How is the CUI useful?

In the world of govroam (and 802.1X in general) when a user visits another site, the only information the a site has to identify the user is their outer identity and their calling station id (MAC address). Whilst this information is useful (when coupled with authentication event timestamp and IP address) without liaison with the Home site it is insufficient to provide a definitive identifier for the individual. This presents difficulties for the enforcement of AUP and the production of accurate stats.

CUI can help with accountability. If you have a visitor who breaks your AUP and you decide to ban them, how do you enforce this ban? You can't ban the outer identity because i) the user can change that to whatever they like and ii) the same outer identity could be used by multiple visitors (e.g. anonymous@camford.ac.uk) so you may end up blocking other innocent users. If you ban the CSI the user could just login on another device or spoof their CSI. Also, the MAC address may change as the result of the privacy features of the newest operating systems. By having a CUI you can definitively identify the user and block them based on the CUI. Additionally, if you do have an AUP issue when contacting the home site a CUI provides a more reliable link to the user than a CSI which could be spoofed.

CUI can help with measuring the usage of your govroam service. With only outer identity and CSI, it is difficult to determine how many visitors a site has. For example you could have 10 users all using govroam with the outer identity anonymous@govroam.uk. But is that really 10 different users or is it a single user on 10 different devices, or 5 users with 2 devices each etc? CUI solves this as each unique user has a different CUI (and the CUI is the same across all of the user's different devices).

How do I request a CUI for a user (Visited site)?

If you require a CUI for a user, you simply attach RADIUS attribute 89 (Chargeable-User-Identity) with a null value to the Access-Request.

The Home site authenticating the request should, upon receipt of a NUL Chargeable-User-Identity, generate the CUI value and return it in subsequent replies. This all falls down however if the Home organisation (IdP) has a RADIUS service which doesn't support CUI or hasn’t configured their RADIUS server to respond to CUI requests - you won’t get back a CUI.

If you do get back a CUI for a user, you must then include this in your internal accounting packets and not modify the value.

How do I generate a CUI for a user (Home site)?

If you receive a CUI request RFC 4372 says you should respond with the CUI for the user being authenticated. Whilst the RFC doesn’t specify the method, a CUI must be a transformation of the username. Therefore the recommended method for govroam is to MD5 hash the username together with a salt(*) and the visited site Operator Name.

Ideally the Visited site ORPS should send their Operator Name (Attribute 126) together with the CUI Request, however in cases where this is absent, the govroam NRPSs will inject Operator-Name on behalf of the Visited site using the value in the Identifier field in the Organisation setting panel on the

Configure page on Support server.

What does govroam say about CUI?

The govroam Technical Specification states that Visited organisations SHOULD request Chargeable-User-Identity (CUI) in Access-Request packets forwarded to the NRPS if CUI is supported by the ORPS. Home organisations SHOULD respond with a Chargeable-User-Identity (CUI) attribute in an Access-Accept, if the Home RADIUS server supports CUI, where CUI is solicited in the authentication request from the Visited organisation, as described in RFC 4372.

Moreover, a Chargeable-User-Identity response may only be generated by the Home organisation on the condition that the Access-Request from the Visited site contains a non-empty Operator-Name attribute. The value of Chargeable-User-Identity attribute returned in the response MUST have a constant value for each individual user and Operator-Name value. The value of the Chargeable-User-Identity attribute MUST be generated in such a way so as to ensure that the matching of this value to the actual user identity is possible only by the Home site.

(*) 'Salting' is a way of making passwords etc. more secure by adding a random string of characters before the MD5 hash is calculated, which makes it harder to reverse (the longer the random string, the harder you make it).