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: Book Oven, Inc. dba Pressbooks

1.2 Information below is accurate as of this date: 03/10/2020

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 to avoid responses going unanswered if personnel changes occur.

Department (or Contact Name): Pressbooks Support Team (Steel Wagstaff)
Email Address: premiumsupport [at] pressbooks.com (steel [at] pressbooks.com)
Telephone: N/A

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.

As a service provider, we only consume attribute information from institutions in order to provision access to our authoring platform. We do not release or share this attribute information with other entities.

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://pressbooks.com/wp-content/uploads/2019/05/2019-05-01-Privacy-Policy-PressbooksEDU.pdf

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?
Pressbooks SAML SSO	☐	• **uid** (urn:oid:0.9.2342.19200300.100.1.1, samAccountName, or equivalent) • **mail** (urn:oid:0.9.2342.19200300.100.1.3, email-address, or equivalent) If no value is available we fall back to uid@127.0.0.1 https://github.com/pressbooks/pressbooks-saml-sso/blob/f270ed71f8e5ccadf2127589533e5315fefa5e1c/inc/class-saml.php#L243-L259 **Optional:** eduPersonPrincipalName (urn:oid:1.3.6.1.4.1.5923.1.1.1.6, or equivalent) Upon the first launch for a given user, if mail cannot match an existing person, and this value is present, we'll try to use it. https://github.com/pressbooks/pressbooks-saml-sso/blob/f270ed71f8e5ccadf2127589533e5315fefa5e1c/inc/class-saml.php#L785-L795	Authentication purposes only	No
Pressbooks CAS SSO	☐	• **user identifier** [The user's NetID, as returned by phpCAS::getUser(). https://github.com/pressbooks/pressbooks-cas-sso/blob/0ce94b6b3d70cc71435f166737688c94699bdad3/inc/class-cas.php#L220]	Authentication purposes only	No
Presbooks OIDC SSO	☐	• **user identifier** (eduPersonTargetedID) • **affiliation** (eduPersonScopedAffiliation)	Authentication & authorization purposes only	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.

We do not store personally identifiable 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.

We do not store personally identifiable information.

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

We do not store personally identifiable information.

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?

Pressbooks maintains open source repositories & public documentation for our bilateral SSO tools.

Pressbooks SSO CAS

repo: https://github.com/pressbooks/pressbooks-cas-sso
docs: https://docs.pressbooks.org/integrations/cas-sso/

Pressbooks SSO SAML

repo: https://github.com/pressbooks/pressbooks-saml-sso
docs: https://docs.pressbooks.org/integrations/saml-sso/

We also maintain a tool that allows a Pressbooks network to provide multilateral SSO (a single network interacting with multiple IdPs) using a wayfinder and OpenID Connect. We make use of OpenAthens Keystone to provide some of these services.