Participant Name: University of Guelph

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: University of Guelph

2.1.2. Information below is accurate as of this date: October 2, 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?

https://www.uoguelph.ca/web/privacy/
and
https://www.uoguelph.ca/ccs/security/internet/web-access-management

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: Gayleen Gray

Title or role: Associate Director and Deputy CIO, Strategy and Partnerships,

Computing and Communications Services

Email address: ggray@uoguelph.ca

Telephone: 519-824-4120 Extension 54699

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

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?

The set of people eligible for receiving an electronic identity is decided by the executive management of the University of Guelph in association with the CIO – for students it is the Registrar; for staff, faculty and retirees it is the VP Human Resources. Guest, Service and departmental identities require sponsorship from a recognized department and are authorized by Director, Dean or Chair of a department. Exceptions are allowed – these require approval of the same authorization departmental identities. All identities must have an official source of record.

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

100 percent

3.2 Electronic Identity Credentials

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.

Office of Registrarial Services submits student and graduate student registration information, including biographical and academic attributes via a custom interface during the offer of admission process. The Centre for Open Learning and Educational Support is responsible for vetting student data for Open Learning and Distance Education Students. Human Resources provides identity data for staff and faculty and visiting academics. Computing and Communications Services Department is the source of record for guest, departmental and service identities – information is submitted by electronic and hard copy forms – it is the responsibility of the Director, Dean or Chair to ensure that identity information submitted is correct and accurate user id and password.

3.2.1. 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 / Password

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:

Security Officer, University of Guelph

3.2.2. 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.

The University of Guelph Single Sign on solution is based on Oracle Access manager. Session timeout is set to 1hour and session timeout is max 8 hours – the Web Access management solution provides for Single Log Out functionality - Single Logout invalidates the session token – alternatively tokens are invalidated at browser close. The SSO implementation protects the IdP and the IdP session length is 30 seconds. The policy agent for the IdP is protected via OS permission and changes monitored and audited – vlan for communications are protected by physical and software firewalls with access strictly regulated.

3.2.3. 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?

Userid/Netid and eduPersonPrincipalName in 2009 the University adopted a no recycle policy – there are exceptions, these are rare and require special authorization and investigation such that reuse does not collide with information in other institutional repositories. Reassignment is generally by special request from executive offices, Deans, Directors and Departmental Chairs.

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?

Identity information based on Registrarial data is update 2x day (365) – our staff data is updated biweekly based on data obtained from University of Guelph HR and is based on active appointments. Biographical information except for Givenname changes must be made at the source of record for that individual. Individuals are allowed to update their own password change security questions and password. All other changes are made by the source of record for each attribute and changes are submitted via changes in data feeds or special update files. The CCS Help Centre and CCS Identity management team are allowed to make manual changes to information in the identity repository.

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

What is considered public is determined by role and follows the general rule s of expectation of privacy. For business related identities, biographical elements such as name, departmental affiliation, office location, business telephone and fax numbers and email address are considered public information. For students the only identity information considered public are name and email address.

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.

The majority of institutional level Academic and Business related applications, including: Learning Management System, University Financial and HR applications and software distribution. Future plans include the campus email and student information.

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?

We consider our IdP attribute assertions to be highly reliable (99% accuracy)

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 provided to participants cannot be repurposed without express permission of the University of Guelph.

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

All access to student PII must be authorized by Office of the Registrar – all access to Staff PII must be authorized by Human Resources see individual statements in http://www.uoguelph.ca/secretariat/records/

3.6.3. Please provide your privacy policy URL.

http://www.uoguelph.ca/secretariat/privacy/

http://www.uoguelph.ca/info/privacyguidelines/ProtectionofPrivacyandAccesstoInformation.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.

Not applicable, we do not make resources available to other participants.

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

Not applicable, we do not make resources available to other participants.

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

Not applicable, we do not make resources available to other participants.

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

Not applicable, we do not make resources available to other participants.

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

Not applicable, we do not make resources available to other participants.

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?

Not applicable, we do not make resources available to other participants.

____

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?

____

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

Not applicable, we do not make resources available to other participants.

____

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 Identity Provider v2.1.5

5.1.2. What operating systems are the implementations on?

RHEL 5 32-bit

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?

Passwords should never be transmitted in the clear - unintended exposure of credentials or PII must be reported to the Security Officer, University of Guelph as soon as possible. Data provided may not be stored or re purposed for any reason without express permission of the University of Guelph and the official sources of record.