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: Perimeter Institute

1.1.2. Information below is accurate as of this date: November 3, 2017

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?

www.perimeterinstitute.ca/site/privacy-policy

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: Stefan Pregelj
Title or role: Senior Director, Finance and Operations
Email address: spregelj[at]perimeterinstitute[dot]ca
Telephone: 519 569 7600 x510

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?

Electronic identities are issued for a wide range of purposes from an email address through to administrative access to key business systems. Perimeter issues these identities for the following groups of stakeholders:

- Full time researchers including faculty, postdocs, full time graduate students
- Associate and affiliate researchers

- Long term and special status visitors
- Full time administrative staff
- Full and part time contract staff
- Co-op and volunteer staff

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?

- Full time researchers including faculty, postdocs, full time graduate students
- Full time administrative staff

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.

Requests for electronic identities are initiated through the recruitment process that is coordinated and validated by the HR function (People & Culture department). Records of status are maintained within the contact management system which provides the central repository and system of record for all contact information.

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?

Perimeter provides a user ID and password in Active Directory that is synched to Okta’s access and identity management service.

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:

In all cases but the following, all passwords are encrypted:

- Test web site that are only internally accessible;
- The KOHA library system;

The KOHA system is being hardened in the next few months and will no longer pose a security concern. Any and all security concerns should be addressed to the Manager, Technology Services (infosec@pitp.ca).

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.

Perimeter uses Okta's AIM services which use the SOC 2, Type I and Type II processes to successfully audit the operational and security processes of our service and our company. Okta has achieved the Cloud Security Alliance (CSA) Security, Trust, & Assurance Registry (STAR) Level 2 Attestation. Okta has also achieved ISO 27001:2013 Certification, attesting to the commitment to a secure service for our customers.

Specific security features include:

- All customer data is encrypted at data field level
- All customer instances have unique encryption keys
- Okta leverages AWS' highly secure key management service
- Enforced session timeout periods

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?

Perimeter uses rules in its CRM system to issue unique users names and staff IDs.

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?

All contact information is centralized and managed in a single CRM system. Management of user names and staff IDs is restricted to system administrators. Users can update their security questions via Okta AIM system and certain non-sensitive user information (address, emergency contacts, etc.) via an integrated institution portal.

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

A subset of user information is listed on our web site including user names, position, title, research area, biography, and optionally: email and phone number.

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.

- Web sites and content management systems
- Business systems (CRM, finance, HR, etc.)
- Research computing systems

- Network and communication systems

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?

We would describe the reliability as very high as we are a small organization with a centrally managed contact management system run by dedicated staff.

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

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

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

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?

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

2.6.3. Please provide your privacy policy URL.

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.

- Wireless/Internet: unique identifier
- All other systems are authenticated separately through our AIM system and processes.

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

- None

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

- No

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

- No

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

- No

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?

- Check notes on SF features
- Access is restricted to authorized personnel only
- Changes are logged and audited
- Privacy policy restricts the use and dissemination of this information

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?

- Superuser accounts are restricted to the IT deparment
- Superuser accounts are reset on departure of staff

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

- Perimeter identifies or is notified of a security breach with the potential to expose data
- Immediately alert the Perimeter Privacy & Security Committee and initiate a security incident response procedure (SIRP)
- The SIRP includes the following steps:
    - 1. **Detect & Analyze**
    - 2. Containment or Recovery
    - 3. Investigation
    - 4. Restoration
    - 5. Evaluation and Mitigation
- Each of the first four stages includes a notification step. In the initial stage, "Detect & Analyze", an initial assessment is understaken to determine the nature and severity of the breach and then notification is made based on this assessment:
        - 1.1. Alert SIRP team to possible incident (to ensure appropriate communications and process)
        - 1.2. Conduct preliminary analysis (to determine scope and severity)
        - 1.3. Document findings (to facilitate response and resolution)
        - 1.4. Prioritize incident (to determine level of response and notifications)
        - 1.5. **Notify affected parties** (to acknowledge incident and response)
- Perimeter will initiate notification procedures as follows:
    - Notify affected individual(s):
        - after preliminary assessment and no less that 24 hours
        - (a) by email or any other secure form of communication if the affected individual has consented to receiving information from the organization in that manner; (b) by telephone; (c) in person; (d) or by letter delivered to the last known home address of the affected individual;
        - including the following information:
            -
            - a description of the circumstances of the breach;
            - the day on which, or period during which, the breach occurred;
            - a description of the personal information that is the subject of the breach;
            - a description of the steps that the organization has taken to reduce the risk of harm to the affected individual resulting from the breach or to mitigate that harm;
            - a description of the steps that the affected individual could take to reduce the risk of harm resulting from the breach or to mitigate that harm;

        - a toll-free number or email address that the affected individual can use to obtain further information about the breach; and
        - information about the organization's internal complaint process and about the affected individual's right, under PIPEDA, to file a complaint with the Commissioner
    - Notify appropriate law enforcement & government agencies within 24 hours by email or phone
    - Notify appropriate 3rd party agencies within 24 hours by email or phone
- Further notifications will follow as Perimeter completes the investigation and restoration stages of its response process to provide key updates on steps taken to qualify and mitigate any exposure.

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.

Perimeter is using Okta as an identity provider which is SAML compliant. Perimeter also users multiple SaaS services and Drupal which are all SAML compliant.

4.1.2. What operating systems are the implementations on?

Okta is a SaaS service. Drupal is installed on Linux Ubuntu 16.04.

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

SAML 1.1

SAML 2.0: Okta, Drupal

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?

- Not at this time.