

COmanage Use Case 1 –

COmanage is a framework (implemented as an appliance or as a service) that provides coordinated identity management across a variety of applications. By identity management we mean authentication, group and privilege management, and related identity services. The variety of applications includes both collaboration tools (wikis, listprocs, calendaring, content management, etc) and domain specific tools (Grid access, instrument monitoring, etc.)

COmanage can be deployed in several ways, but in each of the variations, COmanage systems interact on attribute levels with many enterprises, spread across several federations, with entities outside of federated identity, and with each other.

The three-part use case below describes the requirements of a COmanage instance deployed as an appliance by an agency sponsored research project. A second use case will describe the requirements of COmanage deployed as a federation level service.

Use case:

Researcher Jean is a member of a CO called A1. They use a COmanage instance that is deployed at a lab that is registered both as an IdP and a SP in a federation (InCommon).

a. Jean wants to grant her class the ability to view one of the instruments operated by A1. The students have Jean's home institution as their IdP. The attribute that the instrument needs for access control is assigned by people within A1.

Issues:

Attributes, semantics and syntax –

There is a community-standard schema – eduCourse – that provides course number information as a unique identifier, scoped to a DNS name. It is not widely populated yet.

The act of authentication associated with all activities in this use case is considered to be InCommon Bronze level.

Assignment of values to attributes –

Legacy student administrative systems are considered to be authoritative in assigning a course entitlement to a student.

The course entitlements assigned by a legacy app are not likely to match the eduCourse schema values and a translation needs to happen

It is expected that the assignment of values are updated every day

Movement and location of attributes – ...

The identifiers used within COmanage and the student identifiers used by the source system on campus are not the same. Some linkage operation must be done, either manually by the user.

The instrument must be manually configured with an ACL to permit viewing access. The ACL contents can be typical individual, pre-configured group or world permissions. It can accept assertions from a manually configured set of sources, but could be configured to join a federation

Legal, privacy and secrecy considerations –

It is permissible to release such information to an “Authorized Outsourcer”

Consent is needed to release otherwise

It is assumed that the release of such info binds the recipient to “proper use”

b. One of the pieces of software that Jean runs is subject to export controls, and nationals from certain countries are not allow to access the instrument. When Jean assigns, within A1, the privilege for TA’s in her course to reset the instrument and so invoke the restricted software, she wants to conform with the federal policy.

Issues

Attributes, semantics and syntax –

The attribute of either citizenship or the ability for a yes/no answer to be provided by an authoritative policy and attribute source.

The act of authentication associated with all activities in this use case is considered to be InCommon Bronze level.

Assignment of values to attributes –

The business process for defining and recording citizenship, for students and for faculty and staff, are ad hocly assigned and their ability to conform with changing policies (e.g. currently restricted nationalities) is unclear

There is no normative schema that holds the attribute “citizenship”

Movement and location of attributes – ...

Legal, privacy and secrecy considerations –

It is permissible to release such information to an “Authorized

It is assumed that the release of such info binds the recipient to “proper use”

c. As part of its outreach effort , A1 resources are made visible through a science gateway portal. The portal gives unauthenticated (to the portal) users one view of A1 resources where users authenticated to the portal are mapped into groups and assigned additional privileges for A1 resources. COmanage would like to export its groups to the portal for access control or otherwise .

Attributes, semantics and syntax –

Assignment of values to attributes –

Movement and location of attributes –

Legal, privacy and secrecy considerations –