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: *Trent University*

2.1.2. Information below is accurate as of this date: *April 1, 2013*

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?

http://www.trentu.ca/secretariat/access.php

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: *Robert Ruggiero*

Title or role: *Network Systems Integration Specialist*

Email address: *robertruggiero@trentu.ca*

Telephone: *705-748-1011 x6041*

Name: *Andre Bell*

Title or role: *Manager, Digital Service Delivery*

Email address: *andrewbell@trentu.ca*

Telephone: *705-748-1011 x7755*

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?

Faculty, staff, applicants, students, alumni, retirees, professors emeritus, sponsored guests.

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?

Faculty, staff, students, professors emeritus.

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.

Creation of an applicant record in the SIS automatically creates a corresponding network ID. The Registrar's Office maintains these records.

Creation of a staff record in the SIS system automatically creates a corresponding network ID. The Research Office or Human Resources maintains these records.

Guest accounts may be created directly in the network directory by IT staff.

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?

User ID 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:

Although all IT managed systems require that passwords be encrypted, there are no technical measures in place that would prevent other campus services from using plain text passwords. Concerns may be addressed to andrewbell@trentu.ca.

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 use Novell Access Manager for campus SSO. NAM will support authentication for our Shibboleth based CAF identity-provider. The default NAM SSO timeout is 60 minutes. Users may also initiate an SSO sign-out by clicking the "Logout" icon from the MyTrent portal menu bar.

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?

Dormant network user IDs are purged after 24 months of inactivity and may be subsequently reissued. The master ID number in the SIS system of record is never purged or reused.

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?

Student information is initially provided by OUAC and may be updated by the Registrar's Office. Staff information is gathered during the hiring process and may be updated by request to the IT department. No self-serve updates are permitted.

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

For students: none.

For staff: name, email, title, department, office location, phone number.

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.

Campus wireless LAN access, student residence network access, and all IT managed network applications with the exception of the SIS/ERP system. These credentials are also used for federated applications such as Google Apps.

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. Department affiliation changes may lag by as much as one monthly payroll cycle, but these are not used to assign role based permissions.

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?

Participants must comply with the policies set out in section 3.6.2 of this document, as well as any local policies governing privacy in their institution and jurisdiction.

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

Ontario Freedom of Information and Protection of Privacy Act (FIPPA)

Trent University Policy on the Protection of Personal Information

3.6.3. Please provide your privacy policy URL.

http://www.trentu.ca/administration/pdfs/PrivacyProtectionofPersonalInformation.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.

EDUROAM: No attributes, successful authentication only.

No other applications are currently offered.

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

N/A

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

N/A

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

RADIUS accounting records are stored with user IDs

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 personally identifiable information is governed by our privacy policy, and enforced by strict role based access controls in our systems of record.

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?

Root level access to the identity management system is required to change attribute ACLs. Only designated system administrators have sufficient access to elevate themselves to root level on this system, and direct root logins only permitted directly from the machine console, which requires an additional level of authentication to access.

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

The Privacy Office is responsible for assessing any compromise of personally identifiable information, and will notify affected individuals either in writing or by telephone as the situation merits.

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.

Novell (NetIQ) Access Manager 3.1.4

5.1.2. What operating systems are the implementations on?

SUSE Enterprise Linux

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

SAML 1.1 and 2.0

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?

N/A