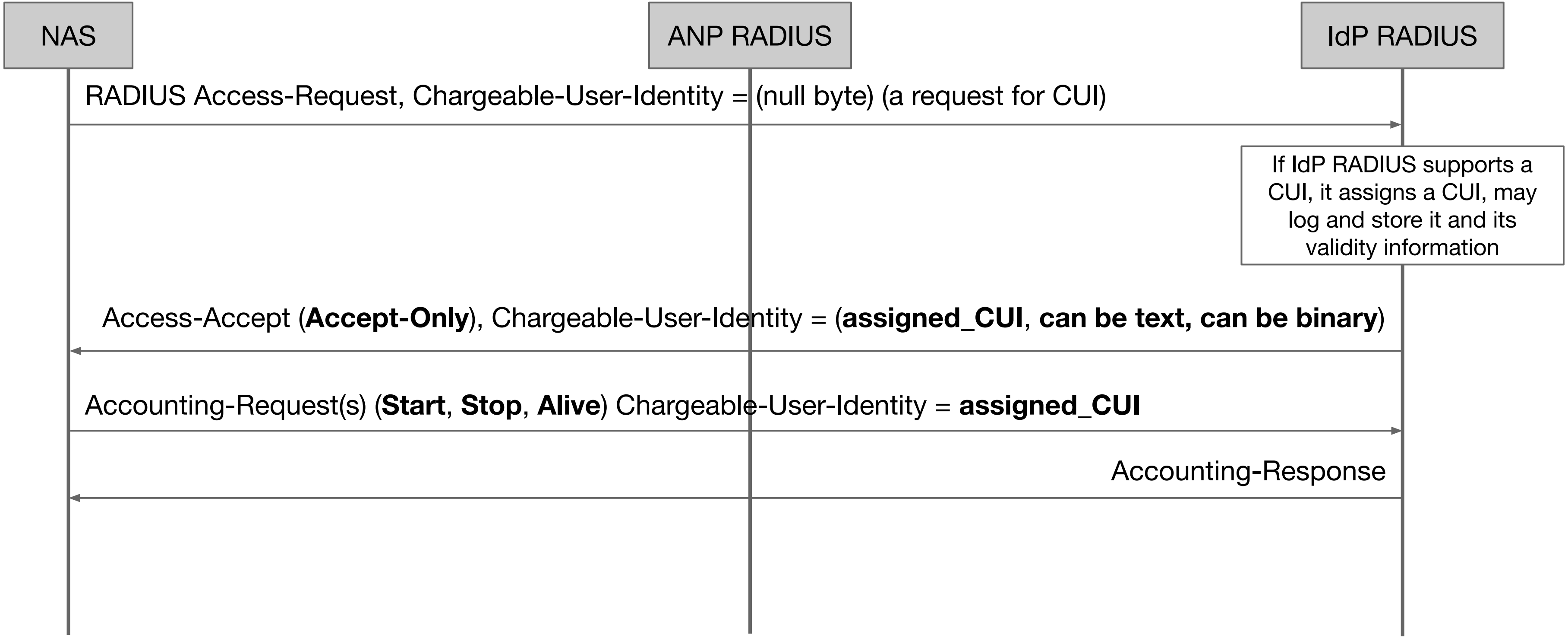
All OpenRoaming ANPs MUST support the Chargeable-User-Identity attribute (#89) [RFC4372] and indicate such by including a CUI attribute in all RADIUS Access-Request packets.

When an end-user has explicitly given their permission to share an immutable end-user identifier with third party ANPs, **the CUI returned by the IDP is invariant over subsequent end-user authentication exchanges between the IDP and the ANP.**

TL;DR

- When implementing and deploying CUI an IdP must either get the subscriber's explicit permission for immutable CUI or implement a time-limited, privacy protected, mutable CUI.
- ANP must have NASes, which implement RFC 4372 or implement the full functionality in ANP RADIUS server/proxy.

Chargeable-User-Identity flow



NAS

ANP RADIUS

IdP RADIUS

RADIUS Access-Request, Chargeable-User-Identity = (null byte) (a request for CUI)

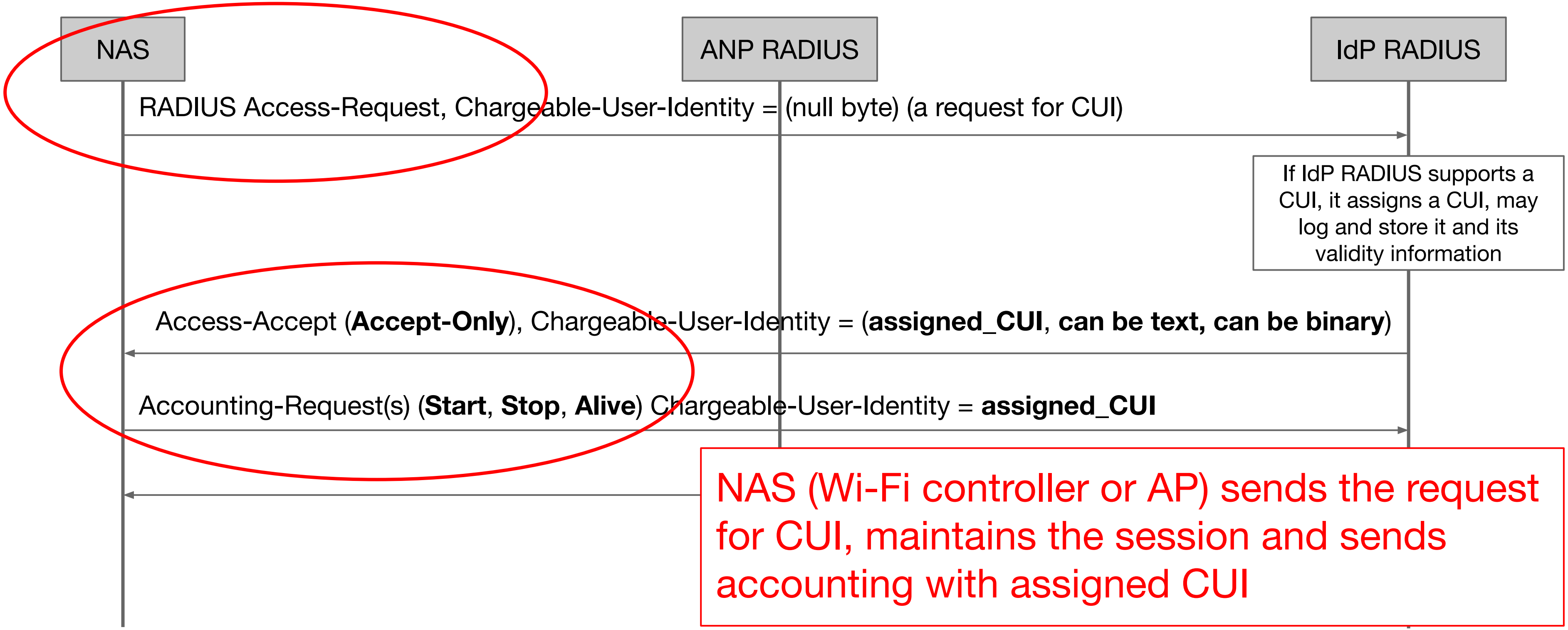
If IdP RADIUS supports a CUI, it assigns a CUI, may log and store it and its validity information

Access-Accept (**Accept-Only**), Chargeable-User-Identity = (**assigned_CUI**, **can be text, can be binary**)

Accounting-Request(s) (**Start**, **Stop**, **Alive**) Chargeable-User-Identity = **assigned_CUI**

Accounting-Response

NAS requests CUI and maintains the session



NAS

ANP RADIUS

IdP RADIUS

RADIUS Access-Request, Chargeable-User-Identity = (null byte) (a request for CUI)

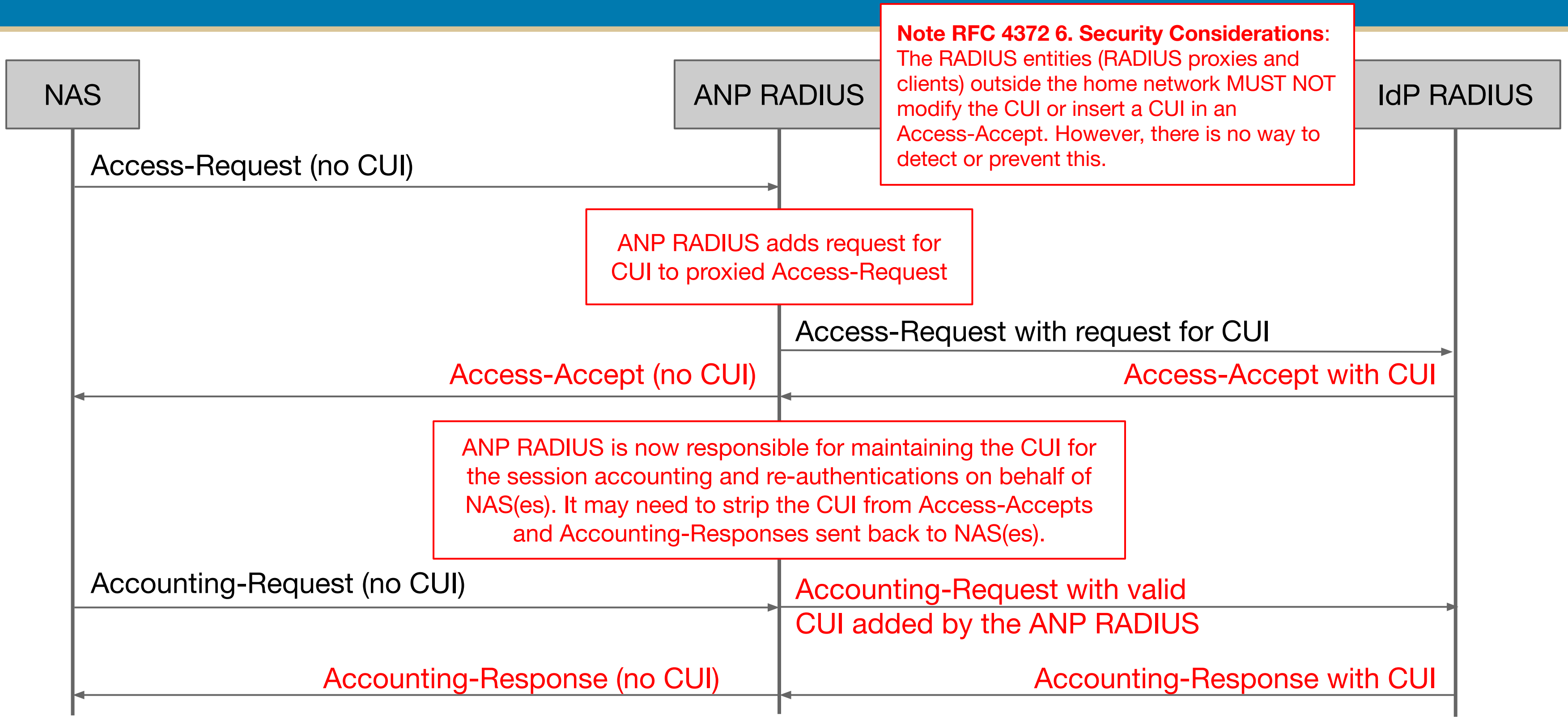
If IdP RADIUS supports a CUI, it assigns a CUI, may log and store it and its validity information

Access-Accept (**Accept-Only**), Chargeable-User-Identity = (**assigned_CUI**, **can be text, can be binary**)

Accounting-Request(s) (**Start**, **Stop**, **Alive**) Chargeable-User-Identity = **assigned_CUI**

NAS (Wi-Fi controller or AP) sends the request for CUI, maintains the session and sends accounting with assigned CUI

What if ANP RADIUS sends the CUI request?



NAS

ANP RADIUS

IdP RADIUS

Note RFC 4372 6. Security Considerations: The RADIUS entities (RADIUS proxies and clients) outside the home network MUST NOT modify the CUI or insert a CUI in an Access-Accept. However, there is no way to detect or prevent this.

Access-Request (no CUI)

ANP RADIUS adds request for CUI to proxied Access-Request

Access-Request with request for CUI

Access-Accept (no CUI)

Access-Accept with CUI

ANP RADIUS is now responsible for maintaining the CUI for the session accounting and re-authentications on behalf of NAS(es). It may need to strip the CUI from Access-Accepts and Accounting-Responses sent back to NAS(es).

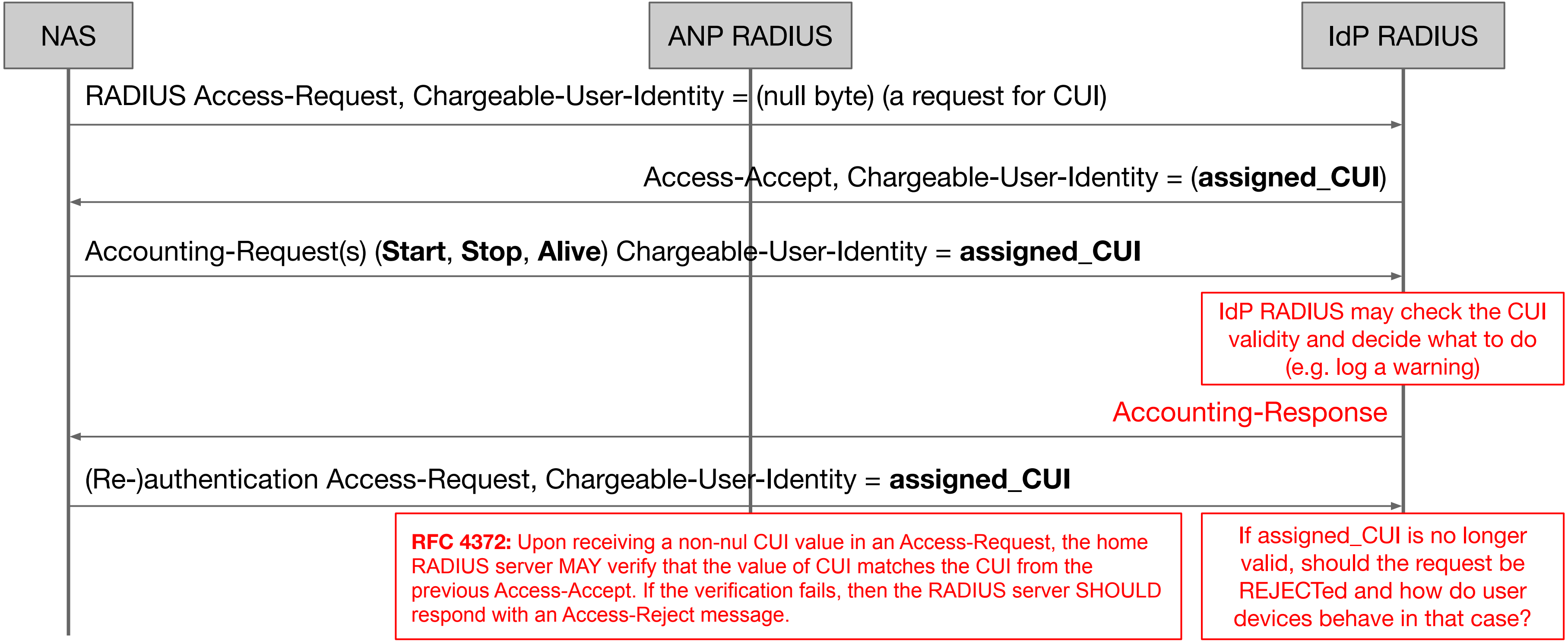
Accounting-Request (no CUI)

Accounting-Request with valid CUI added by the ANP RADIUS

Accounting-Response (no CUI)

Accounting-Response with CUI

Chargeable-User-Identity validity checks?



RADIUS Access-Request, Chargeable-User-Identity = (null byte) (a request for CUI)

Access-Accept, Chargeable-User-Identity = (**assigned_CUI**)

Accounting-Request(s) (**Start**, **Stop**, **Alive**) Chargeable-User-Identity = **assigned_CUI**

IdP RADIUS may check the CUI validity and decide what to do (e.g. log a warning)

Accounting-Response

(Re-)authentication Access-Request, Chargeable-User-Identity = **assigned_CUI**

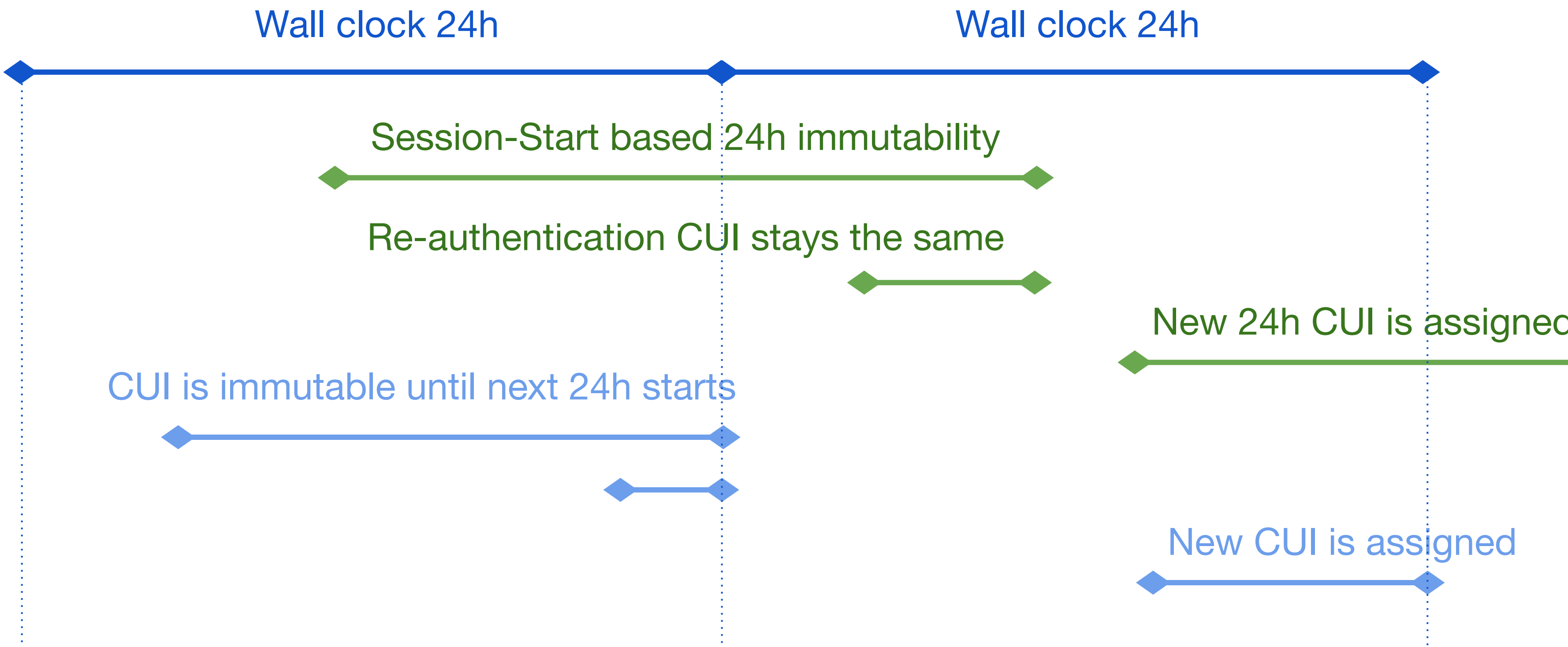
RFC 4372: Upon receiving a non-nul CUI value in an Access-Request, the home RADIUS server MAY verify that the value of CUI matches the CUI from the previous Access-Accept. If the verification fails, then the RADIUS server SHOULD respond with an Access-Reject message.

If assigned_CUI is no longer valid, should the request be REJECTed and how do user devices behave in that case?

Session start or wall clock based immutability?

- Should the Chargeable-User-Identity immutability time be started from accepted Access-Request?
- Or should the immutability be started according to the wall clock time?

24h Chargeable-User-Identity immutability



Wall clock 24h

Wall clock 24h

Session-Start based 24h immutability

Re-authentication CUI stays the same

New 24h CUI is assigned

CUI is immutable until next 24h starts

New CUI is assigned

Should the CUI be immutable across roaming partners?

- If the CUI is the same during its validity time across roaming partners, user could be tracked across different networks.

- If roaming partner id, such as Operator-Name is used to generate CUI, CUI could be roaming partner specific.

Stateful or stateless implementation?

- Stateful implementation (e.g. random CUI assigned for user) requires context sharing between authenticating IdP RADIUS servers, e.g. SQL database.

- In stateless implementation the validity time needs to be included in the CUI (generation), which can make checking of the CUI validity more complex for IdP.

Random, encrypted or hashed CUI?

- A random CUI is best for privacy, but the CUI validity needs to be stored separately => stateful implementation.
- An encrypted (e.g. with public key) CUI may contain identity and validity information inside CUI, but protected from roaming partners => stateless implementation is possible
- A hashed CUI needs to include validity times in the hashed string to comply with privacy requirements. The validity of the CUI may be harder to check (e.g. Session-Start based validity vs Wall clock validity).

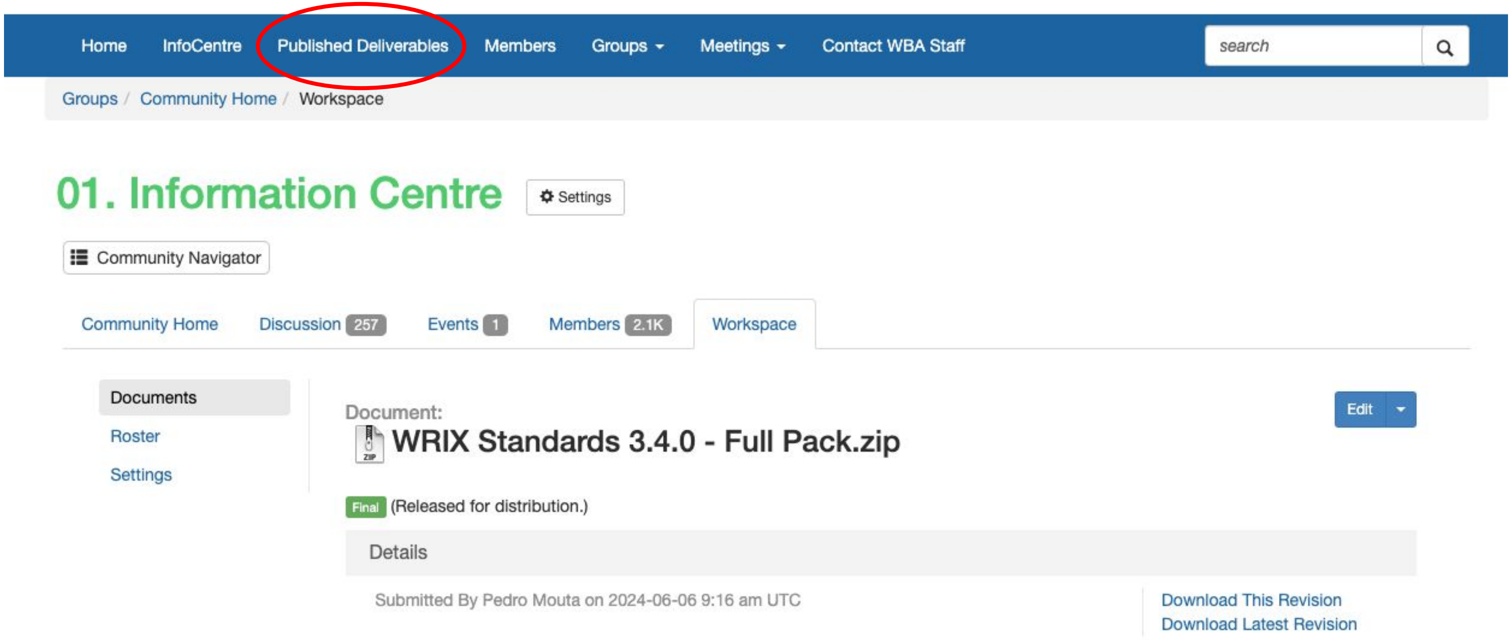
Issues to be considered

- All network equipment vendors do not implement CUI or do not implement it fully (the initial null-byte request):
  - Will the CUI be a MUST requirement for OpenRoaming? For Settled only or also for Settlement-Free?
  - How can an ANP without CUI capability join OpenRoaming?
  - Will the CUI functionality be tested in the OpenRoaming plugfests as a part of the compliance tests?
- As IdPs can implement Session-Start or Wall Clock based CUI immutability as they choose, it may be difficult for ANPs to generate reliable statistics, accounting and/or additional functionality for quota or policy control.

WBA WRIX-N - Network specification

- Part of WRIX Standards 3.4.0 Full Pack available on the WBA Extranet: https://extranet.wballiance.com
- Contains example Python code for generating CUI covering at least immutable and mutable (time limited) CUI generation, section 5.7, pages 30-34.
- Does not contain IdP RADIUS server configuration or implementation instructions => IdP’s responsibility is to check and configure the implementation properly (if IdP wants to support CUI)

WBA Extranet – WRIX Standards 3.4.0 Full Pack.zip



01. Information Centre

Document:

WRIX Standards 3.4.0 - Full Pack.zip

Final (Released for distribution.)

Details

Submitted By Pedro Mouta on 2024-06-06 9:16 am UTC

https://extranet.wballiance.com/ -> Published Deliverables