Participant Name:__Royal Roads 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: Royal Roads University

2.1.2. Information below is accurate as of this date: Sept 25th, 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?

http://www.royalroads.ca/about/rru-board-policies
http://computerservices.royalroads.ca/knowledge-base-section/accounts-passwords

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: Stephen Beaudry
Title or role: Manager of Server, Network and Telecommunication Infrastructure
Email address: steve.beaudry@royalroads.ca
Telephone: (250)391-2600 ext. 4149

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?

Accounts are granted to Staff, Faculty, Associate Faculty and Students registered in Degree programs. The department of Human Resources approves all staff, faculty and associate faculty accounts, while the department of the Registrar approves all student accounts.

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?

Staff, Students, Faculty and Associate Faculty

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.

Electronic accounts are created through one of two streams, either our 'Staff' process, or our 'Student' process.

Staff accounts must be requested through an internally developed system known as 'CAMP (Computer Accounts Management Process)', which then triggers a request for approval to the HR department. Once HR has approved the account, an automated set of scripts creates the computer account and notification is sent to appropriate departments, including payroll, IT, office planning, etc.

Student accounts are created by a set of automated scripts triggered through registration in our Student registration system. For a student account to be created, the person must be identified to the satisfaction of the registrar, enrolled in a degree program, and have paid the appropriate deposit.

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?

At this point, we use Kerberos and LDAP to authenticate users, based on username and password, stored in our Microsoft Active Directory.

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:

We do not use, nor allow, the use clear-text password transmission for any accounts.

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 do not have a 'single sign-on' system in place at this time. While we expect to implement such a system in the next year, it will only be used to authenticate our internal accounts, not for CAF Service Providers.

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?

We do not recycle usernames (our primary identifier) under any circumstances at this 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?

Staff information is updated via the 'CAMP (Computer Accounts Management Process)' system, which delivers notifications to appropriate departments. Staff are able to update certain details online, but not username or real name. Accounts have a maximum of two year lifespan, which must be manually extended by the account supervisor near expiry.

Students may update certain information about themselves through an online tool 'myadmin'. This does not include real name or username.

All staff name change requests, must be approved through the HR department, and manually entered by the IT department. All student name change requests must be requested and approved through the Registrar, and manually entered by the IT department.

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

Staff names, positions and phone numbers are published in an online directory.

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.

File storage, Finance Systems, Email systems, Resource scheduling systems, Learning management systems, Remote access, Wireless access, Web sites

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?

All primary identity information (username, real name) are assigned and managed through departments and processes that require physical verification of identity to a government issued ID. For example, name change requests must be accompanied by photo ID and legal certificate of name change.

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?

Attributes should be limited to Authentication and Authorization on a case by case basis, never used to produce any sort of publishable list.

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

British Columbia Freedom of Information and Protection of Privacy Act

3.6.3. Please provide your privacy policy URL.

http://www.royalroads.ca/about/privacy-policy

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 – only need to verify the individual is a valid user.

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

We log the username, home institution, and client MAC address for network audit purposes.

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?

Access to Personally Identifiable Information is limited to those business units that have an identified business need for the information. These are limited through Filesystem Access controls (where information is stored in files), or by application enforced user restrictions (where information is stored in a database).

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?

Super-user access is restricted to a very select few user accounts within the IT department, and these accounts are not used for regular access.

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

Royal Roads University maintains personal information of consumers and will notify customers if personal information has been subject to a security breach in accordance with the Freedom of Information and Privacy Protection Act (FOIPPA). The notification will be done as soon as possible, in one of the following manners:

- Written notification
- Electronic, if this is the customary means of communication between the University and client, or
- Telephone notice provided that you can directly contact your customer.

Notification may be delayed if a law enforcement agency determines that it will impede a criminal investigation.

The Office of the Information and Privacy Commissioner of British Columbia will be notified of all unauthorized disclosures of personal information in the manner prescribed by that agency.

If an investigation into the breach or consultation with law enforcement agencies or the Office of the Information and Privacy Commissioner of British Columbia determines there is no reasonable likelihood of harm to consumers, or if the personal information was encrypted or made unreadable, notification is not required.

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.

We use RADIUS to authenticate eduroam clients for the wireless network. We are not using any SAML products.

5.1.2. What operating systems are the implementations on?

OpenSUSE Linux

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

None

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