canarie

Participant Name: Fanshawe College
Peter Gilbert - CIO

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: Fanshawe College

2.1.2. Information below is accurate as of this date: March 17, 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?

Email – pgilbert@fanshawec.ca

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: Jimmy Tom

Title or role: Senior Manager, Network Services and Computer Operations

Email address: jtom@fanshawec.ca

Telephone: 519-452-4430 x4890

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?

Staff are granted identities and provided access to systems needed to perform their roles. Human Resources validates the employment status of employees to the ITS department.

Students are granted identities and provided access to systems needed for their learning environment once they have been accepted as students. The Office of the Registrar validates the status of students to the ITS department.

Contractors and service staff may also be granted system access in order to perform tasks on behalf of the College. Applicants to the College receive an account in order to interact with web-based resources that allow them to move from applicant to student.

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 and Faculty who move among the CAF Service Provider sites, and students with courses that have course maps involving other educational institutions.

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.

Human resources provides the list of new employees to the ITS department while department managers identify changing roles for staff already employed. The Office of the Registrar maintains the list of active and past students who require access to our systems.

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?

Username and password are the current credentials issued to staff, faculty and students.

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:

Concerns of this manner may be discussed with the Manager, Network Services and Computer Operations.

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.

Fanshawe uses Shibboleth and CAS integration for a SSO solution, although most applications validate using our Active Directory credentials via LDAP.

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?

sAMAccountName is unique to the individual, however can be reassigned after a number of years not associated at the College. While there currently does not exist a formal process for this, the College may review this in the future. EmployeeNumber is unique to an individual and at this time has no reassignment.

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 is acquired through HR and Office of the Registrar processes. Accounts are generated by a designated set of staff working within the Technical Support Services department. Staff are not currently able to update their own information on-line.

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

Published staff data includes telephone extension, mobile and fax numbers, and office location are items which can be viewed through our Outlook system. There is no published student information available.

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, SharePoint, ERP, CRM, Student Information System, Learning Delivery System, File Shares

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?

Highly reliable and accurate.

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
No

b) be used to purchase goods or services for your organization?
Yes
No

c) enable access to personal information such as student record information?
Yes
No

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?

We would prefer to provide only information that might be available to our internal users via Outlook.

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

College Policy 1-I-18 Freedom of Information and Protection of Privacy. The purpose of this policy is to outline the principles associated with providing access to public information while protecting the privacy of personal information and the confidentiality of third party information, in accordance with government legislation.

3.6.3. Please provide your privacy policy URL.

Our Freedom of Information and Protection of Privacy policy is available at http://www.fanshawec.ca/sites/default/files/assets/policies/pdf/1i18.pdf

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.

Initial service will be internet access, with attribute requirement being that the request is coming from someone with current access credentials to a partner site.

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

Validation only.

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

Not currently.

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?

To be determined.

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?

All attribute information is stored in Active Directory (AD). Rights for AD management are strictly controlled.Some synchronization and automated tasks occur between management systems to automate access.

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?

ITS Management reviews requests for AD management rights based on IT role.

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

Has not happened, but would involve reaching out via telephone (email if no phone number present) to identify the nature and timing of the breach.

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 v2.4.0, CAS Server v3.5.2

5.1.2. What operating systems are the implementations on?

Windows Server 2008R2, Apache Tomcat 6.0.37

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

SAML 1.1

SAML 2.0 (Preferred)

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?