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: OCLC, Inc.

1.2 Information below is accurate as of this date: 08/01/2019

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): The management of the EIDM team

Email Address: idm-strategic@oclc.org

Telephone: 1 (800) 848-5878 and ask for the Director of Shared Services

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.

We would release attribute information under contractual agreement with the library that holds the principal, when they request release. Generally, this would be data asserted by the library and not by the Identity Provider.

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.

OCLC has a privacy notice (https://policies.oclc.org/en/privacy/privacy-statement.html), but it does not apply to all of OCLC's products. See the "Hosted Products and Services" section of the notice. It is typically a library's responsibility to provide a privacy notice to its staff and patrons. Depending on the OCLC products involved, there may be a capability for the library to display their notice or a link to their notice. Release notes describe when functionality is available and what steps to take to display a notice.

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?
WMS Management Systems (Library automation software)	☐	**We require an identifier that the library can provide during the provisioning of the user prior to authentication. This single identifier is expected to be unique for users asserted by the IDP and is associated with the IDP's entity ID. This is similar to but not necessarily identical to:** • **user identifier** (eduPersonPrincipalName + eduPersonTargetedID) • **affiliation** (eduPersonScopedAffiliation)	Used to correlate the authenticated user with the authorized users provisioned by the library	This identifier is not shared with others.

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.

OCLC employees are assigned an OCLC account for the purposes of performing their respective jobs in support of our customers and products/services provided. The assignment of the account is managed through our account management process which includes the necessary approvals and review throughout the lifecycle of the account and for the specific authorizations assigned to each employee. Access to personally identifiable information is tightly controlled by both limiting who has authorization to production

data and the handling of production data. It is OCLC's policy that production data resides only in the production environments.

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.

OCLC privileged accounts are also managed through our account management process with additional approvals, reviews and limiting these accounts to only those individual who need privileged accounts.

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

Whether individuals affected by an incident are notified is a fact-specific determination. Notification laws vary. OCLC would notify affected individuals if OCLC were required to do so under applicable laws. OCLC might choose to notify affected individuals when not required under applicable laws.

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.