Participant Name: University of Alberta

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 Alberta**

2.1.2. Information below is accurate as of this date: **October 9, 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?

Information Management and information Technology Policies: https://policiesonline.ualberta.ca/PoliciesProcedures/Pages/Information-Management-and-Information-Technology.aspx

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: **Gordie Mah**

Title or role: **Information Technology Security Officer**

Email address: **gordie@ualberta.ca**

Telephone: **780 492-8607**

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?

Users must have an affiliation with the University of Alberta for an account to be created e.g faculty, staff, student, etc…

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?

Any active account will be identified as a participant in SAML identity assertion for CAF service providers. _

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.

A user is created in our ERP which in in turn will create an account in our Identity Management System.

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?

Kerberos, SAML, and Radius

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:

abuse@ualberta.ca

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.

Sessions will last for 8 hours on our Identity Provider. Service Providers must enforce their own timeouts based on the service requirements. The only trusted method to log out of all services requires that the user completely shut down their browser to expire their sessions.

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?

For all user accounts eduPersonTargetedID is unique for all time. NetID and eduPersonPrincipalName is not unique for the lifetime of the user. Users are able to request that their NetID be changed. Once an account has been deactivated it will not be reissued for at least a year and a half.

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?

Information in our Identity Database is synchronized with our ERP. None of the attributes that are shared through our SAML service can be modified directly by the user.

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

Information about public/private information can be found on our IMS interface site https://sites.google.com/a/ualberta.ca/open-data/people-data

---

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.

Any service that the University requires to perform University business is able to use our electronic identities to identity users

---

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? The attributes are based on data in our ERP and are trusted by our institution.

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?

Ensure that before *eduPersonScopedAffiliation* attribute is provided to other CAF participants, that our University (as in 2.3.1) is notified and approves of this additional use.

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

No formal or documented policies exist in this regard currently as we rely on CAF protocols for this.

3.6.3. Please provide your privacy policy URL.

Suite of Privacy and Security Policies is located at:
https://policiesonline.ualberta.ca/PoliciesProcedures/Pages/Information-Management-and-Information-Technology.aspx

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.

We do not provide any service applications for CAF participants at this time.

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

N/A

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

N/A

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

N/A

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

N/A

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?

The University standard is to encrypt sensitive information in transmission and storage. Human controls include (but are not limited to): privacy and security reviews are required for any new system or major change to existing systems, training and awareness, cover-off and backup, background and criminal records checks for certain areas (such as those with access to sensitive financial or patient/health information), defining roles and required privileges to use for provisioning administrative access, Technical controls include (but

are not limited to): transaction logs, auditing triggers, multi-factor-authentication (in some areas), access controls, network security controls, firewalls (including internal), IPS/IDS, AV, and end-point controls.

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?

The University standard is to encrypt sensitive information in transmission and storage. Human controls include (but are not limited to): privacy and security reviews are required for any new system or major change to existing systems, training and awareness, cover-off and backup, background and criminal records checks for certain areas (such as those with access to sensitive financial or patient/health information), defining roles and required privileges to use for provisioning administrative access, Technical controls include (but are not limited to): transaction logs, auditing triggers, multi-factor-authentication (in some areas), access controls, network security controls, firewalls (including internal), IPS/IDS, AV, and end-point controls.

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

Breach investigations and responses follow the University's standard process and protocol in these cases. Based on an assessment of risks to the potentially affected individuals, the Privacy, Security, and Legal offices determine if, when, how, what, and who to notify. Such notification is also accompanied by notifying the Alberta Provincial Office of the Information and Privacy Commission (OIPC).

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.

SimpleSAMLphp v1.12

5.1.2. What operating systems are the implementations on?

Ubuntu

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?

The University of Alberta prohibits transmission and storage of credentials in clear text. Breaches involving University of Alberta affiliates or information/records must be reported immediately to the University of Alberta (as per Alberta provincial FOIP and HIA legislation).