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: QReserve Inc.

1.2 Information below is accurate as of this date: 01/28/2026

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): QReserve Support

> Email Address: hello@qreserve.com

> Telephone: 289-426-3217

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.

> https://get.qreserve.com/legal/privacy
> https://get.qreserve.com/legal/terms

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://get.qreserve.com/legal/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.

Canadian Access Federation – Trust Assertion Document (TAD)

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?
QReserve Platform	☐	• **user identifier** (eduPersonPrincipalName + eduPersonTargetedID) • **person name** (givenName + sn) • **email address**	For authentication (user identifier, person name, email address) and display purposes (name0	Partially. The person name will populate a public name field that others can see within their organization (e.g. who has booked a resource) if administrators enable this information to be shared. Administrators of a QReserve site will also have access to the email address of users.

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.

As a SOC 2 Type II audited organization (https://get.qreserve.com/security) our security and policy controls have undergone a rigorous third-party audit to ensure that information is stored, processed, and transferred securely in a fashion that meets the functional requirements of our services.

The human and technical controls in place for access to and use of attributes considered personally identifiable information (PII) include technical measures such as multi-factor authentication (MFA), role-based access control (RBAC), and access control lists (ACLs) to restrict access to sensitive systems, along with the use of secure protocols for server access. Data protection is enforced via encryption at rest, network firewalls, and automated vulnerability scanning in cloud environments. Furthermore, for development, cleansed backups are created where PII is anonymized and sensitive data is removed. Human and procedural controls involve mandatory documentation and formal approval from the system or data owner for all access requests and modifications. Personnel screening and training mandates background checks for employees with system access, and new hires must complete security awareness training and sign a confidentiality agreement. Access rights are regularly reviewed, and removal of access is completed promptly, within 24 hours of a role change or termination, and confirmed using termination checklists.

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.

Customers (e.g. universities and colleges) are responsible to assigning privileged access rights to trusted users and QReserve's role-based access controls (RBACs) are in place to ensure that PII is only shared to the level of consent of that university. For example, administrators can choose calendars to be completely anonymous or to display a user's name. Email addresses are only visible to privileged users.

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

In the event of a security or privacy incident, QReserve's Security Team Incident Response Plan is designed to quickly detect, assess, contain, and resolve the incident. A key activity outlined in this plan is the notification of relevant stakeholders, which explicitly includes customers, as well as senior management and legal entities, to be carried out as required to minimize impact.

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?

Click or tap here to enter text.