Canadian Access Federation: Trust Assertion Document (TAD)

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.

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.

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.

Canadian Access Federation: Trust Assertion Document (TAD)

1. Canadian Access Federation Participant Information

1.1.1. Organization name: Olds College

1.1.2. Information below is accurate as of this date: October 2015

1.2 Identity Management and/or Privacy information

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

http://oldscollege.ca/Assets/OldsCollege/shared/BottomNav/Administration/policies/A/A18%20Access%20and%20Protection%20of%20Privacy.pdf

http://oldscollege.ca/Assets/OldsCollege/shared/BottomNav/Administration/policies/E/E03%20Information%20Management.pdf

1.3 Contact information

1.3.1. 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: Joe Guenther

Title or role: Director, Information Technology

Email address: jguenther@oldscollege.ca

Telephone:403-507-7923

2. 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.).

2.1 Community

2.1.1. 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?

Identities are provided to active students, faculty and staff
Temporary ID's are provided to external contractors based on approval from IT Department.

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

Active faculty, staff and students

2.2 Electronic Identity Credentials

2.2.1. 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.

Student accounts are provisioned when the students are admitted as per request from Student Services. Student accounts are deleted after they graduate
Staff and Faculty accounts are provisioned at the request of the HR department. These accounts are locked upon exit from the College.

2.2.2. 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?

Peap-MSCHAPv2 (via Radius) against Microsoft Active Directory
Google Active Directory Sync (GADS)

2.2.3. 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 scenarios where clear-text passwords would be transmitted.

2.2.4. 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.

No plans to implement a SSO solution that would connect to CAF.

2.2.5. 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?

Electronic identifiers are unique. Guest accounts are recovered by changing passwords. Guest accounts have no access to network resources & services and would not be included in federated ID’s such as CAF.

2.3 Electronic Identity Database

2.3.1. 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 acquired through the application process. There is currently no mechanism for students to update this information on their own. All changes are done by IT department staff.
Staff and Faculty information is provided and authorized by the HR department.

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

Staff & Faculty names, email addresses and telephone numbers are available on our website.

2.4 Uses of Your Electronic Identity Credential System

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

Desktop logins with file and print services, wireless network access, email services, ERP services, Moodle LMS access, VPN access

2.5 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.

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

Given the approval procedures through Student Services and HR, and the segregated account procedure in the IT department we have a high confidence in the reliability of our assertions.

2.5.2. 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

2.6 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.

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

Information is provided for Eduroam authentication purposes only, and should not be aggregated or shared with any third party.

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

We are not prepared to releasing our information to any other CAF participants, other than to implement Eduroam.

2.6.3. Please provide your privacy policy URL.

http://oldscollege.ca/Assets/OldsCollege/shared/BottomNav/Administration/policies/A/A18%20Access%20and%20Protection%20of%20Privacy.pdf

3. 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.

3.1 Attributes

3.1.1. 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 will use this information for Eduroam access to our wireless network and internet connectivity, only. We will only require valid authentication.

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

We log all internet access by client IP address. The Eduroam traffic will not be correlated to usernames or personal identity.

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

No

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

No

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

No

3.2 Technical Controls

3.2.1. 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

Because Eduroam is an Identity federation, there will be no third party information actually stored on our network.
Active Directory information is of course encrypted and only accessible through AD admin tools.
The authorization to make changes in our Active Directory is restricted to the personnel in the IT department, and therein restricted by roles. Because our AD information is based on data collected by other business units – Student Services & HR, there are also other personnel that have access to the same information. There are also similar role based restrictions.

3.2.2. 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 type of authorization is limited to very select few individuals within the IT department. This access list is frequently reviewed.

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

Follow Olds College and FOIP policies. E.g. take the compromised service off-line and contact the Olds College FOIP officer who along with Executive advise on the best course of action. Depending on the scope/size of the breach, the Office of the Privacy Commissioner of Alberta may be involved.

4. Other Information

4.1 Technical Standards, Versions and Interoperability

4.1.1. 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

4.1.2. What operating systems are the implementations on?

N/A

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

SAML 1.1

SAML 2.0

4.2 Other Considerations

4.2.1. 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