

Participant Name: MediaCore

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:
 - a. <http://www.mediacore.com/caf-tad/>

You must maintain an up-to-date Trust Assertion Document.

2. Canadian Access Federation Participant Information

2.1.1. Organization name: [MediaCore Technologies, Inc](#)

2.1.2. Information below is accurate as of this date: [September 1st, 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?

<http://www.mediacore.com/legal/>

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: [Anthony Theocharis](#)

Title or role: [Chief of Engineering](#)

Email address: anthony@mediacore.com

Telephone: [1-250-590-9394](tel:1-250-590-9394)

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?

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?

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.

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?

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:

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.

- 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?
-

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?
-

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

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.
-

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?
-

- 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
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

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?

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

3.6.3. Please provide your privacy policy URL.

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.

MediaCore requires the following SAML attributes to be released in order to provision accounts and manage access:

[urn:mace:dir:attribute-def:eduPersonPrincipalName](#)

[urn:mace:dir:attribute-def:mail](#)

[urn:mace:dir:attribute-def:sn](#)

[urn:mace:dir:attribute-def:givenName](#)

The eduPersonPrincipalName is used as the primary key to uniquely identify the user account within MediaCore. This can be tokenized on the IdP side or can be the student's normal unique username within the IdP.

Optionally, an extra attribute can be released to automatically provision and update user Groups, Roles and Memberships within MediaCore:

[urn:mace:dir:attribute-def:eduPersonEntitlement](#)

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

The mail, sn, and givenName attributes are used in order to display which user (if any) is currently logged in; to identify the creator or editor of different resources within MediaCore; to facilitate activity audits by administrators; to facilitate the inspection of class engagement by instructors, and to notify users of relevant events that have occurred within the MediaCore system.

The optional eduPersonEntitlement attribute is used to automatically provision and update User Groups, Roles and Memberships which control the user's access to resources inside MediaCore. By releasing this extra attribute, the Identity Provider can greatly simplify user administration within MediaCore.

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

Yes. User accounts are provisioned and updated on a Just-In-Time basis and persist across sessions until removed by a site Administrator.

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

Yes. The following identifiable data elements may be recorded during a user session:

1. The SAML attributes listed above under 4.1.1.
2. which media items the user viewed
3. which pages the user viewed
4. what file(s) the users uploaded
5. the metadata the user added to their file uploads
6. the user groups and memberships of the user
7. the date/time/ip address of each new login
8. comments that the user posts on media items

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 customer access to the MediaCore platform is via a session whose permissions are scoped to the fine-grained user permissions defined by the current user's roles within the system. As a rule, it is up to the institution to define these roles.

Internal to MediaCore, support and senior technical personnel may also have access to customer account data.

- All personnel accessing customer data via the MediaCore web interfaces are required to login through our own 2-factor single-sign-on infrastructure in order to gain access. In addition all access is provided over HTTPS and is encrypted end-to-end.
- All personnel accessing server infrastructure are required to authenticate via SSH using a public/private key pair or via 2-factor authentication. Only a small subset of personnel is given access to these systems.

All personally identifiable data is stored securely in our primary Canadian datacentre: a hosting facility operated by Netelligent (<http://www.netelligent.ca/>) based in Montreal, Quebec, Canada. The facility is located within the Stock Exchange Tower of Montreal, a prestigious building with major tenants (ATA TMX center disaster recovery of the Federal Government). The facility is covered by a security camera network, and has security guards on-site 24/7/365. The premises are also controlled by access card reader system.

- 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?

The Identity Provider may assign certain users to have Administrator privileges either manually or by use of the eduPersonEntitlement attribute. Within MediaCore, Administrators will have access to the management interface and the Site Settings panel. This panel gives access to the User data as populated by the attributes the Identity Provider has released under 4.1.1 above. Administrators may manually assign other users to have similar Administrator privileges.

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

Our protocol is to assess the scope of the breach, begin rotating any keys that may have been compromised, and, as soon as possible, to notify our customers via their primary support contact (noted in our contract) with full details on the breach, and our ETA on resolution. Following the issue being resolved we conduct a post-mortem on how we can prevent the problem from happening in the future. We also will let you know if there are any immediate steps we require you to take, and will systematically follow up with our primary support contact on ensuring the resolution is implemented.

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.

[Shibboleth 2.4.3 \(dfsg-2ubuntu1\)](#)

5.1.2. What operating systems are the implementations on?

[Ubuntu 12.04](#)

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

[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.](#)