



Participant Name: NAIT

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: Northern Alberta Institute of Technology

2.1.2. Information below is accurate as of this date: April 7, 2017

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?

Privacy Policy: <http://www.nait.ca/privacypolicy.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: Loren Bain

Title or role: Manager Technical Services

Email address: lorenb@nait.ca

Telephone: 780-378-6123

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?

All Employees and Students of NAIT will automatically receive an electronic identity as part of their employment or enrolment. Contractors, Vendors, External Collaborators, Prospective Students may also receive electronic identities. Prospective Students can register for an electronic identity online through the myNAIT Portal in order to register in courses. Other electronic identities that are issued manually require authorization from a NAIT staff member and are given an expiration date usually less than or equal to one year from the requested date.

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?
Active Employees, Contract Staff, and Prospective and Active Students .

Commented [DA1]: I would understand that inclusion of this user type would make statements in section 3.5 untenable.

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.

For Employees, when an employee is hired an Active Directory account is automatically generated using a defined process. The same process disables the Active Directory account upon termination. NAIT Human Resources is responsible for managing the status of employees, and this status is used to provision and disable accounts.

For Students, when a student is accepted into a program or is enrolled in a Continuing Education or Apprenticeship program, an automated process will create their electronic identity in Active Directory using a defined process. This process will remove the account from the directory after 18 months since the last use of the account using last login. NAIT Registrar is responsible for managing the status of students and this status is used to provision and disable accounts.

For Contract Staff, as required a NAIT Staff member may provide a service request to IT to have an account created for a person operating in a staff role under a contract to the individual or to the company for which the individual is employed. The user is required to sign an access agreement and will be provided an account with an expiration typically up

to one year. The IT Service Management Team is responsible for these identities and records.

- 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?

Active Directory and Active Directory Federation Services are used as key authentication technologies that enable identities across various systems. Kerberos, NTLM, WS-Federation, and SAML security protocols are the most common authentication methods. There is a 1:1 relationship between employee records and employee accounts and a 1:1 relationship between student records and student accounts. If an employee is also a student, the employee will have 2 accounts that are not formally linked.

- 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:

There are no known applications soliciting unencrypted clear text passwords across unsecured networks. The contact person for this document can be reached for further questions.

- 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.

NAIT uses Active Directory Federation Services for campus-wide single sign on and will be using this system to authenticate users for CAF service providers. The following security measures are in-place:

- Federation Proxies to limit access to Federation Services in the DMZ.
 - 4-hour SSO session expiration.
 - SSO Logout option on all Service Providers takes the user to a logout page where all sessions are terminated, and users are encouraged to close all browser windows and clear cache on public computers.
-

- 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?

Yes, they are considered unique and are not reused. Employee accounts are disabled upon termination and not deleted so that the account can not be reused. A provisioning database exists for Student accounts so that usernames are not reused and so that a returning student will receive the same username.

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?

Employee information and Student information is updated automatically from the Human Resources and Student Administration systems respectively.

Other accounts are updated by the IT Service Management Team as requested by authorized individuals.

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

All personal information (Name, Email Addresses, Phone Numbers) are protected by FOIP and can only be released as required to provide service to students.

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.

The Active Directory credentials are used for virtually all internal systems with a very few exceptions including file shares, email, PeopleSoft, website etc.

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?

Attribute assertions should be considered reliable. The attributes for student accounts (for example name) have not been physically verified by other documentation (i.e. drivers licenses), but have been provided under agreement that the information provided is 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

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 only be used as required and authorized by NAIT.

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

NAIT's Privacy Policy, the Freedom of Information and Protection of Privacy Act of Alberta and The Privacy Act of Canada.

3.6.3. Please provide your privacy policy URL.

<http://www.nait.ca/privacypolicy.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.

eduPersonPrincipalName

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

none

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

Yes.

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?

All attribute information is encrypted when transmitted over unsecure networks.

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?

NAIT IT Compliance maintains and tests controls to ensure that privileged accounts are appropriately reviewed. Users with privileged accounts are required to sign a privileged access agreement. Changes to privileged access is audited.

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

Actions and disclosure in response to a compromise are conducted to compliance with the law in consultation with NAIT's General Counsel and Executive Committee.

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.

Active Directory Federation Services – Windows Server 2016

5.1.2. What operating systems are the implementations on?

Windows Server 2016

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

SAML 1.1 - Yes

SAML 2.0 - Yes

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?