# 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: University of Prince Edward Island

## 1.2 Information below is accurate as of this date: 10/04/2023

## 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, to avoid responses going unanswered if personnel changes occur.

Department (or Contact Name): Dana Sanderson

Email Address: dsanderson@upei.ca

Telephone: 902- 566-0427

## 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://www.upei.ca/about-upei/policy**

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://files.upei.ca/policy/access_to_information_and_protection_of_personal_information_and_privacy_policy_govbrdgnl0017.pdf**

# 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?

Faculty, staff, students, and alumni of UPEI. Deans, directors, and senior management can approve exceptions

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 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):**<br>• timestamp of authentication requests and corresponding responses<br>• the outer EAP identity in the authentication request (User-Name attribute)<br>• the inner EAP identity (actual user identifier)<br>• the MAC address of the connecting client (Calling-Station-Id attribute)<br>• type of authentication response (i.e. Accept or Reject). | For authentication purposes | No |
| **Example**<br>**{FIM Service 1}** | ☐ | • **user identifier** (eduPersonPrincipalName + eduPersonTargetedID)<br>• **person name** (givenName + sn)<br>• **email address**<br>• **affiliation** (eduPersonScopedAffiliation) | For authentication (user identifier, person name, email address) and authorization (affiliation) purposes | No |
| **{FIM Service 2}** | ☐ | | | |

***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.

**Human Controls:**

1. **Access Policies and Procedures:**

    - **Role-Based Access Control (RBAC):** Access rights are assigned based on job roles and responsibilities. Employees are granted permissions necessary for their specific roles.
    - **Access Approval:** Access requests are approved by designated personnel and are based on a need-to-know basis.
    - **Data Ownership:** Specific individuals or departments are designated as data owners. They are responsible for overseeing the use and access to PII.

2. **Training and Awareness:**

    - **Employee Training:** Regular training sessions educate employees about the importance of data privacy, the company's data protection policies, and the proper handling of PII.
    - **Security Awareness Programs:** Employees are regularly updated about the latest security threats, phishing techniques, and social engineering attempts.

3. **Incident Response:**

    - **Reporting Procedures:** Clear procedures are in place for reporting any suspected data breaches or unauthorized access to PII.
    - **Investigation and Remediation:** A response team investigates reported incidents promptly, takes necessary actions, and implements measures to prevent future occurrences.

**Technical Controls:**

1. **Authentication:**

    - **Multi-Factor Authentication (MFA):** Users are required to provide multiple forms of verification before gaining access, enhancing security significantly.
    - **Strong Password Policies:** Enforced use of passwords that are regularly updated.

2. **Encryption:**

    - **Data Encryption:** PII stored in databases or transmitted over networks is encrypted, ensuring that even if unauthorized access occurs, the data remains unreadable.
    - **End-to-End Encryption:** Messages and files containing PII are encrypted from the sender's end and can only be decrypted by the intended recipient.

3. **Access Control:**

    - **Firewalls and Intrusion Detection Systems (IDS):** These are in place to monitor network traffic and prevent unauthorized access.
    - **Data Loss Prevention (DLP) Tools:** DLP tools monitor and control data transfer over the network to prevent unauthorized sharing of sensitive information.

4. **Audit and Monitoring:**

    - **Audit Trails:** Comprehensive logs record who accessed what data and when. Regular audits of these logs help in detecting and mitigating any unauthorized access.
    - **Real-time Monitoring:** Automated systems monitor network and system activities in real-time, raising alerts for any suspicious behavior.

5. **Secure Development Practices:**

    - **Secure Coding:** Developers follow best practices for secure coding to eliminate vulnerabilities that could be exploited for unauthorized access.
    - **Regular Security Assessments:** Periodic security assessments, including penetration testing and code reviews, identify and address potential vulnerabilities.

6. **Data Masking and Anonymization:**

    - **Data Masking:** Test environments use masked data, ensuring that real PII is not exposed in non-production environments.
    - **Anonymization:** Unnecessary identifiers are removed or altered in datasets, reducing the risk associated with handling sensitive information.

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.

**Human Controls:**

1. **Access Governance:**

    - **Authorization Protocols:** Strict protocols define who can grant access to privileged accounts, ensuring that only authorized personnel can assign such privileges.
    - **Regular Access Reviews:** Periodic reviews are conducted to validate the necessity of super-user privileges. Access is revoked immediately for individuals who no longer require such access.

2. **Segregation of Duties (SoD):**

    - **Role Separation:** Responsibilities are clearly segregated to prevent conflicts of interest. No single person should have complete control over sensitive operations involving PII.
    - **Approval Workflow:** Access requests undergo an approval process involving multiple stakeholders, minimizing the risk of unauthorized access.

3. **Training and Awareness:**

    - **Specialized Training:** Employees with super-user privileges receive specialized training about the importance of data security, the potential risks, and the ethical use of their access.
    - **Regular Awareness Programs:** Continuous education programs keep privileged users updated about the latest security threats and attack vectors.

4. **Incident Response:**

    - **Escalation Procedures:** Clearly defined procedures outline how and when incidents involving privileged accounts are escalated to higher management for immediate action.
    - **Post-Incident Analysis:** After an incident, a thorough analysis is conducted to understand the cause and implement measures to prevent similar occurrences.

**Technical Controls:**

1. **Access Management:**

    - **Just-In-Time Privileges:** Privileged access is granted only for the necessary duration and specific tasks, reducing the window of vulnerability.
    - **Privileged Access Management (PAM) Tools:** PAM solutions manage, monitor, and audit activities of privileged accounts. They enforce strong authentication and authorization mechanisms.

2. **Multi-Factor Authentication (MFA):**

    - **Mandatory MFA:** MFA is mandatory for all privileged accounts, adding an extra layer of security even if credentials are compromised.

3. **Audit and Monitoring:**

    - **Real-Time Monitoring:** Automated systems continuously monitor activities of privileged accounts in real-time, generating alerts for any suspicious behavior.
    - **Audit Trails:** Detailed logs capture every action taken by privileged users. These logs are regularly reviewed and audited for any anomalies.

4. **Encryption and Tokenization:**

    - **Data Encryption:** PII is encrypted both at rest and in transit, ensuring that even if accessed, the data remains unreadable.
    - **Tokenization:** PII accessed by privileged users is replaced with tokens, preventing direct access to sensitive information.

5. **Regular Vulnerability Assessments:**

    - **Penetration Testing:** Regular penetration testing identifies vulnerabilities in systems and applications, ensuring that potential avenues for unauthorized access are promptly closed.

6. **Automated Account Lifecycle Management:**

    - **Automated Provisioning and Deprovisioning:** Privileged accounts are automatically provisioned when needed and deactivated promptly when no longer required, reducing the window of vulnerability.

7. **Regular Security Updates and Patch Management:**

    - **Timely Patching:** Systems and applications are regularly updated with the latest security patches to fix vulnerabilities that could be exploited to gain unauthorized access.

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

**Assessment:**

- **Determine the Scope:** Identify what type of information was compromised, how many individuals are affected, and the potential impact of the breach.

**Legal and Regulatory Compliance:**

- **Understand Legal Requirements:** Research and understand the data breach notification laws applicable to your jurisdiction. Different regions have different regulations regarding the timeframe and method of notification.
- **Comply with Regulations:** Ensure that your notification process complies with the legal obligations in the affected areas.

**Communication Strategy:**

- **Develop a Communication Plan:** Create a clear and concise communication plan detailing how and when affected individuals will be notified.
- **Establish a Contact Point:** Designate a specific contact point (such as a dedicated email address or phone number) for individuals to reach out for more information or assistance.

**Notification Process:**

- **Direct Notification:** Notify affected individuals directly through means such as email, phone calls, or physical mail if contact information is available.
- **Clear and Simple Language:** Use language that is easy to understand, explaining the nature of the breach, the type of information compromised, and the steps individuals can take to protect themselves.
- **Offer Assistance:** Provide resources and support, such as credit monitoring services or helplines, to help individuals navigate the potential consequences of the breach.
- **Timing:** Notify affected individuals as soon as possible after discovering the breach, following legal guidelines.

**Public Communication:**

- **Prepare a Public Statement:** Be prepared to issue a public statement, especially if the breach is widespread or if there is a significant impact on a large number of individuals.
- **Transparency:** Be transparent about the nature of the breach, the steps being taken to address it, and the measures put in place to prevent future breaches.

**Internal Communication:**

- **Internal Notification:** Inform internal stakeholders, including employees, about the breach, the response plan, and their roles in the notification process.

**Follow-up and Support:**

- **Follow-up Communication:** Keep affected individuals informed about the progress of the investigation, actions taken to prevent future breaches, and any additional steps they need to take.
- **Support Services:** Offer ongoing support services, such as identity theft protection, to affected individuals for an extended period after the breach.

**Learn and Improve:**

- **Post-Incident Analysis:** Conduct a thorough analysis of the breach incident. Understand what happened, why it happened, and how a similar breach can be prevented in the future.
- **Update Security Measures:** Strengthen security measures and protocols based on the lessons learned from the breach to prevent similar incidents.

## 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?

Not currently.