

Canadian Access Federation: Trust Assertion Document (TAD) for Participating Organizations

Purpose

Identity attributes are characteristics of an identity -- such as a name, department, location, login ID, employee number, e-mail address, etc.

A fundamental requirement of Participants in the Canadian Access Federation (CAF) is that by their authority they send accurate identity attributes to other Participants to allow access to resources, 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 in this document.

Canadian Access Federation Requirement

The CAF 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 makes 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 includes how supported identity attributes are defined and how attributes are consumed by services.

Publication

Your responses to these questions must be submitted to CANARIE to be posted on the CANARIE website. You must maintain an up-to-date Trust Assertion Document.

Canadian Access Federation – Trust Assertion Document (TAD)

1. Participant Information

1.1 Organization Name: St. Lawrence College of Applied Arts and Technology

1.2 Information below is accurate as of this date: 09/26/2022

1.3 Contact Information

1.3.1. Please list the office, role, department, or individual who can answer questions about the Participant's identity management system or resource access management policy or practice.

Note: This information should be for a department or office rather than an individual, in order to avoid responses going unanswered if personnel changes occur.

Department (or Contact Name): Information Technology Services - Security

Email Address: soc@sl.on.ca

Telephone: 613-544-5400 x1000

1.4 Identity Management and/or Privacy Information

1.4.1. What policies govern the use of attribute information that you might release to other CAF Participants? If policies are available online, please provide the URL.

<https://www.stlawrencecollege.ca/privacy-notice>

1.4.2. Please provide your Privacy Policy URL, as well as information regarding any other policies that govern the use of attribute information that you might release to other CAF Participants.

<https://www.stlawrencecollege.ca/privacy-notice>

2. Identity Provider Information (FIM and/or eduroam)

Identity Providers must meet these two criteria for trustworthy attribute assertions:

- (1) The identity management system is accountable to the organization's executive or business management, and
- (2) The departmental processes and systems for issuing end-user credentials (e.g., user IDs/passwords, authentication tokens, etc.) have in place appropriate risk management measures (e.g. security practices, change management controls, audit trails, accountability, etc.).

2.1 Credential Practices

2.1.1. As an Identity Provider, you define who is eligible to receive an electronic identity.

What subset of persons registered in your identity management system would you identify as "Active" in identity assertions to the other Participants?

Employees, Students, Contractors, Applicants

Canadian Access Federation – Trust Assertion Document (TAD)

2.1.2. Long-lived, non-reassigned, and unique identity identifiers are critical for the safe and sustainable operation of the CAF community.

Do your identity identifiers ever get reassigned?

Yes

No

If “Yes”, please include details, such as the interval between reuse.

Since we use userPrincipalName as the unique identifier for a credential and it aligns with their College email address, we have a policy which prevents the reuse of the unique identifier for a minimum of 5 years after the original owner's account is deleted. If a person with the same name joins the College after that period of time, they may receive the same userPrincipalName and email address as a previous person.

2.1.3. "Attributes" are information elements about the identity of a person in your identity management system. This information is in the attribute assertion you might make to another Participant (Service Provider). These attribute assertions must be considered highly reliable in order for you to join CAF.

Do you consider your attribute assertions to be reliable enough to:

Control access to online information databases licensed to your organization?	<input checked="" type="checkbox"/> Yes <input type="checkbox"/> No
Be used to purchase goods or services for your organization?	<input checked="" type="checkbox"/> Yes <input type="checkbox"/> No
Enable access to personal information such as student record information?	<input checked="" type="checkbox"/> Yes <input type="checkbox"/> No

3. Service Provider Information (Federated Identity Management and/or eduroam)

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.

Canadian Access Federation – Trust Assertion Document (TAD)

3.1 Attributes

3.1.1. What attribute information about an individual do you require? Describe each service that you offer to CAF Participants separately (one service per row).

Service Name	Is this an R&S service?	Attributes Required	Rationale	Is information shared with others?
eduroam	N/A	<p>Standard RADIUS attribute set (Appendix A of the eduroam Compliance Statement):</p> <ul style="list-style-type: none"> • timestamp of authentication requests and corresponding responses • the outer EAP identity in the authentication request (User-Name attribute) • the inner EAP identity (actual user identifier) • the MAC address of the connecting client (Calling-Station-Id attribute) • type of authentication response (i.e. Accept or Reject). 	For authentication purposes	No
Example {FIM Service 1}	<input type="checkbox"/>	<ul style="list-style-type: none"> • user identifier (eduPersonPrincipalName + eduPersonTargetedID) • person name (givenName + sn) • email address • affiliation (eduPersonScopedAffiliation) 	For authentication (user identifier, person name, email address) and authorization (affiliation) purposes	No
{FIM Service 2}	<input type="checkbox"/>			

Notes: The standard attributes for eduroam have been pre-filled to assist with completion. If you are not implementing eduroam, please delete this row.

Additionally, an example of a [Research & Scholarship \(R&S\) Entity Category](#) FIM service and its associated attributes has been included. Please delete this example and enter your own data, as applicable. Add additional rows to the table, as required.

Canadian Access Federation – Trust Assertion Document (TAD)

3.2 Technical Controls

Technical controls are a basis for controlling access to and usage of sensitive data and are expected to be applied across all services. If there are exceptions for a particular service(s), please describe these exceptions.

3.2.1. Describe the human and technical controls in place for access to and use of attributes considered personally identifiable information.

Only those with elevated access privileges can access sensitive data and systems. The data center is only accessible by authorized personnel. Data center physical access is controlled by card-key access and the area is covered by security cameras and an alarm system.

3.2.2. Describe the human and technical controls that are in place for the management of super-user and other privileged accounts that may have the authority to grant access to personally identifiable information.

IT Security creates and administers privileged user accounts for authorized personnel that require elevated privileges. A privileged account may be configured to be a super user where required and is used only when required and not for daily work routines such as email. All privileged accounts are set up with MFA at the time of creation.

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

If personally identifiable information is compromised the privacy office is notified and an investigation is launched. The privacy office will determine what internal and external resources need to be involved to determine the cause of the compromise, the seriousness of the compromise, and any communication that may need to happen.

3.3 Other Considerations

3.3.1. Are there any other considerations or information that you wish to make known to other CAF Participants with whom you may interoperate?

Click or tap here to enter text.