Participant Name: Royal Society of Chemistry

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

whether user-initiated session termination is supported, and how use with “public access sites” is protected.

N/A

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?

N/A

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?

N/A

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

N/A

3.4 Uses of Your Electronic Identity Credential System

3.4.1. Please identify typical classes of applications for which0.005 Tc 0.005 Tw 11.04 0 0 9.94rau1400 -1.15

4. Service Provider Information

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?

No attribute information referring to a specific person is requested or used.

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?

We don't see what personally identifiable information could be available to RSC staff. Access to our Shibboleth test and production servers is limited to our Web Ops team who have set procedures to making any changes to the data on these servers. Our Shib Production server is secured behind our firewall.

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

As we don't handle any, there is none to compromise. If there was a situation where this could happen, we would notify the IDP to notify its users.

---

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.

SP 2.5.3.0

5.1.2.