Participant Name: Grant MacEwan 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: Grant MacEwan University

2.1.2. Information below is accurate as of this date: February 15, 2019

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?

Records Management Policy: https://www.macewan.ca/policies, search for Records Management (D7510)

Information Access and Privacy: https://www.macewan.ca/privacy

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: Tim Crisall

Title or role: Chief Information Security Officer

Email address: crisallt@macewan.ca

Telephone: +1 (780) 497-5040

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?

By default, an electronic identity is provided to persons identified as Applicants, Students, Faculty or Staff. Contingent workers, contractors, and other persons of interest are eligible to be provisioned with an electronic identity through a request process, where an appropriate University employee approves the request.

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?

Students, faculty, and staff.

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.

The processes to establish a person record are managed in the core Student Management and Human Resource Management systems. These processes are owned by the Office of the University Registrar (students, applicants, prospects) and the Human Resources department (faculty, staff, contractors, persons of interest), respectively.

The establishment of an electronic identity is managed through the Identity Management system, owned by the Information Technology Services department. When persons created through the processes above are assigned specific valid roles (e.g. Student, Employee) by the respective administrative systems, an electronic identity is established.

An electronic identity can also be generated manually, on request, and with appropriate documented approval. The Information Technology Services department own 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 ID and Password are always required. Some higher-level access requires an additional second factor to be provided.

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:

Tim Crisall

Chief Information Security Officer

IT Compliance and Information Security Office

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.

MacEwan’s single sign-on (SSO) is provided by a SAML 2 compliant identity provider (IdP). The IdP enforces session timeouts at the authentication point. Users can opt in or out of an extended time to live for their authenticated state. IdP SSO session termination can be initiated by the user from a Sign Out option on the University’s main services portal. Single logout to service provider (SP) endpoints is not supported, but end users are reminded of the SPs they interacted with at the time of the logout of the IdP SSO Session.

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?

The primary person identifier is considered unique for all time. For federated ID purposes, a similarly unchanging, but opaque, identifier will be provisioned.

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?

Primary person identifiers are generated by the core administrative systems owned by the Office of the University Registrar and the HR department. Biographical data enters these systems through a variety of self-service and administrative processes. Additional data about persons, such as roles and affiliations, is assigned through administrative processes, both automatic and manual, in the core administrative systems. Changes in these systems are reflected in the Identity Management system.

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

The information in the Identity Management system is not directly available to the public.

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.

Systems and services providing learning support, electronic communication and collaboration, print and file access, wireless network access, administrative activities, productivity, VPN.

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. Attributes are retrieved in real time from our Identity Management system. The Identity Management system is constantly updated from the core administrative systems.

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 University expects service providers to use the attribute information only for the purposes of providing their service to the University. Refer to Grant MacEwan University Privacy Policy.

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

Grant MacEwan University Privacy Policy.

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

3.6.3. Please provide your privacy policy URL.

https://www.macewan.ca/privacy

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. The attribute information is used to route the authentication request to the appropriate authentication system. The University is not planning to act as a Service Provider in the federated ID network.

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?

Since Grant MacEwan University does not act as a service provider, we do not receive or store external partner attribute information.

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?

Since Grant MacEwan University does not act as a service provider, we do not receive or store external partner attribute information.

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

Since Grant MacEwan University does not act as a service provider, we do not receive or store external partner attribute information.

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 IdP, currently on version 3.3.3.

5.1.2. What operating systems are the implementations on?

SuSE Linux Enterprise Server (SLES) 12.3

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

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 other considerations.