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: Calgary Catholic School District

1.2 Information below is accurate as of this date: 02/02/2022

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): Mike Meyer

Email Address: mike.meyer@cssd.ab.ca

Telephone: 403-500-2796

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.

CCSD is subject to the Alberta Freedom of Information and Protection of Privacy Act (the FOIP Act). CCSD is also committed to providing a website that respects your privacy while you visit us online. This privacy statement summarizes our privacy practices is in the process to be updated, but it will be located on our main website page www.cssd.ab.ca.

Here are the main links:

- Alberta's Freedom of Information and Privacy Protection Act (FOIP)
- FOIP page on CSSD's Website
- AP 180 Freedom of Information and Protection of Privacy (FOIP)

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.

- Alberta's Freedom of Information and Privacy Protection Act (FOIP)
- FOIP page on CSSD's Website
- AP 180 Freedom of Information and Protection of Privacy (FOIP)

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 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.

There is limitation for remote access to the the radius server and the Wireless System.

Only the individuals that need access to the information as part of maintaining the system will have access to the information. Depending on their role or job function, users will be granted specific access on the Radius Server and the wireless system

We also follow the principle of positive access only, meaning users have minimal privilege/access according to their job/role, and are granted access only as needed.

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.

Only the individuals that need access to the information as part of maintaining the system will have access to the information. Only the team that looks after the Radius and Wi-Fi equipment has access.

Actions with escalated permissions are coordinated through proper change management system, with appropriate authorization and escalation where needed.

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

Please consider our AP180 about the Freedom of Information and Protection of Privacy Act (the FOIP Act)

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?

We will appreciate to be notified about any incident that may impact CSSD data security, which may impact its availability, integrity or confidentiality.