NC STATE UNIVERSITY

NC State Attribute Release Policy (ARP)

Attributes

Attributes are data elements that are used to provide identity information to requesting applications, or in the case of federated identity access - service providers (SP). Attributes are based on standard LDAP definitions or the eduPerson, eduOrg and eduCourse Object Classes. Commonly used attributes are listed in Table 1.1 below.

Attribute	Attribute Description
givenName	givenName – first name
sn	surname (last name)
displayName	Usually full name
mail	email address
EPPN	**eduPersonPrincipalName** – scoped username (e.g. jdoe@ncsu.edu)
EPTID	**eduPersonTargetedId** – Unique identifier (per service provider)
EPSA	**eduPersonScopedAffiliation** – Affiliation status (staff, student, …) with scoping modifier (@ncsu.edu, @ecu.edu, …)
EPE	**eduPersonEntitlement** – List of authorization for the person; this proposal assumes course information will not be in EPE
UID	un-scoped username (e.g. UnityID, jdoe), also called Principle

(Table 1.1)

Default ARP (by Federation)

NC State University belongs to a number of different trust federations which include different member populations. As a result, the "default" Attribute Release Policy for each federation varies based on the trust relationship NC State has with the other federation members, the need for certain attribute data and the risk associated with sharing attributes with other members providing resources to the federation. Listed below are the federations and the corresponding default ARP.

Exceptions to the "default" release of attributes can occur in any of the federations, however, any ARP for external (corporate) service providers, whether a member of the InCommon Federation or a standalone federation, requires a contract or legal agreement which explicitly states how the attributes will be used. This includes the initial connection to the service provider, as well as any capture or storage of the user attributes and the protection and deletion of that data throughout and at the termination of the agreement.

InCommon

The InCommon Federation is a national higher education and research federation whose participants include higher education members as well as sponsored partners that include corporate and government service providers.

Attribute	Attribute Description
EPTID	eduPersonTargetedId – Unique identifier (per service provider)
EPSA	eduPersonScopedAffiliation – Affiliation status (staff, student, …) with scoping modifier (@ncsu.edu, @ecu.edu, …)
EPE	eduPersonEntitlement – List of authorization for the person; this proposal assumes course information will not be in EPE

NCTrust

NCTrust is a pilot federation created for the purpose of exploring the use of federated identity management for K-20 populations accessing online resources across the state of North Carolina. It is inclusive of K-12 students and as minors are not legally able to make decisions about the release of personal data, the default ARP needs to be particularly well controlled.

Attribute	Attribute Description
EPTID	eduPersonTargetedId – Unique identifier (per service provider)
EPSA	eduPersonScopedAffiliation – Affiliation status (staff, student, …) with scoping modifier (@ncsu.edu, @ecu.edu, …)
EPE	eduPersonEntitlement – List of authorization for the person; this proposal assumes course information will not be in EPE

UNC Identity Federation

The UNC Identity Federation was created to share online resources and applications within the UNC System. With the addition of SPs to the federation being tightly controlled by UNC-GA, there is little risk associated with releasing Personally Identifiable Information (PII) to these applications, however, the amount of information released is still confined to commonly used attributes that will identify an individual's affiliation (student, faculty, staff), organization (university) and principle name or NetID. Class information might also be required, but this would be dealt with on a SP by SP basis.

Attribute	Attribute Description
givenName	givenName – first name
sn	surname (last name)
displayName	Usually full name
mail	email address
CPID	campusPermanentId – Unique, two-way, permanent identifier, non-FERPA protected in nature (within UNC-only)
EPPN	eduPersonPrincipalName – scoped username (e.g. jdoe@ncsu.edu)
EPTID	eduPersonTargetedId – Unique identifier (per service provider)
EPSA	eduPersonScopedAffiliation – Affiliation status (staff, student, …) with scoping modifier (@ncsu.edu, @ecu.edu, …)
EPE	eduPersonEntitlement – List of authorization for the person; this proposal assumes course information will not be in EPE

NC State University Identity Federation

The identity federation of NC State will be used in much the same way as other federations, however, as Shibboleth will over time replace the WRAP and Portal authentication for web applications there will be many more SPs on campus. Certain attributes will be included to assist with notification for expired passwords, FERPA privacy blocks, etc. The expectation is that over time, groupings of SPs will allow a more "focused" approach in releasing attributes. For example some applications only need to know a user is a member of campus (they have a university login account). Other applications might need to know enrollment information for students to allow access to course data, reserved books for a particular class, or other restricted web resources. The default list of attributes will initially be those indicated below.

Attribute	Attribute Description
NAME	sn – surname (last name), givenName – first name, displayName, eduPersonNickname, PreferedName
mail	email address
EPPN	eduPersonPrincipalName – scoped username (e.g. UnityID@ncsu.edu)
EPTID	eduPersonTargetedId – Unique identifier (per service provider)
EPSA	eduPersonScopedAffiliation – Affiliation status (staff, student, …) with scoping modifier (@ncsu.edu, @ecu.edu, …)
EPE	eduPersonEntitlement – List of authorizations for the person; this proposal assumes course information will not be in EPE
CRS	university regular enrollment course memberships (eduPersonEntitlement or eduCourseOffering or eduCourseMember)
UID	un-scoped username, UnityID (e.g. jdoe), also called Principle
Private	flag indicating FERPA privacy block
PWDexpired	flag indicating password has expired, SP can use as needed
ExpirationDate	date password expires, SP can use as needed

urn/url/oid Tables

SAML1.1 Attribute Name	Meaning
urn:mace:dir:attribute-def:**givenName**	First Name
urn:mace:dir:attribute-def:**sn**	Surname
urn:mace:dir:attribute-def:**eduPersonPrincipalName (EPPN)**	username
urn:mace:dir:attribute-def:**eduPersonTargetedID (EPTID)**	Targeted ID*
urn:mace:dir:attribute-def:**eduPersonAssurance (EPA)**	Level of Assurance

SAML2.0 Attribute Name	Meaning
urn:oid:2.5.4.42	First Name
urn:oid:2.5.4.4	Surname
urn:oid:1.3.6.1.4.1.5923.1.1.1.6	username
urn:oid:1.3.6.1.4.1.5923.1.1.1.10	Targeted ID*
urn:oid:1.3.6.1.4.1.5923.1.1.1.11	Level of Assurance

** Appropriate values for the eduPersonTargetedID attribute are defined in the EduPerson Object Class Specification (200604). These values are opaque, persistent, randomly generated strings that are particular to each user AND service provider (SP) or service provider group. Each user will have a different eduPersonTargetedID value for each SP he/she accesses, and each SP will always receive the same value for the same user every time he/she accesses the service. The eduPersonTargetedID attribute allows an SP to identify multiple accesses by the same user, while at the same time protecting the anonymity of the individual. The NC State University IdP generates a unique random value the first time a user accesses an SP and stores that value in a database for use in subsequent requests.*

Appendix A

Additional Attributes and SP-Specific ARPs

Google Apps for Education

Attribute	Attribute Description
EPSA	eduPersonScopedAffiliation – Affiliation status (staff, student, …) with scoping modifier (@ncsu.edu, @ecu.edu, …)
Principle/UID	Username (UnityID)

OrgSync Calendaring Application (Student Organizations) – "Requested"

Attribute	Attribute Description
sn	Last name
givenName	First name
mail	Email address