UCSB Attribute Release Info

Current IdP Practices

The UCSB IdP does not release any attribute, singly or in combination, that would be classified as PII, regardless of the trust relationship with the relying party (RP).

UCSB only federates principals within the class of “associates”. The default associate category currently includes employees, students, and emeriti (former employees). The “affiliate” category includes all miscellaneous demographics for which no specific identity proofing process has been done. Affiliates default to LOA-0 and are not asserted to be principals within the UCSB IdP. Generally, an affiliate has the option to go through the identity proofing process sufficient to qualifying for LOA-1 assertion.

Anonymous relying parties (RP) are not supported. To receive a response from the UCSB IdP, an RP must be present either within the InCommon metadata or as a special case within the UCSB metadata. An RP within the InCommon metadata will only receive specific responses as defined below in (1) or (2). UCSB will not create special case metadata for other than a UCSB internal request that has passed through the identity advisory group process. Any UC service provider (SP) requesting this special case consideration must have a UCSB sponsor. UCSB attribute release will only occur for four categories of RP.

The four cases are --

1) InCommon Defined RP’s not known to UCSB .

2) RP present within InCommon and a contractual relationship with the UC Regents or UCSB.

3) Business of the UC or UCSB.

4) Special cases.

(1) InCommon Defined RP’s not known to UCSB

transientID, eduPersonScopedAffiliation (EPSA), eduPersonEntitlement (EPE) are released.

EPSA includes “member”, “employee”, “student”. EPE includes “common-lib-terms”.

(2) RP present within InCommon and a Contractual Relationship

transientID, givenName, sn, displayName, mail, EPSA, eduPersonPrincipalName (EPPN), EPE, UCnetID, UCTrustAssurance, UCTrustCampusIDShort

EPPN is constructed as UCSBnetID@ucsb.edu. UCTrustAssurance is blank or “basic” for InCommon Silver compliant principals.

(3) Business of the UC or UCSB

Adds employeeID and other foreign key strings as required by UC databases. No PII is ever used as a foreign key.

(4) Special Cases

HathiTrust has a specific business relationship with the UCSB Library.

Additional Information

All four categories for which any attribute data is returned will follow a successful authentication. Note that category (1) allows an unknown to UCSB RP to determine that the principal in question is a student. The student has volunteered their status as a student by completing the authentication process, and this falls well within FERPA guidelines.

The basic processes of identity proofing for the UCSB IdP create LOA-1 credentialed principals. LOA-2 identity proofing for InCommon Silver compliance is designed to be a manual, in-person process at the identity help desk. LOA-0 principals are created by various automated processes that do not involve any review. All LOA-0 principals have a time-to-live (TTL), the maximum setting for which can be a year, and may not be federated.

UCTrust “basic” can only be manually assigned to a principal. No work is being done to develop this further because InCommon Silver compliance will be achieved within the 2012 calendar year. When InCommon Silver certification becomes operational, both the UCTrustAssurance and eduPersonAssurance values will be provided by the UCSB IdP.

Any principal that has passed their ending date is removed from the identity repository referenced by the Shibboleth IdP. Such principals are still within the IAM, but must have an update made to their ending date in order to requalify for inclusion in federated authentication. LOA-0 principals are never federated.

All demographic categories have one or more sponsoring organizations. The UCSB IAM only sponsors employees, emeriti and students.

The UCSB IdP is incapable of supporting principals that do not conform to our requirements for being within a valid, non-temporary demographic, LOA-1 identity proofing and a well-defined TTL (ending date) that is maintained by the sponsoring organization for that demographic. SP’s and/or functional organizations who wish to propose the creation of a category of currently unsupported principals must provide a written business case. The UCSB IAM organization is available for consultation in writing such a proposition, and when finalized, will participate in bringing it to UCSB IT governance for conceptual approval and funding.