

Canadian Access Federation: Trust Assertion Document (TAD)

1. Purpose

A fundamental requirement of Participants in the Canadian Access Federation is that they assert authoritative and accurate identity attributes to resources being accessed, 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 below.

1.1 Canadian Access Federation Requirement

Currently, the 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 should make 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 would include how supported identity attributes are defined and how attributes are consumed by services.

1.2 Publication

Your responses to these questions must be:

1. submitted to CANARIE to be posted on the CANARIE website; and
2. posted in a readily accessible place on your web site.

You must maintain an up-to-date Trust Assertion Document.

2. Canadian Access Federation Participant Information

2.1.1. Organization name: *London Health Sciences Centre*

2.1.2. Information below is accurate as of this date: *September 24, 2014*

2.2 Identity Management and/or Privacy information

2.2.1. Where can other Canadian Access Federation Participants find additional information about your identity management practices and/or privacy policy regarding personal information?

Privacy Office for London Health Sciences Center:

Telephone: (519) 685-8500, Extension 32996

E-mail: Privacy@lhsc.on.ca

URL: http://www.lhsc.on.ca/Patients_Families_Visitors/Privacy/Privacy_Policy.htm

2.3 Contact information

2.3.1. Please list person(s) or office who can answer questions about the Participant's identity management system or resource access management policy or practice.

Name:	David Schned
Title or role:	Director, Information Technology Services
Email address:	David.Schned@lhsc.on.ca
Telephone:	519-685-8500 x35221

3. Identity Provider Information

Two criteria for trustworthy attribute assertions by Identity Providers are: (1) that the identity management system be accountable to the organization's executive or business management, and (2) the system for issuing end-user credentials (e.g., userids/passwords, authentication tokens, etc.) has in place appropriate risk management measures (e.g. security practices, change management controls, audit trails, accountability, etc.).

3.1 Community

3.1.1. As an Identity Provider, how do you define the set of people who are eligible to receive an electronic identity? If exceptions to this definition are allowed, who must approve such an exception?

All employees and affiliates are technically eligible if there is a role specific requirement for them to have access.

Affiliates – Individuals who are not employed by the organization but perform specific tasks at or for the organization, including:

- *Credentialed Professional Staff with a hospital appointment (e.g. physicians, midwives, dentists)*
- *Students*
- *Volunteers*
- *Contractors or contracted workers who may be members of a third party contract or under direct contract with the organization.*
Individuals working at the organization but funded through an external source.

3.1.2. All of the above go through some sort of approval, either by Human Resources, the individuals leader, Medical Affairs, Student Affairs, Lawson Research, Health Records, or by an internal process where a leader and periodically other such as Privacy, IT Security or Health Records will have to approve access or elevated access. What subset of persons registered in your identity management system would you identify as a "Participant" in SAML identity assertions to **CAF** Service Providers?

Students, Credentialed Professional Staff and employees.

3.2 Electronic Identity Credentials

3.2.1. Please describe, in general terms, the administrative process used to establish an electronic identity that results in a record for that person being created in your electronic identity database? Please identify the office(s) of record for this purpose.

All employees and affiliates (e.g. physicians, mid-wives, dentists) are automatically entitled to receive an electronic identity on some of our systems e.g. network and email. Elevated access or access to additional systems is currently a manual process. Requests for

access, or elevation of access, is facilitated via a web-based form. Only authorized requesters have access to this form, as it is protected by network authentication and group membership.

Student access are requested by our Student Affairs department or Lawson Research. They do the vetting and approval prior to sending to ITS. Third-party access requests have to either come in through the request form and are approved by the responsible leader.

- 3.2.2. What authentication technologies are used for your electronic identity credentials (e.g., Kerberos, userID/password, PKI, ...) that are relevant to Canadian Access Federation activities? If more than one type of electronic credential is issued, how is it determined who receives which type? If multiple credentials are linked, how is this managed (e.g., anyone with a Kerberos credential also can acquire a PKI token) and audited?

UserID and password

- 3.2.3. If your electronic identity credentials require the use of a secret password or PIN, and there are circumstances in which that secret would be transmitted across a network without being protected by encryption (e.g., “clear text passwords” are used when accessing campus services), please identify who in your organization can discuss with any other Participant concerns that this might raise for them:

No known circumstances. Use primary contact above if any questions

- 3.2.4. If you support a “single sign-on” (SSO) or similar campus-wide system to allow a single user authentication action to serve multiple applications, and you will make use of this to authenticate people for **CAF** Service Providers, please describe the key security aspects of your SSO system including whether session timeouts are enforced by the system, whether user-initiated session termination is supported, and how use with “public access sites” is protected.

We do not use SSO at this time.

- 3.2.5. Are your primary electronic identifiers for people, such as “NetID,” eduPersonPrincipalName, or eduPersonTargetedID considered to be unique for all time to the individual to whom they are assigned? If not, what is your policy for re-assignment and what is the interval between such reuse?

Yes, they are unique and only used once.

3.3 Electronic Identity Database

- 3.3.1. How is information in your electronic identity database acquired and updated? Are specific offices designated by your administration to perform this function? Are individuals allowed to update their own information on-line?

Direct feed from our HR system and manual updating by our IT Governance team.

3.3.2. What information in this database is considered “public information” and would be provided to any interested party?

None.

3.4 Uses of Your Electronic Identity Credential System

3.4.1. Please identify typical classes of applications for which your electronic identity credentials are used within your own organization.

Network authentication, e-mail, clinical system access, HR and Financials...pretty well all systems access require authentication or network group membership.

3.5 Attribute Assertions

Attributes are the information data elements in an attribute assertion you might make to another Canadian Access Federation Participant concerning the identity of a person in your identity management system.

3.5.1. Please describe the reliability of your identity provider attribute assertions?

Reliable

3.5.2. Would you consider your attribute assertions to be reliable enough to:

a) control access to on-line information databases licensed to your organization?

Yes

b) be used to purchase goods or services for your organization?

Yes

c) enable access to personal information such as student record information?

Yes

3.6 Privacy Policy

Canadian Access Federation Participants must respect the legal and organizational privacy constraints on attribute information provided by other Participants and use it only for its intended purposes.

3.6.1. What restrictions do you place on the use of attribute information that you might provide to other Canadian Access Federation participants?

We would expect other CAF participants to treat the information as confidential and appropriately protect and not disclose that information to others. If there were disclosures

required, that we approve and in the event of an accidental disclosure, that we are notified immediately.

3.6.2. What policies govern the use of attribute information that you might release to other Canadian Access Federation participants?

Privacy, Confidentiality and Security of Confidential Information policies.

3.6.3. Please provide your privacy policy URL.

http://www.lhsc.on.ca/Patients_Families_Visitors/Privacy/Privacy_Policy.htm

4. Service Provider Information

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.

4.1 Attributes

4.1.1. What attribute information about an individual do you require in order to manage access to resources you make available to other Participants? Describe separately for each service application that you offer to CAF participants.

User ID and Password

4.1.2. What use do you make of attribute information that you receive in addition to basic access control decisions?

None

4.1.3. Do you use attributes to provide a persistent user experience across multiple sessions?

No

4.1.4. Do you aggregate session access records or record specific information accessed based on attribute information.

No

4.1.5. Do you make attribute information available to other services you provide or to partner organizations?

No

4.2 Technical Controls

4.2.1. What human and technical controls are in place on access to and use of attribute information that might refer to only one specific person (i.e., personally identifiable information)? For example, is this information encrypted for storage in your system?

Access to the directory service is controlled

4.2.2. Describe the human and technical controls that are in place on the management of super-user and other privileged accounts that might have the authority to grant access to personally identifiable information?

Privileged accounts must be authorized by the Manager, Technology Solutions, ITS. Privileged accounts are assigned to individuals and are used only in the performance of the relevant tasks.

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

Upon discovery the organization's Privacy office will contact the impacted individuals to inform them of the nature of the compromise and discuss appropriate follow-up and remediation actions.

5. Other Information

5.1 Technical Standards, Versions and Interoperability

5.1.1. Identify the SAML products you are using. If you are using the open source Internet2 Shibboleth products identify the release that you are using.

None

5.1.2. What operating systems are the implementations on?

N/A

5.1.3. What versions of the SAML protocol (1.1 or 2.0) do you support in your implementations.

SAML 1.1 – *Not supported*

SAML 2.0 – *Not supported*

5.2 Other Considerations

5.2.1. Are there any other considerations or information that you wish to make known to other Canadian Access Federation Participants with whom you might interoperate? For example, are there concerns about the use of clear text passwords or responsibilities in case of a security breach involving identity information you may have provided?

No