

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: Grant MacEwan University

2.1.2. Information below is accurate as of this date: November 29, 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?

The Records and Information Management Policy (D7510) is the parent policy that extends to all members of the University community. It can be accessed at <http://www.macewan.ca/wcm/ExecutiveandGovernance/BoardofGovernors/PolicyManual/index.htm#3>. This policy describes regulation and procedures used in the University with regard to the collection, use, disclosure and protection of personal information as well as how access to information will be provided under Part 1 of the Alberta Freedom of Information and Protection of Privacy Act. Further guidance on the collection, use, disclosure and protection of personal information is provided on our IAPPO website at <http://www.macewan.ca/wcm/Administrative/InformationAccessandPrivacyProtectionOffice/index.htm>. The privacy policy and practices specific to University websites, for example information collected automatically via the Internet, can be accessed at <http://www.macewan.ca/wcm/Forms/Privacy/index.htm>.

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: Jim Ross

Title or role: Coordinator, Information Security and Compliance

Email address: RossJ@macewan.ca

Telephone: 780-497-4402

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 tokens, 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?

Electronic identity is provided automatically to student applicants, registered credit and non-credit students, staff and faculty. Contingent workers, contractors and other Persons of Interest are eligible to receive electronic identity through a request process. In most cases a MacEwan employee, directly connected to the requester, vouches for and approves the request. Certain types of requests require the approval of IT Information Security.

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 and students

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.

Applicants, Students, Faculty and Staff: Identity is created for these groups through automated work-flow. MacEwan's Human Resources Department and the Office of the University Registrar own the administrative processes.

Identity can also be manually generated on request and with appropriate documented approval. The Information and Technology Services department owns the administrative process.

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 Name 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:

Name: Jim Ross

Title or role: Coordinator, Information Security and Compliance

Email address: RossJ@macewan.ca

Telephone: 780-497-4402

- 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.

Our SSO services are not used to authenticate people 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?

Our identifiers are considered unique for all 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?

Student identity information is acquired through the online registration process in collaboration with Apply Alberta. The data is collected by our ERP application and passed on to our Identity Management application. This information is automatically updated whenever there is a change to the student’s status as determined by the Office of the University Registrar.

Staff and Faculty identity information is acquired through the hiring process. Human Resources is responsible for all on-boarding. A record is created in our ERP and passed on to our Identity Management application. This information is automatically updated whenever there is a change to a staff member’s status.

Both staff and students can update their bio-demographic information through a self-service facility in our ERP.

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

None of this information is considered public information.

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.

Email and messaging, Learning Management Systems, eCommerce, print and file services, wireless network access, authentication and authorization to our ERP application, staff and student portal, various ldap-enabled productivity applications.

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? Our assertions are highly reliable.

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?

The attributes we provide to other Canadian Access Federation participants are collected and used in accordance with Alberta's Freedom of Information and Protection of Privacy Act. Use of the attributes we share with other Canadian Access Federation participants is limited to their original intended use of extending access to certain host network resources.

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

<http://www.macewan.ca/wcm/Forms/Privacy/index.htm>

IT Internal Control Standards regulating the export and use of MacEwan personally identifiable information

3.6.3. Please provide your privacy policy URL.

<http://www.macewan.ca/wcm/Forms/Privacy/index.htm>

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.

Users of Eduroam wireless access provide an email address of a participating institution. That attribute information is used to route the authentication request to the appropriate authentication system.

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

No additional use

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?

Admin and privileged access to our identity vault is subject to well-designed and effective access controls that are based on the principle of least privilege.

- 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?

Admin and privileged access to our identity vault is subject to well-designed and effective access controls that are based on the principle of least privilege.

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

Incident response is a coordinated activity between the offices of IT Information Security and Compliance, and the University's Information and Privacy Protection Office. Privacy and information security breaches are assessed, evaluated, contained if necessary, investigated for root cause and communicated in accordance with internal standards and procedures. MacEwan uses criteria established by the Alberta Privacy Commissioner to assess whether there is real risk of significant harm as a result of the loss of, unauthorized access to or unauthorized disclosure of an individual's personal information in making decisions about individual privacy breach notification.

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.

None

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.

N/A

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

