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.

1. Participant Information

1.1 Organization Name: CANARIE Inc.

1.2 Information below is accurate as of this date: 02/25/2020

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.

Department (or Contact Name): **Nancy Carter (Chief Financial Officer)**

Email Address: **nancy.carter@canarie.ca**

Telephone: **613-943-5437**

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.

CANARIE Privacy Policy: https://www.canarie.ca/about-us/privacy-policy/

CAF Participation Agreement: https://www.canarie.ca/?wpdmdl=10721

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.canarie.ca/about-us/privacy-policy/

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?

CANARIE issues electronic identities to individuals with immediate and active relationships with CANARIE, based on our internal HR policies. This includes staff, board members, contractors, and certain CANARIE partners.

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.

N/A

2.1.3. "Attributes" are informational 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 & Entity ID	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
eduroam Visitor Access (https://eva.eduroam.ca/shibboleth)	☒	• **user identifier** (eduPersonPrincipalName) • **person name** (givenName + surname + cn) • **display name** • **email address** • **affiliation** (eduPersonAffiliation + eduPersonScopedAffiliation)	For authentication and authorization (affiliation) purposes	No
CANARIE Ticketing System (TTS) (https://tts.canarie.ca/shibboleth)	☐			
CANARIE Research Software Portal (https://science.canarie.ca/shibboleth)	☒			
CANARIE SharePoint (http://adfsgw.canarie.ca/adfs/services/trust)	☐			

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.

CANARIE follows and applies industry security best practices for managing access to resources. Services that contain personally identifiable information (PII) have audit capabilities to identify who accesses, retrieves or has administrator control over this information. Audit is used for both access logging and for the purpose of operating and diagnosing the health of the service.

All of our services are firewalled and stored in virtualized infrastructure.

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.

Service Administrator accounts are limited to a small number of users. Assignment of these privileges is performed by the CANARIE IT department and follows a documented approval process.

Different services have different levels of capabilities and administrators of those services use best practices to balance the targeted utility of a service and the protection/masking of identity information.

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

In the case of a localized identity breach, CANARIE will work to notify those impacted. If outside organizations need to report a breach to us, please contact cybersecurity@canarie.ca so we can assist with the local coordination.

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?

N/A