Participant Name: Compute Canada

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: Compute Canada

2.1.2. Information below is accurate as of this date: June 20, 2016

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 and data protection policy (public Web site):

https://www.computecanada.ca/wp-content/uploads/2016/02/PrivacyPolicy_en_V1.0.pdf

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:	Dr. Jonathan Ferland
Title or role:	Director of Information Security
Email address:	jonathan.ferland@computecanada.ca
Telephone:	514.343.6111 ext/poste 8852

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 tokes, 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?

Anyone with a current (non-expired) role in the Compute Canada Database (CCDB), which is the directory of all users, principal investigators, and team members (i.e., consortium staff). Roles are given per the Compute Canada Access Policy, online at https://www.computecanada.ca/research-portal/accessing-resources/access-policy/

3.1.2. What subset of persons registered in your identity management system would you identify as a "Participant" in SAML identity assertions to **CAF** Service Providers?

Same as 3.1.1.

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.

Individuals apply for a username and associated role(s) in CCDB (https://ccdb.computecanada.ca). Local support personnel at that individual's institution validate the identity and affiliation. If no local support personnel are available, regional personnel identify a staff member to validate the identity. All records are maintained in CCDB.

In the future, it is intended that institutional affiliation and roles will instead be validated through CAF, via released attributes from institutions, as described below.

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+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:

Transmission of clear text passwords is not permitted, per the Security Council's "Directive on Password Management," which also prohibits storage of passwords as cleartext, and forbids unencrypted transmission of passwords. 2.3.1 identifies the role for discussion of any concerns.

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.

SSO is not yet implemented, but is planned for the future. These details will be updated in the TAD, when known.

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?

They are to be unique for all time.

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?

Acquisition and updates are by users. Validation of identity is per 3.2.1, and is renewed annually.

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

Per the privacy policy, "public information" is defined as "any Information that is neither Personal Information nor Sensitive Information." All information stored in CCDB is considered either Personal information or Sensitive information, unless defined otherwise.

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.

Advanced research computing applications, primarily accessed either via direct command-line login (typically via ssh), or through some sort of Web portal via https.

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?

See 3.2.1. Compute Canada is not the primary identity provider for most users, and instead relies on the home institutions to provide identity information. Compute Canada validates the information, and then renews annually.

Compute Canada is the primary identity provider only for its own personnel, and others for whom no other identity provider is available. In those cases, Compute Canada will validate, and maintain currency, of identity information for such individuals.

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, for individuals for which Compute Canada is the primary identity provider

c) enable access to personal information such as student record information?
Yes, for individuals for which Compute Canada is the primary identity provider

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?

All use must be consistent with Compute Canada’s privacy policy. We anticipate having multilateral agreements with CAF members for attribute sharing, but are not yet party to such agreements. Therefore, disclosure to other CAF participants is limited to public information, per section 3.3.2.

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

Policies mentioned in section 2.2.1.

3.6.3. Please provide your privacy policy URL.

https://www.computecanada.ca/wp-content/uploads/2016/02/PrivacyPolicy_en_V1.0.pdf

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.

Compute Canada intends to develop SSO based on individual's institutional affiliation and status.

The three current/planned Services are:

1. Compute Canada Database: https://ccdb.computecanada.ca
2. Compute Canada Globus Portal: https://computecanada.ca/en/globus-portal
3. CCCloud: https://www.computecanada.ca/research-portal/national-services/compute-canada-cloud/

All Compute Canada Services will utilize the Research & Scholarship (R&S) Entity Category (https://refeds.org/category/research-and-scholarship/), which makes use of the following attribute bundle:

REQUIRED:

- personal identifiers: mail, displayName OR (givenName AND sn), and eduPersonPrincipalName

DESIRED:

- pseudonymous identifier: eduPersonTargetedID
- affiliation: eduPersonScopedAffiliation

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

Institutional affiliation and type (i.e., faculty, student, staff).

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

Yes, that is the intent.

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

Yes. Service logs are maintained, for access and activity. In addition, some research platforms and portals may provide Web-based access to resources, for which session access records may be used to provide a consistent user experience. Finally, the SAML attributes mentioned above will persist for their defined lifetime.

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

Compute Canada intends to share eduPerson and/or similar information with CAF members. Research platforms and portals hosted within Compute Canada may make use of such information, or become party to the forthcoming SSO environment. Additional attributes may be considered for sharing when needed to verify identities (i.e., affiliations/roles such as “faculty” or “student”).

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?

Compute Canada’s internal database (CCDB) includes PII. The database is protected through normal system access controls (i.e., authenticated access only by authorized systems personnel and programmers), and is backed up hourly. Data and backups are not currently encrypted, other than passwords, which are stored via a one-way hash.

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?

Compute Canada’s security program is under development. Currently, the SHARCNET consortium, led by the University of Western Ontario, hosts, secures, and provides access control to the CCDB’s underlying computational system, including database, backups, software, etc.

Within the CCDB, which is a custom Web/database application, there are different services and different levels of access control. There are a small number of managers (i.e., super-users within the application) who can grant privileges.

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

Currently, Compute Canada’s incident response relies on the hosting institutions to secure and monitor systems. Over time, systems will move to a more centrally managed and monitored environment, although still hosted at member institutions. If a data breach occurred, Compute Canada would first identify the institution(s) where the breach occurred, and then determine the institutions from which PII or other information was compromised. Compute Canada would then work with those institutions on mitigation and response. Most Compute Canada members are universities, and any such actions would be in close cooperation with the campus CIO/CTO and cognizant security office. Compute Canada is currently working with the Canada Foundation for Innovation to develop a security program that makes the different roles, responsibilities, and expectations more explicit.

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.

shibboleth-2.5.4-3.1 and later

5.1.2. What operating systems are the implementations on?

See section 5.1.1. Primarily RHEL/derivatives and Ubuntu**.**

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

SAML 1.1: not in production, may be offered in the future if needed for backward compatibility.

SAML 2.0: Planned for the future

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?

It is anticipated that Compute Canada will be the primary identity provider for a relatively small number of users (on the order of 100 or fewer), and will mainly rely on existing CAF members for asserting the identity, affiliation, and role/type of users who are seeking access to Compute Canada resources.

There are over 10,000 users from Canadian institutions, mainly universities, colleges and research institutions. This number is growing over time, and user status changes over time, including loss of eligibility for access to resources when there is no appropriate affiliation.

It is hoped that SSO will be developed, in which campus-based authentication will give users ease-of-use for access to resources. Compute Canada will provide authentication and identity management services when it is the primary identity provider for a user, and can offer those services when coordination with the home institution is not available or has not yet occurred.