

Accessing Digital Objects in a Repository

Use Case ID	DIGITAL_REPOSITORY_01
Use Case Name	Accessing Digital Objects in a Repository
Level	System
Context Diagram	
Type	<p>Generalised - <i>a generic use case representing variations on a theme</i></p> <p>Summary: For individuals to access digital objects from repositories within the AAF (Australian Access Federation).</p> <p>On a regular basis, users will be accessing either their own or shared digital objects (documents, datasets, workflows, etc) potentially from any repository with authentication and access conforming to the AAF.</p>
Description	<p>Some of the digital objects may be long-lived (archived), and a solution will need to cater for changes in personal attributes of the owner of the digital object, and of those authorized to access it.</p> <p>Research data has a dynamic and continuous lifecycle. Individuals have various interactions with the data over its lifecycle (e.g curation, access, use). To determine the value of the data, details of all interactions <u>must</u> be recorded and preserved and identity information has to persist over the data's lifecycle.</p>
Priority	Essential
Frequency of Use	Regularly
Goals/Benefits	To access repositories seamlessly within the AAF (Australian Access Federation)
Actors	Primary: Individual Secondary: Service Provider

Triggers

- Individual identities (institutional) are provisioned.
- Digital Object Browser (Service Provider) and Individual's IdP trust each other.
- Digital Object Browser (Service Provider) and Digital Object Repository trust each other.

Pre-conditions

Post-conditions on Success Identified user has appropriate level of authorization.

Post-conditions on Failure

Extension Points

Normal Flow of events

1.0 Accessing a Digital Object in a Repository

1. Individual starts a digital object repository browser.
2. Individual's identity, or lack of identity, is established with the digital object repository browser.
3. Individual attempts to access a restricted digital object.
4. The user's identity is shared between the Digital Object Repository Browser and the selected Digital Object Repository.
5. The Digital Object Repository determines Individual's authorization based on identity and access rights.
6. Individual is allowed access to the selected digital object.

Alternate Flow of events

Exception Flows

DR1.0.1 E1 Authorisation denied (after step 5)

6: Individual is denied access and reason is communicated.

Includes Use Cases

A user's access to a digital object in a repository should not be affected by:

Special Requirements

- Change in email address
- Change in nameOr unnecessarily by a change of institution/affiliation, because their unique identification depends on it.

Assumptions

Required Attributes:

Data Items

- Globally unique identifier
- **eduPersonNickname, cn, displayName** NB. There may be quite a lot of other optional auEduPerson attributes which dictate a user's access to an object, e.g. eduPersonAffiliation

Messages

1. Individual identifiers must be unique, not change, or be recycled.
2. Service Providers must be able to uniquely identify Individuals. The known identity of Individuals is a requirement for access, logging, and audit.

Business Rules

External Interfaces Related Artifacts

Notes

If a user has write access to a digital repository in the Federation, then digital objects that they store there will need to be associated with one or more attributes from the auEduPerson schema that uniquely identifies the user within the Federation. The digital objects stored in these repositories may be quite long-lived.

Authors: Anthony Beitz and Lyle Winton

Stakeholders: AAF, ANDS, ARCHER, AAF, VERSI,
VPAC

Issues

- No attribute or set of attributes from the existing draft of the auEduPerson schema currently uniquely identifies a user within the AAF and is unaffected by a change in affiliation, email address, or name.