Canadian Access Federation:
Trust Assertion Document (TAD) for Service Providers

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: ARUCC

1.2 Information below is accurate as of this date: 01/27/2026

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): Parchment Digitary, by Instructure

Email Address: support@digitary.net

Telephone: Click or tap here to enter text.

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.

As a Service Provider, the platform consumes attributes solely for the purpose of session provisioning and service delivery for the authenticated user; we do not release, share, or redistribute attribute information to other CAF Participants.

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://mycreds.ca/privacy-policy/
https://trust.instructure.com/

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

Not applicable

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.

As a part of the platform architecture, CAF remains the primary custodian of identity. Our controls are focused on the secure ingestion, minimized storage, and audited access to the specific attributes (PII) passed to us upon the successful completion of authentication through CAF. The returned attributes are specifically used to identify learners onto the MyCreds Learner Portal and correctly associate them with their issued documents and badges. Our security controls are independently verified through our annual SOC2 Type II audit, ISO27001 compliance and other controls ensuring that the PII shared is handled appropriately. Further information is available here: https://trust.instructure.com/.

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.

Our management of privileged accounts is strictly governed by the Principle of Least Privilege. To ensure total transparency, every action performed by users is captured as a part of audit controls that are also streamed to centralized logging environments, where real-time alerts and proactive monitoring immediately notify our security operations team of any unauthorized access. This technical framework is validated through regular access control audits and re-certifications.

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

In the event of a PII compromise, we execute a notification protocol strictly aligned with GDPR Articles 33 and 34. We first notify the relevant supervisory authority within 72 hours of discovery unless the breach is unlikely to result in a risk to individuals. Crucially, when a breach is likely to result in a high risk to the rights and freedoms of individuals, we notify those affected directly and without delay. This communication is delivered in plain language and includes the nature of the breach and the specific remediation measures taken to mitigate the impact.

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?

No