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: BC CANCER, PART OF THE PROVINCIAL HEALTH SERVICES AUTHORITY

1.2 Information below is accurate as of this date: 01/11/2024

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): Office of Research Administration

Email Address: itdirector@bccrc.ca

Telephone: 604-675-8193

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.

BCCRC, being a department of PHSA, follows the provincial regulations and privacy policies.

The PHSA policies can be found at http://www.phsa.ca/privacy which reference the BC Freedom of Information and Protection of Privacy Act (FIPPA) found at https://www.bclaws.gov.bc.ca/civix/document/id/complete/statreg/96165_01

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 for Privacy Policy URLs from PHSA and province of BC

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?

We will create a group access policy across our computer accounts to limit access to those who will be accessing eduroam. As many of our researchers already have access to eduroam via higher-ed affiliations (primarily SFU & UBC), this group access policy will be limited to FTE of BC Cancer Research without pre-existing affiliations.

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
Not applicable at this time	☐			

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.

All staff/researcher PII is stored by PHSA in their information systems. BCCRC does not have direct access to this information or the systems unless authorized by PHSA. Authorization is done via a request to PHSA with supervisor approval. Computer account information for BCCRC accounts is controlled by and limited to the BCCRC IT staff, with the exception of account information deemed public such as email address, phone number and visible via tools such as outlook. Most research data on the BCCRC systems is anonymized or de-identified. Research data containing PII is typically stored offsite on PHSA clinical storage systems. Research data (regardless of containing PII) is constrained to access controlled with Group Access Policies. Membership in a Group Access Policy is done via approval from both the employee supervisor and the data owner.

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.

Super-user privilege and access to elevated accounts is restricted to members of the systems team. Training must be completed before access is granted. Use of “sudo” is recommended over explicit use of the root password.

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

Depending on the scope of a compromise, a general notification to all computer accounts may be distributed via email informing the user committee of the scope and impact of the compromise. Data owner(s) of compromised information will be directly contacted. The data owner(s) will then notify affected parties as per the BC government FIPPA regulations. All media contact is done via BC Cancer or PHSA media services.

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?

None.