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.

1. Participant Information

1.1 Organization Name: Carlton Trail College

1.2 Information below is accurate as of this date: 06/15/2026

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): IT Manager

Email Address: it@carltontrailcollege.com

Telephone: 3066822623

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.

Federated Identity and Attribute Information Sharing

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.

Privacy Statement

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?

Staff, Students, Vendors

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.

Click or tap here to enter text.

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?	☒ Yes ☐ No
Be used to purchase goods or services for your organization?	☒ Yes ☐ No
Enable access to personal information such as student record information?	☒ Yes ☐ 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.

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	**Standard RADIUS attribute set (Appendix A of the eduroam Compliance Statement):** • 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}**	☐	• **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}	☐			

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.

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.

Carlton Trail College applies administrative, technical, and operational controls to protect attributes that may be considered personally identifiable information. Access to attribute information is limited to authorized users and approved services based on business need, role, and least-privilege principles. Attribute use is limited to the purpose for which the information was provided, such as authentication, authorization, troubleshooting, security monitoring, privacy compliance, or approved operational support. Technical safeguards include controlled account provisioning and deprovisioning, role-based access permissions, password and authentication controls, logging and monitoring of relevant systems, endpoint protection, vulnerability and patch management, and secure handling of records and evidence. Access, use, disclosure, retention, and disposal of personal information are expected to align with College privacy, security, records management, and applicable legislative requirements, including LAFOIP where applicable.

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.

Privileged and super-user accounts are restricted to authorized Information Technology personnel or approved service providers with a defined operational need. Privileged access must be approved, assigned individually where practical, limited to the minimum access required, and removed or adjusted when the need ends, responsibilities change, or security concerns are identified. Administrative accounts are managed separately from standard user accounts where practical and are subject to stronger authentication, careful password handling, limited sharing, and monitoring appropriate to the system and risk. Use of privileged access is expected to be for authorized administration, support, security, troubleshooting, or incident response purposes only. Privileged account activity may be logged, reviewed, and escalated where suspicious activity, unauthorized access, compromised credentials, misuse, or privacy risk is suspected. Supplier or vendor privileged access must be approved before use, limited to the approved support purpose, and removed or adjusted when no longer required.

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

If personally identifiable information is suspected or confirmed to be compromised, Carlton Trail College assesses the incident to determine the nature of the information involved, the individuals affected, the likelihood and severity of harm, whether unauthorized access, use, disclosure, alteration, loss, or destruction occurred, and what containment or corrective actions are required. The College takes reasonable steps to contain the incident, preserve relevant evidence, investigate the cause, revoke or adjust access where required, remediate affected systems or accounts, and document the incident and response actions. Potentially affected individuals are notified where appropriate based on the results of the assessment, applicable legal or policy requirements, and the level of risk. Notifications may include a description of the incident, the type of information involved, recommended protective steps, and contact information for follow-up. Where required, the College may also notify appropriate internal authorities, service providers, regulators, law enforcement, or other relevant parties.

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?

Carlton Trail College interoperates with other CAF Participants on the understanding that attribute information will be requested, released, used, retained, and disclosed only for authorized authentication, authorization, security, troubleshooting, and operational purposes. The College expects participating services to follow applicable CAF requirements, respect the purpose for which attributes are provided, request only the minimum information required, and apply appropriate safeguards to

protect personal and sensitive information. Any concerns related to attribute handling, unauthorized access, privacy, security, service misuse, or operational issues should be reported promptly to the College contact identified in this Trust Assertion Document so that the matter can be assessed, contained, escalated, and resolved as appropriate.