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: St. Thomas University

1.2 Information below is accurate as of this date: 01/30/2026

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): Frank Pani

Email Address: itsdirector@stu.ca

Telephone: 506-452-0484

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.

St. Thomas University's release and use of identity attributes provided to other CAF Participants is governed by:

The Right to Information and Protection of Privacy Act (RTIPPA) of New Brunswick — see the Government of New Brunswick overview and resources, and the consolidated text of the Act:

Overview & resources: gnb.ca – Information access and privacy / RTIPPA
https://www.gnb.ca/en/gov/information-access-privacy/rippa-act.html
• Consolidated statute: R-10.6 – Right to Information and Protection of Privacy Act
https://laws.gnb.ca/en/document/cs/R-10.6

St. Thomas University's Policy on Privacy and Protection of Information — see:
• Policy statement page: Policy Statement on Privacy and Protection of Information (STU)
https://www.stu.ca/policy-statement-on-privacy-and-protection-of-information/

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.

See above 1.4.1.

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?

"Active" persons for identity assertions are:
• Current employees (faculty and staff) with an active HR relationship.
• Currently enrolled students.
• Retirees/emeriti who have been explicitly authorized to retain an account.
• Sponsored affiliates (e.g., visiting scholars and contractors) for the duration of an active sponsorship/business need.

Note: Student accounts remain active for a short, defined post-completion grace period to support wrap-up activities; sponsored affiliate access ends when the engagement or sponsorship ends.

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

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.

Human controls (governance & access):

• Least-privilege administration. Access to identity attributes in the institutional directory is restricted to a very small cohort within ITS. Privileged access is granted only to designated administrators, with any broader delegation considered only where the tools allow tightly scoped changes.
• Privacy oversight and legal basis. Handling of personal information is governed by the Right to Information and Protection of Privacy Act (RTIPPA) of New Brunswick and the University's Policy on Privacy and Protection of Information; the University's Privacy Officer oversees responses to any potential privacy incidents under RTIPPA

Technical controls (identity platform & protection):

• Authoritative directory & central management. Identity attributes originate from authoritative systems (HR and the Student Information System) and are centrally managed in Microsoft Active Directory / Aszure. Attribute creation and updates are performed by ITS, ensuring consistency and control over directory data.
• Strong authentication & SSO. Users authenticate with institutional credentials; passwords are never transmitted in clear text. For campus services (e.g., Microsoft 365 and moodle.stu.ca), users are prompted for multi-factor authentication (MFA) when required.
• Identifier hygiene. Primary identifiers are unique and not re-assigned, supporting reliable, privacy-preserving federation identifiers.
• Data minimization for attribute release. When asserting attributes to relying parties, only the minimum attributes necessary are released, and receiving parties are expected to handle the data securely and delete it when no longer required.

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.

Human controls (who can hold privileged access & how it's governed)

• Strictly limited custodianship. Privileged ("super-user") access to identity attributes is held by a very small number of individuals within ITS. Access is granted only where required for job duties, and any future delegation (e.g., to HR for employee-specific attributes) is allowed only when the tools can constrain changes to that group's scope of authority.
• Policy and oversight. Handling of personal information by privileged users is governed by the Right to Information and Protection of Privacy Act (RTIPPA) and STU's Policy on Privacy and Protection of Information; the University's Privacy Officer provides oversight and guidance on questions or incidents

involving personal information. [canarie.ca], [STU-Policy...nformation | PDF]

Technical controls (how privileged access is protected & monitored)

- **Authoritative directory & role scoping. Identity attributes are centrally managed in Microsoft Active Directory by ITS. Administrative group membership is restricted to designated admins; changes to attributes are performed via controlled administrative tooling.**
- **Secure authentication practices. Passwords are never transmitted in clear text; authentication to campus services is protected, and identifiers are unique and not re-assigned, reducing risks of privilege confusion or impersonation.**
- **Change control and accountability. Privileged operations are performed under established security practices with change management controls and auditability consistent with federation expectations (e.g., audit trails and accountability for administrative actions).**

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

If STU becomes aware of an actual or suspected compromise of PII, we follow the steps below:

1 - Activate privacy incident response and notify the University's Privacy Officer.
ITS immediately engages the Privacy Officer to lead response under the Right to Information and Protection of Privacy Act (RTIPPA) and the University's Policy on Privacy and Protection of Information. The original TAD specifies that notification decisions are taken case-by-case in consultation with the Privacy Officer. Our incident response is documented, reviewed yearly and documented as an artifact as part of our NIST standard (incident response).

2. Contain, investigate, and assess risk.
We contain the incident, confirm the scope and data elements involved, and assess potential harm, guided by RTIPPA and institutional policy (incident response)..

3. Determine notification requirement and audience.

4. Notify affected individuals "as soon as practicable," with clear, actionable content.
Where notification is required, communications to affected individuals typically include: what happened (and when, if known), what information was involved, steps taken to contain and mitigate, recommended protective actions for the individual, and how to contact STU for assistance. Artifact documented under compromised accounts.

5. Coordinate with third-party service providers when they are involved.
If a service provider experiences a breach affecting STU data, they are contractually obligated to promptly notify STU with incident details (nature, timing, cause, responsible party if known, mitigation, and prevention measures). STU then proceeds with Steps 1–4 and communicates with affected individuals where appropriate.

6. Engage external authorities and stakeholders as appropriate.

7. Document, remediate, and review. Log in our incident tracker.

We maintain records of the incident, notifications, and corrective actions, and we review controls to reduce the likelihood or impact of recurrence, consistent with University policy.

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?

Nothing at this time.