Date: June 1, 2007

To: Kris Hafner

From: Bruce James

Subj: Certification of UCSD ERS

Kris, enclosed is another UCTrust Statement of Compliance, this time for San Diego Effort Reporting. If you would sign and file this agreement we will be in compliance with UC Trust requirements as a Service Provider for San Diego Effort Reporting.

We look like we’ll be live with SD in the next couple of weeks!

Bruce
Statement of Compliance

To:  Associate Vice President  
      Information Resources and Communications  
      University of California, Office of the President  
      1111 Franklin Street, 7th Floor  
      Oakland, CA 94607-5200  
      FAX: (510) 451-4340

The undersigned certify that [name or brief description of the Credential Provider or Resource Provider] **UC Effort Reporting System** complies with the policies, principles, and requirements of UCTrust, as described in **UCTrust University of California Identity Management Federation Service Description and Policies**.

The undersigned acknowledge that compliance with the policies, principles and requirements of UCTrust, as they may be amended, is subject to periodic inspection and audit. Failure to demonstrate ongoing compliance with such policies, principles and requirements in all material respects that is not resolved in a timely manner will result in the revocation of the provider’s participation in UCTrust.

The following information is included in this certification.

- Attached: A copy of the **InCommon Federation: Participant Operational Practices** statement that was provided when joining InCommon
- Contact information for the Credential Provider’s or Resource Provider’s help desk:
  - Organization Name: IR&C
  - E-mail: bruce.james@ucop.edu
  - Telephone Number: 510 987-0588
  - Fax Number: 510 763-5597
- The Uniform Resource Identifier (URI) that identifies this Credential Provider or Resource Provider within InCommon: [https://ers.ucop.edu/ucsd]

[Signature and Title, Credential Provider or Resource Provider] 6-1-07  
Date

[Signature and Title, Campus Chief Information Officer] 6-4-07  
Date

cc: Campus Controller
INCOMMON FEDERATION: PARTICIPANT OPERATIONAL PRACTICES

Participation in InCommon Federation ("Federation") enables the participant to use Shibboleth identity attribute sharing technologies to manage access to on-line resources that can be made available to the InCommon community. One goal of the Federation is to develop, over time, community standards for such cooperating organizations to ensure that shared attribute assertions are sufficiently robust and trustworthy to manage access to important protected resources. As the community of trust evolves, the Federation expects that participants eventually should be able to trust each other's identity management systems and resource access management systems as they trust their own.

A fundamental expectation of InCommon Participants is that they provide authoritative and accurate attribute assertions to other participants and that participants receiving an attribute assertion protect it and respect privacy constraints placed on it by the Federation or the source of that information. In furtherance of this goal, InCommon requires that each participant make available to other participants certain basic information about any identity management system, including the identity attributes that are supported, or resource access management system that they register for use within the Federation.

Two criteria for trustworthy attribute assertions by Credential Providers are: (1) that the identity management system fall under the purview of the organization’s executive or business management, and (2) the system for issuing end-user credentials (e.g. PKI certificates, userids/passwords, Kerberos principals, etc.) specifically have in place appropriate risk management measures (for example authentication and authorization standards, security practices, risk assessment, change management controls, audit trails, etc.).

InCommon expects that Resource Providers, who receive attribute assertions from another organization, respect the other organization's policies, rules and standards regarding the protection and use of that data. Furthermore, such information should be used only for the purposes for which it was provided. InCommon strongly discourages the sharing of that data with third parties, or aggregation of it for marketing purposes without the explicit permission\(^1\) of the identity information provider.

\(^1\) Such permission already might be implied by existing contractual agreements.

Federation Overview

InCommon\(^{TM}\) Federation
c/o Internet2
1000 Oakbrook Drive, Suite 300
Ann Arbor MI 48104
1. Federation Participant Information

1.1 The InCommon Participant Operational Practices information below is for:

InCommon Participant organization name  **UC Office of the President (UCOP)**

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)  **http://www.ucop.edu/irc/itlc/uctrust/**

**https://atyourserviceonline.ucop.edu/ayso/html/ayso_privacy_policy.htm**

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  **Mr. David Walker**

Title or role  **Director, Advanced Technologies**

Email address  **david.walker@ucop.edu**

Phone  **(510) 987-0500**      FAX  **(510) 839-2623**

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. 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 allowed, who must approve such an exception?

**N/A (UCOP is currently a Resource Provider only).**

---

3 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/

InCommon™ Federation
c/o Internet2
1000 Oakbrook Drive, Suite 300
Ann Arbor MI 48104
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.

\[N/A \text{ (UCOP is currently a Resource Provider only).}\]

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?

\[N/A \text{ (UCOP is currently a Resource Provider only).}\]

**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?

\[N/A \text{ (UCOP is currently a Resource Provider only).}\]

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

\[N/A \text{ (UCOP is currently a Resource Provider only).}\]

**Your Uses of Your Electronic Identity Credential System**

2.10 Please identify typical classes of applications\(^5\) for which your electronic identity credentials are used within your own organization?

\[N/A \text{ (UCOP is currently a Resource Provider only).}\]

**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.

---

\(^5\) Please see [http://www.incommonfederation.org/docs/benefits/incommon_usecases.html](http://www.incommonfederation.org/docs/benefits/incommon_usecases.html)
3.3 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?

*Information is exchanged via a secure https connection, and only non-identifiable information is transferred, such as a UC Net ID. No publicly usable identification is exchanged. Further information regarding access control and policy may be found at www.ucop.edu/ucophome/policies/bfb/is3.pdf*

3.4 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 Resource Provider application does not support “super user” or privileged accounts for administrative access. To support this function, there exists administrative applications accessible via separate (private) secured access (HTTPS) URL’s. Access to these applications is through the use of login/password accounts that are issued on an individual, need-to-have basis. All accounts are tracked in a local database. Further information regarding access control and policy may be found at www.ucop.edu/ucophome/policies/bfb/is3.pdf*

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

*Refer to the following URL: http://www.ucop.edu/irc/itsec/securitybreach.html*

4. Other Information

4.1 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 version 1.3*

4.2 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?

*None.*
[1.3] Other InCommon Participants may wish to contact this person or office with further questions about the information you have provided or if they wish to establish a more formal relationship with your organization regarding resource sharing.

[2] Many organizations have very informal processes for issuing electronic credentials. For example, one campus does this through their student bookstore. A Resource Provider may be more willing to accept your assertions to the extent that this process can be seen as authoritative.

[2.1] It is important for a Resource Provider to have some idea of the community whose identities you may represent. This is particularly true for assertions such as the eduPerson “Member of Community” or “student,” etc. A typical definition might be “Faculty, staff, and active students” but it might also include alumni, prospective students, temporary employees, visiting scholars, etc. In addition, there may be formal or informal mechanisms for making exceptions to this definition, e.g. to accommodate a former student still finishing a thesis or an unpaid volunteer.

This question asks to whom you, as a Credential Provider, will provide electronic credentials. This is typically broadly defined so that the organization can accommodate a wide variety of applications locally. The reason this question is important is to distinguish between the set of people who might have a credential that you issue and the subset of those people who fall within your definition of “Member of Community” for the purpose of InCommon attribute assertions.

[2.2] The assertion of “Member of Community” is often good enough for deciding whether to grant access to basic on-line resources, e.g. library-like materials or websites. InCommon encourages participants to use this assertion only for “Faculty, Staff, and active Students” but some organizations may have the need to define this differently. InCommon Resource Providers need to know if has been defined differently.

[2.3] For example, if there is a campus recognized office of record that issues such electronic credentials and that office makes use of strong, reliable technology and good database management practices, those factors might indicate highly reliable credentials and hence trustworthy identity assertions.

[2.4] Different technologies carry different inherent risks. For example, a userID and password can be shared or “stolen” rather easily. A PKI credential or SecureID
[2.10] In order to help a Resource Provider assess how reliable your identity assertions may be, it is helpful to know how your organization uses those same assertions. The assumption here is that you are or will use the same identity management system for your own applications as you are using for InCommon purposes.

[2.11] Your answer to this question indicates the degree of confidence you have in the accuracy of your identity assertions.

[2.12] Even “public information” may be constrained in how it can be used. For example, creating a marketing email list by “harvesting” email addresses from a campus directory web site may be considered illicit use of that information. Please indicate what restrictions you place on information you make available to others.

[2.13] Please indicate what legal or other external constraints there may be on information you make available to others.

[3.1] Please identify your access management requirements to help other Participants understand and plan for use of your resource(s). You might also or instead provide contact information for an office or person who could answer inquiries.

[3.2] As a Resource Provider, please declare what use(s) you would make of attribute information you receive.

[3.3] Personally identifying information can be a wide variety of things, not merely a name or credit card number. All information other than large group identity, e.g. “member of community,” should be protected while resident on your site.

[3.4] Certain functional positions can have extraordinary privileges with respect to information on your systems. What oversight means are in place to ensure incumbents do not misuse such privileges?

[3.5] Occasionally protections break down and information is compromised. Some states have laws requiring notification of affected individuals. What legal and/or institutional policies govern notification of individuals if information you hold is compromised?

[4.1] Most InCommon Participants will use Internet2 Shibboleth technology but this is not required. It may be important for other participants to understand whether you are using other implementations of the technology standards.
Glossary

access management system

The collection of systems and or services associated with specific online resources and/or services that together derive the decision about whether to allow a given individual to gain access to those resources or make use of those services.

assertion

The identity information provided by a Credential Provider to a Resource Provider.

attribute

A single piece of information associated with an electronic identity database record. Some attributes are general; others are personal. Some subset of all attributes defines a unique individual.

authentication

The process by which a person verifies or confirms their association with an electronic identifier. For example, entering a password that is associated with an UserID or account name is assumed to verify that the user is the person to whom the UserID was issued.

authorization

The process of determining whether a specific person should be allowed to gain access to an application or function, or to make use of a resource. The resource manager then makes the access control decision, which also may take into account other factors such as time of day, location of the user, and/or load on the resource system.

Credential Provider

A campus or other organization that manages and operates an identity management system and offers information about members of its community to other InCommon participants.

electronic identifier

A string of characters or structured data that may be used to reference an electronic identity. Examples include an email address, a user account name, a Kerberos principal name, a UC or campus NetID, an employee or student ID, or a PKI certificate.

electronic identity

A set of information that is maintained about an individual, typically in campus electronic identity databases. May include roles and privileges as well as personal information. The information must be authoritative to the applications for which it will be used.

electronic identity credential

An electronic identifier and corresponding personal secret associated with an electronic identity. An electronic identity credential typically is issued to the person who is the subject of the information to enable that person to gain access to applications or other resources that need to control such access.

electronic identity

A structured collection of information pertaining to a given individual. Sometimes referred to as an "enterprise directory."
<table>
<thead>
<tr>
<th>Term</th>
<th>Definition</th>
</tr>
</thead>
<tbody>
<tr>
<td>identity</td>
<td><em>Identity</em> is the set of information associated with a specific physical person or other entity. Typically a Credential Provider will be authoritative for only a subset of a person’s identity information. What identity attributes might be relevant in any situation depend on the context in which it is being questioned.</td>
</tr>
<tr>
<td>identity management system</td>
<td>A set of standards, procedures and technologies that provide electronic credentials to individuals and maintain authoritative information about the holders of those credentials.</td>
</tr>
<tr>
<td>NetID</td>
<td>An electronic identifier created specifically for use with on-line applications. It is often an integer and typically has no other meaning.</td>
</tr>
<tr>
<td>personal secret (also verification token)</td>
<td>Used in the context of this document, is synonymous with password, pass phrase or PIN. It enables the holder of an electronic identifier to confirm that s/he is the person to whom the identifier was issued.</td>
</tr>
<tr>
<td>Resource Provider</td>
<td>A campus or other organization that makes on-line resources available to users based in part on information about them that it receives from other InCommon participants.</td>
</tr>
</tbody>
</table>
Job: 140
Date: 5/31/2007
Time: 9:25:14 PM