Participant Name: Bow Valley College

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: Bow Valley College (BVC)

2.1.2. Information below is accurate as of this date: January 31, 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 on BVC's privacy policy can be found on its main website at http://www.bowvalleycollege.ca/privacy-policy.html

Compliance by BVC with the Freedom of Information and Protection of Privacy Act of Alberta is mandatory. Additional information can be found at http://www.servicealberta.ca/foip/

Policies that are related to Privacy (e.g. Privacy and Access Policy) and Identity Management (e.g. Information Management Policy) can be accessed through the BVC Board contact at http://www.bowvalleycollege.ca/about-bvc/offices-and-governance/board-of-governors/policies.html Note: We are currently preparing PDF versions of BVC policies.
If you are looking for BVC policies and do not work for BVC, please contact the person listed on the site to request the policy topic for which you would like a copy.

Other documentation can be accessed by contacting the ITS department at helpdesk@bowvalleycollege.ca or 403.410.1611

2.2.2. 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: Mark Prevey
Title or role: Acting ITS Director
Email address: mprevey@bowvalleycollege.ca
Telephone: 403.410.1618

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., user-ids/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?

Faculty, staff and students are eligible when they are active members of the College; Alumni keep their electronic identity; contractors and external people become eligible where an existing BVC supervisor takes responsibility for that person's action (extended access to the network) or a BVC employee verifies access (to limited wireless service) is required to support a BVC event or service. There are no exceptions.

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, students

3.2 Electronic Identity Credentials

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.

1. Students – Must be an active in Student System (ERP); other status such as alumni are limited to their individual MyBVC login ; the registrar's office is responsible for confirming identity and IT services ensure identity is maintained in AD

2. Employees – Must be active employee in the BVC HR system (ERP); the HR department is responsible for confirming identity and IT services ensure identity is maintained in AD

3. Contractor – has been legally contracted to provide BVC with a product or service and requires temporary (less than a year) access to the network; the immediate supervisor to the contractor is responsible for confirming identity and IT services ensure identity is maintained in AD.

4. Wireless access (short term): temporary limited accounts are created for external people using the College's facilities for an event; identity is confirmed by a BVC employee directly involved in the event (e.g. sponsor or room booking) and IT services ensure identity is maintained in AD

3.2.1. What authentication technologies are used for your electronic identity credentials (e.g., Kerberos, user ID/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?

Current authentication technologies are Integrated Windows Authentication (NTLM and Kerberos) and forms-based authentication. Multiple credentials are not linked.

3.2.2. 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 circumstances that a secret would be transmitted across a network without being protected by encryption. For Participant concerns, please contact James Cairns, ITS, Bow Valley College

3.2.3. 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.

Not currently.

3.2.4. 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?

Electronic identifiers are unique

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?

Staff and faculty with a HR record in BVC's ERP are allowed to sign into their own personal web services and update some items otherwise changes are performed by HR, all changes workflow to HR for validation. Student information is updated through specific/designated people in the Registrar's

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

Name, email address, desktop telephone number, department
http://bowvalleycollege.ca/talk-with-us/contacts.html

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 services, ERP services, wireless access, Student Portal (MyBVC), D2L services, access to file servers (staff & faculty), VPN Services, business 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?

As our identity provider federation system is AD FS 2.0, and the identities currently being asserted are Active Directory integrated identities that have been vetted through a rigorous and thorough process, the reliability of the iP attribute assertions is very 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?

Sharing of attribute information would follow established policies and procedures designed to protect the privacy and integrity of all members of the BVC community. Restrictions include but are not limited to FOIP expectations.

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

Freedom Of Information and Protection of Privacy Act (FOIP); Personal Information Protection Act (PIPA);Health Information Act (HIA)

3.6.3. Please provide your privacy policy URL.

http://www.bowvalleycollege.ca/privacy-policy.html

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.

There are currently no service applications offered at this time.

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

All additional attribute information is discarded at the claim made

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?

Attributes are protected by Access Control Lists. Changes to AD are controlled through the appropriate departments (HR and Registrars) access by ITS personnel is limited through role requirements. E.g. Help Desk support for user accounts.

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?

This type of access is severely restricted to a very limited number of people. Access is monitored and anomalies researched immediately.

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

Follow FOIP and BVC requirements. E.g. disable the service that has been compromised, contact BVC FOIP officer who along with Executive advise on best course of action, depending on the scope/size of breach the Office of the Privacy Commissioner of Canada may be involved. Following FOIP is mandatory.

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.

N.A.

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.

SAML 1.1

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