Participant Name:__CANARIE Inc. _____

CANARIE 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: __CANARIE Inc._____

2.1.2. Information below is accurate as of this date: ____January 29, 2015_____

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?

CANARIE's privacy policy can be found at: https://canarie.ca/privacy-policy

Requests for additional information beyond what is in this document should go to canarieit@canarie.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: Nancy Carter

Title or role: Chief Financial Officer

Email address: nancy.carter@canarie.ca

Telephone: (613) 943-5437

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?

Response:

CANARIE issues accounts to people with immediate and active relationships with CANARIE based on CANARIE's internal HR policies which encompass: staff, board members, contractors, and those who partner with CANARIE.

When this active relationship ceases, the accounts relating to this individual goes through a deactivation process that is manual where access is restricted or revoked according to CANARIE's internal HR policy and the discretion of the executive management team.

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?

Response:

Participants are people who have an active account per the above response

---

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.

Response:

Requests for electronic identities to be created are handled by the central IT department of CANARIE. The requests originate as a result of an existing business process or at the request of either the executive management team or network operations team.

Provided the request meets the necessary criteria for creation, an account is created with the appropriate permission levels assigned. The end user is provided an initial password and is asked to immediately change it upon first use.

The office of record is the CFO group for which the contact information is in 2.3.1

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?

Response:

CANARIE uses Active directory to manage electronic credentials. Standard Active Directory credential policies are in effect for: password strength and password rotation that is 90 days or less.

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:

Response:

CANARIE's practices are to only used encrypted means of transmitting passwords across the network either via SSL encryption or VPN where not possible.

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.

Response:

CANARIE uses Shibboleth 2.3 for it's SSO environment and the default configuration for it with a session time of 3hrs. User-initiated session termination is 'close the browser' to release the credentials which is also directed at any public use sites

---

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?

Response:

eduPersonPrincipalName maps to samAccountName which may very infrequently change.

eduPersonTargetedID is based on eduPersonPrincipalName and the target site so follows the same infrequent change practice

The practice is to not re-assign the samAccountName but may be re-assigned once a period of 1 year has passed which in turn influences the eduPersonPrincipalName and eduPersonTargetedID.

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?

Response:

Information is maintained by central IT. Systems of record are HR and the operational systems within the network operations centre. Individuals do not self manage their identity information and follow existing internal HR practices for name changes or entitlement changes due to role within the organization

---

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

Response:

Public information is what is published on the CANARIE website under the heading 'our team' which is a white pages like list of common name, phone number, and role within CANARIE.

All other data is considered internal to CANARIE.

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.

Response:

Typical classes of applications are sign on for: personal access on both laptops and desktops , remote VPN access, server access, network device access, internal application access, 3rd party access via Shibboleth

---

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?

Response:

Highly 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?
RESPONSE: Yes

b) be used to purchase goods or services for your organization?
RESPONSE: Yes

c) enable access to personal information such as student record information?
RESPONSE: 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?

RESPONSE:

CANARIE is to be the only recognized authority on CANARIE attribute information and assertions regarding CANARIE identities. Other participants who seek information about CANARIE identities and the assertions about them should not rely on a 3rd party to provide

that. Instead, participants should request establishing a relationship with CANARIE either for a one-time information exchange or establishing an ongoing process so as to ensure they are consuming accurate and authoritative information.

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

RESPONSE:

Please see 2.2.1

3.6.3. Please provide your privacy policy URL.

RESPONSE:

CANARIE's privacy policy can be found at: https://canarie.ca/privacy-policy

---

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.

RESPONSE:

CANARIE operates a number of services but tries to simplify attribute release in a single set of required and optional attributes.

This set of attributes being requested are detailed in this document:

https://tts.canarie.ca/otrs/public.pl?Action=PublicFAQZoom;ItemID=22

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

RESPONSE:

Use of information depends on a service by service basis. CANARIE uses a number of tools that each require a form to uniquely identify a user so that when they return to the tool their information and settings are preserved and intact.

Our preference is to use eduPersonTargetedID but when that is not possible eduPersonPrincipalName and email are used as primary identifiers in the various services.

See the document mentioned in 4.1.1 for additional details.

Name information about a user is requested to properly identify a user such that an account may be more easily found within the existing tool and end users may have a personalized experience.

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

RESPONSE:

Yes, see 4.1.2 for more details.

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

RESPONSE:

Aggregate reports are used wherever possible for any health,status, or usage metric that may be reported on (e.g. number of distinct users by day).

Each service does record who performed what action and by whom and is guided by the principles as outlined here: http://www.canarie.ca/en/privacypolicy

---

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

RESPONSE:

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?

RESPONSE:

The CANARIE IT department follows and applies industry security best practices for managing access to resources. Services that contain PII have audit capabilities to identify those who access and retrieve information or have administrative control on it.

Service administration activities are limited to a small number of users. Services are managed and stored behind a firewalled and virtualized infrastructure.

Assignment of administrator privilege is done through the CANARIE IT department and existing approval processes for line of business managers.

Different services have different capabilities and where possible audit logging is enabled. Audit is used both for access logging and also for the purpose of operating and diagnosing the health of the service.

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?

RESPONSE:

Privileged users are assigned through the CANARIE IT department using existing approval processes for line of business managers.

Different services have different levels of capabilities and administrators of those services use best practices to balance the targeted utility of a service and protection/masking of identity information.

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

RESPONSE:

In the case of a local identity breach, the CANARIE IT department will work to notify those impacted. If outside organizations need to report a breach to us, use the canarieit@canarie.ca address and our CANARIE IT department will handle the local coordination.

---

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.

RESPONSE:

Shibboleth 2.3.0

5.1.2. What operating systems are the implementations on?

RESPONSE:

Redhat 6.1

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

SAML 1.1

RESPONSE: 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?
