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: myLaminin Corp.

1.2 Information below is accurate as of this date: 10/17/2023

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, in order to avoid responses going unanswered if personnel changes occur.

Contact Name: Ash Bassili

Email Address: ashbassili@mylaminin.net

Telephone: (443)824-3081

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.

The myL Information Security policy has been established to outline techniques and procedures the company will use to keep information on myLaminin systems safe from external and internal threats. This policy can be made available on request to appropriate parties.

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://www.mylaminin.net/privacy-policy

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?
myLaminin RDS (Research Data Sharing)	Yes	• **user identifier** (eduPersonPrincipalName + eduPersonTargetedID) • **person name** (givenName + sn) • **email address** • **affiliation** (eduPersonScopedAffiliation)	For authentication (user identifier, person name, email address) and authorization (affiliation) purposes	No

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.

Encryption at rest is done for the MongoDB database on Atlas. Encryption keys are managed by myLaminin through AWS KMS. Limited access is allowed to database clusters via individual and group access permissions.

All accounts with access to MongoDB Atlas or AWS are tracked by Vanta and must be assigned to an appropriate owner in the myLaminin team.

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.

Two factor authentication is required on AWS IAM and MongoDB Atlas accounts. AWS passwords must follow our password policy and are to be updated every 90 days. Vanta compliance software is used to track access of IAM (AWS) users and flag inactive (90+ days) accounts to be disabled. Vanta tracks use of the root AWS account and gives an alert if used.

All accounts with access to MongoDB Atlas or AWS are tracked by Vanta and must be assigned to an appropriate owner in the myLaminin team.

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

The following information is available in the myLaminin Information Security policy which can be made available to appropriate parties on request.

"If it is determined during the Analysis Phase that a Security or Privacy Incident has occurred that constitutes a Data Breach, with notification obligations based on applicable legislation, regulation, or similar jurisdictional requirements, then notification of such Data Breach shall be handled by the SIRT and provided to the impacted parties by email, telephone, or other appropriate means agreed upon by myLaminin and the applicable party, or by means stipulated under applicable data protection or privacy law, within twenty-four (24) hours upon myLaminin SIRT becoming aware of the Data Breach. Additional activities noted under '5.6. Post-Incident Activities' may also be initiated under the direction of the SIRT.

When determining the parties to be notified of such Data Breach, the SIRT will analyze the impacted parties (customers, Data Controllers, PII Principals, Third Parties, government bodies) and determine the applicable relationships between the parties (controller, joint controller, processor and/or subprocessor), the applicable contractual obligations, and the applicable laws, regulations, or like jurisdictional requirements. Based on this analysis, myLaminin will notify applicable parties as follows based on myLaminin role as a:

- Controller – Notify the applicable government body, and if the Data Breach is likely to result in a high risk to the rights and freedoms of PII Principals, notify the PII Principals.
- Joint Controller – Notify the other controller and the applicable government body, and if the Data Breach is likely to result in a high risk to the rights and freedoms of PII Principals, notify the PII Principals.
- Processor – Notify the controller.
- Sub-processor – Notify the processor, and where appropriate and feasible, the controller."

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?

N/A