Canadian Access Federation: Trust Assertion Document (TAD)

1. Purpose

A fundamental requirement of Participants in the Canadian Access Federation is that they assert authoritative and accurate identity attributes to resources being accessed, and that Participants receiving an attribute assertion protect it and respect privacy constraints placed on it by the asserting Participant.

To accomplish this practice, CANARIE requires Participants to make available to all other Participants answers to the questions below.

1.1 Canadian Access Federation Requirement

Currently, the community of trust is based on “best effort” and transparency of practice. Each Participant documents, for other Participants, their identity and access management practices, which they can confidently meet. Each Participant should make available to other Participants basic information about their identity management system and resource access management systems registered for use within the Canadian Access Federation. The information would include how supported identity attributes are defined and how attributes are consumed by services.

1.2 Publication

Your responses to these questions must be:

1. submitted to CANARIE to be posted on the CANARIE website; and
2. posted in a readily accessible place on your web site.

You must maintain an up-to-date Trust Assertion Document.

Canadian Access Federation: Trust Assertion Document (TAD)

2. Canadian Access Federation Participant Information

2.1.1. Organization name: University of Victoria

2.1.2. Information below is accurate as of this date: **2020-03-02**

2.2 Identity Management and/or Privacy information

2.2.1. Where can other Canadian Access Federation Participants find additional information about your identity management practices and/or privacy policy regarding personal information?

Identity Management: https://www.uvic.ca/systems/services/loginspasswords/index.php

Protection of Privacy Policy:
https://www.uvic.ca/universitysecretary/assets/docs/policies/GV0235.pdf

2.3 Contact information

2.3.1. Please list person(s) or office who can answer questions about the Participant's identity management system or resource access management policy or practice.

Name: Garry Sagert
Title or role: Director, UVic Online
Email address: gsagert@uvic.ca
Telephone: 1-250-721-7692

3. Identity Provider Information

Two criteria for trustworthy attribute assertions by Identity Providers are: (1) that the identity management system be accountable to the organization's executive or business management, and (2) the system for issuing end-user credentials (e.g., userids/passwords, authentication tokes, etc.) has in place appropriate risk management measures (e.g. security practices, change management controls, audit trails, accountability, etc.).

3.1 Community

3.1.1. As an Identity Provider, how do you define the set of people who are eligible to receive an electronic identity? If exceptions to this definition are allowed, who must approve such an exception?

The identity management system restricts access to electronic identity to only those individuals that meet specific criteria in our local systems of record (SORs). The SOR sources are:

- Banner General Person database
- Continuing Studies Student Records System (SRS)

UVic guests are allowed access to electronic identity through a sponsorship process, and must be renewed for ongoing access to online resources.

3.1.2. What subset of persons registered in your identity management system would you identify as a "Participant" in SAML identity assertions to **CAF** Service Providers?

SAML identity assertions are restricted to standards-track values assigned to the multi-valued eduPersonAffiliation attribute released by our Shibboleth Identity Provider. These values include ("employee", "faculty", "staff", "student").

These eduPersonAffiliation values are defined as:

Employee: principal has an active employee record in the Banner HR system

Faculty: principal is an active employee that has a a current faculty appointment in the Banner HR system

Staff: principal is an active employee that has a current staff appointment (non-faculty) in the Banner HR system

Student: principal is an active:

- Registered or admitted UVic graduate, or undergraduate student
- Registered UVic Continuing Studies student

3.2 Electronic Identity Credentials

3.2.1. Please describe, in general terms, the administrative process used to establish an electronic identity that results in a record for that person being created in your electronic identity database? Please identify the office(s) of record for this purpose.

Electronic identity records are created in our identity management system for people that meet specific business criteria for members of the UVic community.

UVic employees are on-boarded through the hiring process managed through the UVic HR Office (https://www.uvic.ca/hr)

UVic students are on-boarded through enrolment processes managed by the UVic Office of the Registrar (https://registrar.uvic.ca/)

UVic Continuing Studies students enrol through a process managed by UVic Continuing Studies (https://continuingstudies.uvic.ca/)

3.2.2. What authentication technologies are used for your electronic identity credentials (e.g., Kerberos, userID/password, PKI, ...) that are relevant to Canadian Access Federation activities? If more than one type of electronic credential is issued, how is it determined who receives which type? If multiple credentials are linked, how is this managed (e.g., anyone with a Kerberos credential also can acquire a PKI token) and audited?

UVic supports a campus-wide username/password credential pair called the UVic NetLink ID. This credential is used for access to CAF resources.

3.2.3. If your electronic identity credentials require the use of a secret password or PIN, and there are circumstances in which that secret would be transmitted across a network without being protected by encryption (e.g., “clear text passwords” are used when accessing campus services), please identify who in your organization can discuss with any other Participant concerns that this might raise for them:

UVic does not support clear-text passwords for access to campus resources. CAF resources will be authenticated through HTTPS channels.

3.2.4. If you support a “single sign-on” (SSO) or similar campus-wide system to allow a single user authentication action to serve multiple applications, and you will make use of this to authenticate people for **CAF** Service Providers, please describe the key security aspects of your SSO system including whether session timeouts are enforced by the system, whether user-initiated session termination is supported, and how use with “public access sites” is protected.

UVic supports open-source Apereo CAS for campus SSO. CAS supports authentication for the UVic Shibboleth IdP.

The default CAS SSO timeout is 2 hours. Users may initiate an SSO sign-out by clicking the CAS SSO “Sign Out of UVic” link on UVic web-sites integrated with CAS.

3.2.5. Are your primary electronic identifiers for people, such as “NetID,” eduPersonPrincipalName, or eduPersonTargetedID considered to be unique for all time to the individual to whom they are assigned? If not, what is your policy for re-assignment and what is the interval between such reuse?

UVic NetLink ID and eduPersonPrincipalName are considered to be unique for all time to the individual assigned. eduPersonTargetedID is also considered to be unique.

3.3 Electronic Identity Database

3.3.1. How is information in your electronic identity database acquired and updated? Are specific offices designated by your administration to perform this function? Are individuals allowed to update their own information on-line?

Attributes in the identity warehouse are updated according to administrative updates in the systems of record for each attribute. UVic has designated offices that perform these updates: Office of the Registrar, HR & Benefits, Finance, Continuing Studies

Individuals may update some personal information via self-serve such as their “preferred email address”.

3.3.2. What information in this database is considered “public information” and would be provided to any interested party?

Public information includes UVic employee contact information.

3.4 Uses of Your Electronic Identity Credential System

3.4.1. Please identify typical classes of applications for which your electronic identity credentials are used within your own organization.

Access to learning management systems, online file-storage systems, collaboration systems, library/research databases, web sites, email systems, computer lab workstations.

3.5 Attribute Assertions

Attributes are the information data elements in an attribute assertion you might make to another Canadian Access Federation Participant concerning the identity of a person in your identity management system.

3.5.1. Please describe the reliability of your identity provider attribute assertions?

Highly reliable.

3.5.2. Would you consider your attribute assertions to be reliable enough to:

a) control access to on-line information databases licensed to your organization?
Yes

b) be used to purchase goods or services for your organization?
Yes

c) enable access to personal information such as student record information?
Yes

3.6 Privacy Policy

Canadian Access Federation Participants must respect the legal and organizational privacy constraints on attribute information provided by other Participants and use it only for its intended purposes.

3.6.1. What restrictions do you place on the use of attribute information that you might provide to other Canadian Access Federation participants?

Attributes are to be used in accordance with the policy and procedures defined in the UVic Protection of Privacy Policy, linked in section 1.2.1.

3.6.2. What policies govern the use of attribute information that you might release to other Canadian Access Federation participants?

- BC Freedom of Information and Protection of Privacy Act (FOIPPA)
- UVic Information Security Policy: https://www.uvic.ca/universitysecretary/assets/docs/policies/IM7800.pdf
- UVic Protection of Privacy Policy

3.6.3. Please provide your privacy policy URL.

https://www.uvic.ca/universitysecretary/assets/docs/policies/GV0235.pdf

4. Service Provider Information

Service Providers, who receive attribute assertions from another Participant, shall respect the other Participant's policies, rules, and standards regarding the protection and use of that data. Such information must be used only for the purposes for which it was provided.

Service Providers are trusted to ask for only the information necessary to make an appropriate access control decision, and to not misuse information provided to them by Identity Providers. Service Providers must describe the basis on which access to resources is managed and their practices with respect to attribute information they receive from other Participants.

4.1 Attributes

4.1.1. What attribute information about an individual do you require in order to manage access to resources you make available to other Participants? Describe separately for each service application that you offer to CAF participants.

1) HubZero Portal for Digital Humanities Researchers :
    - Portal belongs to Research & Scholarship entity category, and accepts the standard attributes in the R&S payload:
        - Mail
        - eduPersonPrincipalName
        - displayName (or givenName and sn)
        - eduPersonScopedAffiliation

4.1.2. What use do you make of attribute information that you receive in addition to basic access control decisions?

1) HubZero portal
    a. Attributes are used to personalize accounts for researchers, and allow collaboration within the portal

4.1.3. Do you use attributes to provide a persistent user experience across multiple sessions?

1) HubZero portal
    a. Yes. Biographic attributes reside on each account, and allow researchers to identify each other in the portal environment.

4.1.4. Do you aggregate session access records or record specific information accessed based on attribute information.

1) HubZero portal – No

4.1.5. Do you make attribute information available to other services you provide or to partner organizations?

1) HubZero portal – No

4.2 Technical Controls

4.2.1. What human and technical controls are in place on access to and use of attribute information that might refer to only one specific person (i.e., personally identifiable information)? For example, is this information encrypted for storage in your system?

1) HubZero portal
    a. User accounts
        i. Researchers may create a basic account on initial successful login to the system through federated-SSO. These accounts are assigned an entry-level role that provides the same privileges as a non-logged in user. It is not until the user is approved by an administrator that they can use the dashboard and edit their profile.
        ii. A HubZero portal administrator must manually assign user roles or permissions to grant further access to the portal services and data.
    b. Portal accounts database data is not encrypted at rest.

4.2.2. Describe the human and technical controls that are in place on the management of super-user and other privileged accounts that might have the authority to grant access to personally identifiable information?

1) HubZero portal
    a. Privileged Accounts
        i. These are only available to UVic Systems Administrators that manage the portal infrastructure in the Research Data Centre.

4.2.3. If personally identifiable information is compromised, what actions do you take to notify potentially affected individuals?

1) HubZero portal
    a. HubZero is not intended to contain Personally Identifiable Information. Before receiving access, users must agree to a Terms of Use. UVic researchers that are employed by UVic are also subject to GV0235 - Protection of Privacy Policy.

5. Other Information

5.1 Technical Standards, Versions and Interoperability

5.1.1. Identify the SAML products you are using. If you are using the open source Internet2 Shibboleth products identify the release that you are using.

Identity Providers:

- Shibboleth Identity Provider v3.4.6

Service Providers:

- HubZero Portal : Shibboleth Service Provider v 3.0.4

5.1.2. What operating systems are the implementations on?

Identity Provider:

Shibboleth IdP: Redhat Enterprise Linux 6.x

Service Providers:

HubZero Portal: RedHat Enterprise Linux 7.x

What versions of the SAML protocol (1.1 or 2.0) do you support in your implementations?

- SAML 1.1 – No
- SAML 2.0 - Yes

5.2 Other Considerations

5.2.1. Are there any other considerations or information that you wish to make known to other Canadian Access Federation Participants with whom you might interoperate? For example, are there concerns about the use of clear text passwords or responsibilities in case of a security breach involving identity information you may have provided?

As an IdP, UVic is SIRTFI compliant, https://www.canarie.ca/identity/fim/sirfti/. As a result, we have logs and records of user activity, monitor our systems and will help in the event of an incident (typically on SP end).

6.0 Version History

Version	Date	Author	Notes
1.0	April 11, 2019	Corey Scholefield	Updates to sections 3, 4 and 5
2.0	April 26, 2019	Veronica Augustin	Updates to: • 4.2.1 following consult with Research Computing Services • 4.2.3 following consult with Information Security • 5.1 following consult with UVic Online and RCS
2.1	May 6, 2019	Veronica Augustin	Incorporated updated hyperlinks from Scott.
2.2	Feb 25, 2020	Veronica Augustin	Incorporated Ray's updates.
2.3	Mar 2, 2020	Veronica Augustin	Mario reviewed and approved.
2.4	April 6, 2020	Ivan Petrovic	Updates to section 4, contact info