Level of Assurance Requirements 2014

Face to Face Level of Assurance Requirements 2014:

Face-to-face level of assurance requires that a new member of an identity federation (student, faculty, staff, etc) has appeared in person and presented a valid photo ID to verify his/her identity at the time his/her digital credentials are created. As stated in UCTrust policy: "A government or University issued ID with a picture must be presented to and verified by an officer of the Credential Provider as belonging to the registrant."

Verification of identity is already part of our standard CalNet deputy training, but we want to reiterate the importance of complying with this policy to ensure we comply with UC Trust standards.

CalNet deputies should never issue a token for someone before they have verified that person's identity.

Requirements if someone is not on Campus

The UC Trust federation has specific guidelines for establishing "face-to-face" level of assurance when users are not actually physically present. The guidelines state the following:

- The registrant must be prompted for at least two identifying attributes that are verified as belonging to the registrant. The attributes should be chosen to be relatively accessible to the registrant, but not to others. Examples include employee or student ID, birth day and month, etc.
- The process should include a step to confirm existing records [official records maintained by the University] of the registrant's electronic mail address, telephone number, or postal address. For example, a confirming email or a letter sent to registrant's postal address requiring a response would suffice. This step should either precede issuing credentials or be capable of revoking already-issued credentials in a timely manner.