Participant Name: Evogh, Inc.

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: _____~~

~~2.1.2. Information below is accurate as of this date:~~
_____
_____

~~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?~~

_____
_____

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: Bob Koche

Title or role: Vice President of Business Development

Email address: bob.koche@evogh.com

Telephone: +1.408.250.0025

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?

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.

The SeeVogh Video Collaboration Service provides combined Video Conferencing and Document/Desktop sharing for all attendees in online meetings. Servers run in the Cloud, either public or private. Login is required only for the purpose of Creating meetings. In order to enable logins using Federated Authentication the attributes used would be: first name, last name, email, eppn, affiliation

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

The Attribute Information is used solely for the purpose of Account Creation in the SeeVogh Server(s). SeeVogh makes no other use of information provided through Federated Authentication Services. Only people who need to Create meetings require an Account in the SeeVogh System.

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

Yes. Once Created the Account remains active for future login to SeeVogh.

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

Email, first name, last name and affiliation are stored in the SeeVogh DB. Additionally, the following meeting information for registered users only is retained: meeting booking time, start and end times, the maximum number of attendees, the video resolution, the duration of the meeting. Meeting attendees other than the registered users are anonymous and no information is collected on these attendees.

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

No Attribute Information is shared with other services, nor with Partners.

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?

SeeVogh was architected to minimize the collection of personal information about the user community. The only data saved that is related to a registered user is the meeting name, configuration (size, quality, duration), start/stop times and number of attendees. Beyond that nothing from the meeting is saved. This protects everyone's privacy. The video reflector is located on the customer's network so further control and protection is available to the system administrator. The data that is collected is stored on a special database service provided by goDaddy.com where they have a service team that focuses on the integration of operating system, database and network security to assure a safe and reliable service. Additionally, the user's password is encrypted in the database so that administration staff can only access user data and not authentication information. GoDaddy's security policy and associated agreements related to their serives may be found at the following web address. http://www.godaddy.com/legal-agreements.aspx?ci=46445&otab=2

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?

Since the information that is stored is the registered user's name and a few meeting attributes (see above), there is limited exposure, as well as, limited interest in this data by nefarious individuals. That said the information is accessible to those limited few who have admin rights to this database. As stated previously this is a very small group at Evogh. This group is required to have the most complex password as required by our database service provider. Additionally, any additional admin accounts require the approval of the software development engineer and the CEO of the company. The creation of a new admin account generates a system message to all other admins at Evogh alerting them that a new admin account was created.

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

In the event of a security breach at the database hosting location Evogh will notify any users who's data may have been accessed along with System Administrators who have a relationship with those potentially compromised users. Fortunately, the data stored is minimal so the risk is only to registered users and then only the meeting names and meeting attributes associated with those meetings. Nothing used during the meeting such as content, videos, documents or attendee lists are collected or saved by SeeVogh thus reducing the impact of a privacy leak in such an unlikely event.

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.

Linux, CentOS 6.2, shibboleth (shibd) v 2.4.3, mod_ssl, openssl 1.0.0-fips, apache v 2.2.15. These versions will change with time as new releases become available.

5.1.2. What operating systems are the implementations on?

Linux, CentOS 6.2

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

SAML 1.1 – we don't support SAML 1.1

SAML 2.0 – we support 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?

Evogh, Inc. will work with CAF Participants to enable reasonable and responsible security procedures consistent with requirements and industry practice.