

INCOMMON FEDERATION: PARTICIPANT OPERATIONAL PRACTICES

1. Federation Participant Information

1.1 The InCommon Participant Operational Practices information below is for:

InCommon Participant organization name 9STAR RESEARCH, INC.

The information below is accurate as of this date June 29, 2006

1.2 Identity Management and/or Privacy information

Additional information about the Participant's identity management practices and/or privacy policy regarding personal information can be found on-line at the following location(s).

URL(s) For Privacy Policy, <http://www.protectnetwork.org/policies/privacy.html>. For Levels of Assurance, <http://www.protectnetwork.org/pn/loa> . For IdM practices <http://www.protectnetwork.org/policies/index.html> .

1.3 Contact information

The following person or office can answer questions about the Participant's identity management system or resource access management policy or practice.

Name ProtectNetwork IdM Office, 9STAR RESEARCH, INC.

Title or role _____

Email address support AT protectnetwork DOT org

Phone +1 (512) 322-5343 FAX +1 (512) 233-0655

2. Credential Provider Information

The most critical responsibility that a Credential Provider Participant has to the Federation is to provide trustworthy and accurate identity assertions.¹ It is important for a Resource Provider to know how your *electronic identity credentials* are issued and how reliable the information associated with a given credential (or person) is known.

Community

2.1 If you are a Credential Provider, how do you define the set of people who are eligible to receive an *electronic identity*? If exceptions to this definition are

¹ The documents "InCommon: Assertion Reliability" and "InCommon: Attribute Assertion Levels of Assurance" discuss how authentication policies and practices might affect the appropriate use of identity assertions you might make. See <http://www.incommonfederation.org/docs/policies/>

allowed, who must approve such an exception?

ProtectNetwork (a division of 9STAR Research, Inc.) is both a Registration Authority (RA) as well as a Credential Service Provider (CSP). ProtectNetwork provides SAML based Shibboleth identities to end-users at two different levels of assurance (LOA), namely 1 and 2. A detailed description of the credentialing process is available at <http://www.protectnetwork.org/policies/index.html> . Exceptions to the policy are managed by our IdM Office with approvals from the executive management and corporate legal counsel of the company.

- 2.2 “Member of Community”² is an assertion that might be offered to enable access to resources made available to individuals who participate in the primary mission of the university or organization. For example, this assertion might apply to anyone whose affiliation is “current student, faculty, or staff.”

What subset of persons registered in your identity management system would you identify as a “Member of Community” in Shibboleth identity assertions to other InCommon participants?

We currently do not support “Member of Community” attribute assertion in our ProtectNetwork Shibboleth IdP service.

Electronic Identity Credentials

- 2.3 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. For example, “Registrar’s Office for students; HR for faculty and staff.”

Shibboleth identities at the ProtectNetwork IdP site are handled by the Identity Management(IdM)Office at 9STAR RESEARCH, INC. The IdM Office leadership reports to the President of 9STAR RESEARCH, INC. The process of obtaining credentials is described in detail at <http://www.protectnetwork.org/policies/idmpractices.html> .

² “Member” is one possible value for eduPersonAffiliation as defined in the eduPerson schema. It is intended to include faculty, staff, student, and other persons with a basic set of privileges that go with membership in the university community (e.g., library privileges). “Member of Community” could be derived from other values in eduPersonAffiliation or assigned explicitly as “Member” in the electronic identity database. See <http://www.educause.edu/eduperson/>

- 2.4 What technologies are used for your electronic identity credentials (e.g. Kerberos, userID/password, PKI, ...) that may be used with InCommon actions? 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 credential) and recorded?

ProtectNetwork uses userID/password credentials for all its users that request Shibboleth ID's at LOA-1 and 2. UserID/passwords are created and managed according to recommendations outlined in <http://www.protectnetwork.org/policies/index.html>.

- 2.5 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 (i.e. "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:

We only transmit temporary passwords via email when the user forgets their password and has to reset their own password at the ProtectNetwork site. The users however are advised to log into their account at the ProtectNetwork website to create a new password of their choice which are not transmitted via email. The temporary passwords expire within 24 hours. Participants are encouraged to contact our ProtectNetwork IdM team with questions and concerns at any time. The team can be contacted anytime at the contact information provided earlier.

- 2.6 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 InCommon Resource 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.

The only SSO system we use is Shibboleth coupled with Tomcat's form-based authentication. Session timeouts are enforced and users can terminate their sessions by closing their browsers. All communication are encrypted with SSL/HTTPS.

- 2.7 Are your primary electronic identifiers for people, such as "net ID," eduPerson EPPN, 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 is there a hiatus between such reuse?

Yes, all electronic identifiers including EPPN, EPTID and uid are unique and permanently assigned to the first individual end-user who requests it. Our database retains record of all accounts provisioned and identifiers are never re-issued to anyone other than the person who

*they were originally assigned to. For further details,
<http://www.protectnetwork.org/policies/index.html>.*

Electronic Identity Database

- 2.8 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?

LOA-1 identities are issued automatically to anyone with a valid email account. LOA-2 identities are only issued after proper identity proofing is performed by our IdM Office. The process of obtaining credentials is described in detail at <http://www.protectnetwork.org/policies/idmpractices.html>.

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

Users' First and Last names, eduPersonPrincipalName and LOA attributes are provided to any Shibboleth Service Provider only after the end-user has been authenticated by the ProtectNetwork IdP servers. All other information about the end-user is kept private by the ProtectNetwork IdP.

Your Uses of Your Electronic Identity Credential System

- 2.10 Please identify typical classes of applications³ for which your electronic identity credentials are used within your own organization?

Horde for accessing Email, Calender, FileSharing, etc.

Grouper for accessing group membership information.

Signet for accessing privilege information.

Corporate Website and Portal with protected documents for customers, vendors and partners.

Attribute Assertions

Attributes are the information data elements in an attribute assertion you might make to another Federation participant concerning the identity of a person in your identity management system.

³ Please see http://www.incommonfederation.org/docs/benefits/incommon_usecases.html

2.11 Would you consider your attribute assertions to be reliable enough to:

control access to on-line information databases licensed to your organization?

be used to purchase goods or services for your organization?

enable access to personal information such as student loan status?

Privacy Policy

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.

2.12 What restrictions do you place on the use of attribute information that you might provide to other Federation participants?

Handling of end-user attributes by third party Shibboleth Service Providers is handled on a case by case basis by the ProtectNetwork IdM team with approval from the executive management and legal counsel of the company. We plan to require, by default and in good faith, such third parties and service providers, to always keep end-user attribute information confidential and use it only for the official business purposes that they are authorized to perform.

2.13 What policies govern the use of attribute information that you might release to other Federation participants? For example, is some information subject to FERPA or HIPAA restrictions?

See Section 2.12

3. Other Information

3.1 Technical Standards, Versions and Interoperability

Identify the version of Internet2 Shibboleth code release that you are using or, if not using the standard Shibboleth code, what version(s) of the SAML and SOAP and any other relevant standards you have implemented for this purpose.

Shibboleth IdP 1.3

3.2 Other Considerations

Are there any other considerations or information that you wish to make known to other Federation participants with whom you might interoperate, e.g., concern about the use of clear text passwords or responsibilities in case of a security breach involving identity information you may have provided?

Security incidents involving ProtectNetwork users and systems should be reported to the ProtectNetwork team at support AT protectnetwork DOT org.