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: 08/28/2020

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.

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): Association of Registrars of the Universities and Colleges of Canada (ARUCC) with support provided by Digitary

Email Address: tech@aruccnationalnetwork.ca/ caf@digitary.net

Telephone: 1 905 703 7485/ +1 250 744 0445

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.

ARUCC and it's service provider, Digitary, do not release any attribute information. ARUCC's service provider is an attribute consumer only.

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.

The specific privacy policy to be employed for use across the Canadian National Network is yet to be finalised but will be based on the privacy policy employed elsewhere and as shown here: https://www.aruccnationalnetwork.ca/privacy-policy and https://core.digitary.net/#/privacy

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?
ARUCC National Network	☐	• **user identifier** (student ID) • **person name** (givenName + sn) • **email address** • **IdP account expires flag** (optional)	For authentication (user identifier, person name, email address)	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.

ARUCC and its service provider, Digitary, consider security and privacy to be paramount. Operationally, ARUCC relies on Digitary to power and oversee the document issuance platform of the ARUCC National Network which uses CAF as a mechanism to support single sign for its members. On ARUCC's behalf, Digitary employs a hybrid model comprising a combination of experienced in-house Digitary resources supported by outsourced industry specialists. Digitary's senior management team, the highly experienced in-house Digitary team covers information security functions across the Digitary IT infrastructure, application development, and general operations, including for the ARUCC National Network document issuance platform. Digitary is supported by a third-party security governance and compliance partner, Security Centric, which provides outsourced Information Security Officer (ISO) expertise. Digitary is operationally supported by Data Privacy experts Sytorus, who have helped Digitary to prepare for, and maintain, continued GDPR compliance and other privacy regulations. AlertLogic provide 24/7 intrusion detection on

the ARUCC National Network IT infrastructure and their Security Operations Centre (SOC) provides remediation support to Digitary's infrastructure teams supporting the ARUCC National Network in the event of an incident.

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.

All actions are recorded in an audit trail within the Digitary applications on behalf of the ARUCC National Network. In addition, access to all underlying AWS systems is audited using AWS CloudTrail and CloudWatch services that log, monitor and alert responsible persons of any unusual patterns of activity. In addition, SumoLogic log analysis and reporting mechanisms are employed to ensure that incidents are easily auditable and collatable across the entiry Digitary infrastructure including the ARUCC National Network and anomalies are detected quickly and easily. AlertLogic 24/7 monitoring looks for intrusion detection patterns and high-risk detections are reviewed by AlertLogic's security team, with an escalation path to Digitary's support team for rapid remediation and subsequent notification to ARUCC and its Participants on the ARUCC National Network.

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

ARUCC is supported by Digitary's robust Incident and Breach Notification Policy that complies with GDPR as well as respective privacy and reporting legislation such as in Canada. When a personal data breach is likely to result in high risk to the rights and freedoms of natural persons, the data breach must be communicated to the data subject without undue delay, in a written, clear and legible format. The notification to the affected data subject should include, the nature of the personal data breach, the name and contact details of the Data Protection Officer and/or any other relevant point of contact, a description of the likely consequences of the personal data breach, a description of the measures taken or proposed to be taken to address the personal data breach (including measures to mitigate its possible adverse effects).

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.