**Participant Name: St. Thomas University**

# 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: **St. Thomas University**

2.1.2. Information below is accurate as of this date: **1 January, 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?

**St. Thomas University is subject to the Right to Information and Protection of Privacy Act of the Province of New Brunswick.**

## 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: **Dan Hurley**

Title or role: **ITS Director**

Email address: **itsdirector@stu.ca**

Telephone: **506-452-0484**

# 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?

**Employees of the University and registered students become eligible when they are hired or start taking courses. Certain retired staff and most retired faculty retain their identity upon leaving. Visiting scholars, contractors etc. may be granted an identity upon request from HR or a department. Visiting Scholars and contractors would lose their identity upon completion of their engagement with St. Thomas. Student identities are retained for a short period after courses are complete so that students completing research etc. retain access to University services (the length of this period is under review.)**

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?

**Employees (faculty and staff), some retirees, current students, possibly occasional contractors and visiting scholars.**

## 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.

**Employees – Human Resources requests the creation of an identity and ITS creates the identities (we are currently in the process of providing tools to HR so that they can do this themselves)**

**Students – Student identities are created by a scripted process, which refers to our Student Information System (Ellucian Colleague.) The registrar's office is the owner of that data, but ITS creates the identities.**

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:

**None of our systems transmit passwords in clear text**

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 are not currently using any SSO**

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?

**Identifiers are unique (we do not recycle)**

## 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?

**ITS Staff creates and manages the information in the identity database (MS Active Directory). We hope to delegate some of this attribute management to HR for employee identities in the future. Student identities are largely created through a scripted process. Users can change their own passwords via a web tool.**

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

**ITS would not disclose this information. Requests for such information would be directed to the Registrar's Office or Human Resources. HR does publish a phone directory, but this is (currently) not connected to the Identity Database.**

## 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 access, wireless network access, library access, Learning Management System.**

## 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?

**Attribute data originates from the SIS or HR and is centrally managed in Active Directory. The reliability should be high.**

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?

**Information that we pass to CAF and other participants should be used solely for authentication to eduroam. We would expect that the minimum information required is requested, that the information is managed in a secure way and deleted immediately once it has been used. We acknowledge that certain data will be retained in logs for six months as per the TERENA agreement.**

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

**Right to Information and Protection of Privacy Act of the Province of New Brunswick**

3.6.3. Please provide your privacy policy URL.

**Information on the Right to Information and Protection of Privacy Act of the Province of New Brunswick. may be found at http://www2.gnb.ca/content/gnb/en/services/services_renderer.200949.html.html. Information on St. Thomas University's policies for faculty and staff may be found at http://w3.stu.ca/stu/administrative/hr/policies/default.aspx and students may be**

**found at http://w3.stu.ca/stu/currentstudents/policies/default.aspx. The university will be reviewing its various privacy policies in light of the provincial legislation.**

# 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.

**We only offer eduroam as a CAF service – A user would need to enter userID and password to connect to eduraom and we would pass that along to CAF. We would only retain such information as ends up in radius logs – specifically we would under no circumstances retain passwords, password hashs or encrypted passwords.**

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

**Information is logged by RADIUS server for six months.**

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?

**Attribute information exists in an MS Active Directory directory. Access to this directory is controlled an only available to a few people. We are looking at delegating some attribute management to HR, but this will only be done once we are**

**confident that the tools available allow them to only make changes for which they are authorized.**

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?

**This level of access is held by a very small number of individuals within ITS.**

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

**We would work with the University's Privacy Officer designated under the New Brunswick Right to Information and Protection of Privacy Act on a case-by-case basis.**

# 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.

**N/A**

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

SAML 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?

**No**