Canadian Access Federation: Trust Assertion Document (TAD)

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.

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.

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.

Canadian Access Federation: Trust Assertion Document (TAD)

1. Canadian Access Federation Participant Information

1.1.1. Organization name: Ciena

1.1.2. Information below is accurate as of this date: May 1st, 2019

1.2 Identity Management and/or Privacy information

1.2.1. Where can other Canadian Access Federation Participants find additional information about your identity management practices and/or privacy policy regarding personal information?

https://www.ciena.com/privacy/

1.3 Contact information

1.3.1. 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: Ciena

Title or role: IT

Email address: itservicedesk@ciena.com

Telephone: +1 800-921-1114

2. 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.).

2.1 Community

2.1.1. 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?

Any Ciena employees, contractors and interns are eligible to receive an electronic identity.

The specific list of these people and possible exceptions are defined by the Ciena's External Research department of the Office of the CTO.

2.1.2. What subset of persons registered in your identity management system would you identify as a "Participant" in SAML identity assertions to **CAF** Service Providers?

Only Ciena employees, contractors and interns who work with the Ciena Environment for Network Innovation (CENI).

The specific list of these people and possible exceptions are defined by the Ciena's External Research department of the Office of the CTO.

2.2 Electronic Identity Credentials

2.2.1. 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.

Electronic identities are established through a formal user registration process beginning with a formal request from HR to the IT Specialist, who maintains a record for all access requests.

2.2.2. 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?

Ciena uses user name and password for authentication.

2.2.3. 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 such circumstances, all authentication information is encrypted.

2.2.4. 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.

The authentication flow is protected with user credentials (IWA for on prem users) along with MFA enforcement.

The session termination is 12 hrs for both on and off premise connections.

2.2.5. 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?

Our primary unique identifier is UPN. Also, this can be combined with employeeID to further ensure the identity (if application supports multiple SAML assertions).

Reassignment conflict is protected with lookup tools in place to ensure the userID is not reused. The tool queries Ciena Active Directory, database systems, engineering ldap HR records. Same ID is reused in case of a rehire.

2.3 Electronic Identity Database

2.3.1. 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?

Acquisition and updates are managed by Ciena’s **HR** and IT Department. However, users can also update their own information online.

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

There is no public information, and nothing would be provider to any external to Ciena party without any exception and under any circumstances.

2.4 Uses of Your Electronic Identity Credential System

2.4.1. Please identify typical classes of applications for which your electronic identity credentials are used within your own organization.

Email client.

2.5 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.

2.5.1. Please describe the reliability of your identity provider attribute assertions.

Attributes are securely mapped from Active Directory to the IdP directory database. Only the Org Admins for Identity Platform can make an authorized change.

2.5.2. 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

2.6 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.

2.6.1. What restrictions do you place on the use of attribute information that you might provide to other Canadian Access Federation participants?

Do not use any attributes; we do not provide this information to CAF participants.

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

The privacy policy.

2.6.3. Please provide your privacy policy URL.

https://www.ciena.com/privacy/

3. 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.

3.1 Attributes

3.1.1. 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.

Not applicable: nothing is provided.

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

Not applicable: nothing is provided.

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

Not applicable: nothing is provided.

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

Not applicable: nothing is provided.

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

No, we do not.

3.2 Technical Controls

3.2.1. 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 user name is stored within the domain controller in Active Directory. The data within the domain controller is encrypted and is accessible by Ciena's IT Department only. There is no personal identifiable stored on the domain controller

3.2.2. 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 management of privileged accounts and the authority to grant access to personally identifiable information is a centralised function managed by Ciena's IT Department.

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

Our notification process is inline with the PIPEDA (Personal Information and Electronic Document Act).

4. Other Information

4.1 Technical Standards, Versions and Interoperability

4.1.1. Identify the SAML products you are using. If you are using the open source Internet2 Shibboleth products identify the release that you are using.

We are using Okta as our primary IdP.

4.1.2. What operating systems are the implementations on?

Okta is a cloud based service (built on Amazon Web Services platform)

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

SAML 2.0

4.2 Other Considerations

4.2.1. 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?

Signed SAML assertion is preferred for enhanced level of security.