

# **INCOMMON FEDERATION: FEDERATION OPERATING PRACTICES AND PROCEDURES**

October 10, 2004

This document describes at a high level how the InCommon Federation (“Federation”) support organization is structured and how it operates in accordance with the InCommon, LLC Operating Agreement. Specific details and logistics are left to the discretion of the InCommon Operations Manager (“OM”).

InCommon Participants should review this document to help assess what potential risks, if any, might be incurred by their participation in the Federation. Please see Appendix A for further discussion of areas where risk might be a factor. Please contact the Federation office for clarification or additional information.

## **1 Role of the InCommon Federation Organization**

The Overview of the InCommon Federation (“Overview”) defines the mission of the Federation and the principles and governance structure under which the Federation operates. The Overview also outlines the general activities undertaken by the Federation on behalf of its Participants.

The administrative and operational functions of the Federation are carried out by the OM in accordance with the LLC Operating Agreement. These responsibilities include development of the Federation Participant community, processing applications and Participant metadata, overseeing operation of certain Federation service platforms, and other duties as assigned by the InCommon Steering Committee or the officers of InCommon, LLC.

## **2 Management Structure**

Responsibility for management of the business and affairs of the LLC are vested with the InCommon Steering Committee (“Steering Committee”). Specific authority may be delegated by the Steering Committee to the OM.

The Steering Committee approves the Federation Operating Practices and Procedures (FOPP) document and ensures that it accurately reflects how the Federation operates. Any changes to this FOPP will be communicated directly to each Participant within 15 business days of the change going into effect.

## **3 Organizational Structure**

### **3.1 Offices and Records**

The Federation office postal and email addresses and telephone number are:

InCommon Federation Organization

c/o Internet2  
1000 Oakbrook Dr, Suite 300  
Ann Arbor, MI 48104  
Email address: [incommon-admin@incommonfederation.org](mailto:incommon-admin@incommonfederation.org)  
Telephone: 734-913-4250

All records of the Federation are kept at this location.

### **3.2 Personnel**

The InCommon LLC consists of at least two officers: the Operations Manager and the Secretary. Other officers may be appointed by the Steering Committee. The OM will provide guidelines and direction for the operational aspects of the Federation which will be carried out by Internet2.

Internet2 will hire and manage personnel who will provide administrative, communications, and operational support to the OM.

### **3.3 Advisory Committees**

The Steering Committee may designate Committees to develop position papers and/or provide advice on particular matters of importance to the Federation. At least one member of the Steering Committee will participate in each Advisory Committee to ensure good communication between the Committee and the Steering Committee. Additional membership in such committees will be defined by the Steering Committee and typically will be drawn from the Participant community. Other individuals may be asked to participate based on their particular knowledge of the subject matter.

Two advisory committees exist currently.

#### **3.3.1 Communication, Membership, Pricing and Packaging (CMPP) Committee**

The InCommon Federation CMPP Committee advises the Steering Committee on issues such as which organizations might be accepted as members of the Federation, what fee structure might apply to various classes of members, and how best to communicate with members about activities of the Federation.

#### **3.3.2 Policy Committee**

The InCommon Federation Policy Committee advises the Steering Committee on matters of Federation principles and practices. Its recommendations will reflect the wishes of Participants with regard to strengthening the trust fabric of the Federation, developing standards for evaluating levels of assurance among Credential Providers, and arbitrating differences in the trust needs of Participants.

### **3.4 Meetings**

The Steering Committee meets no less frequently than once per year, typically by conference call. Minutes are kept of the Steering Committee meetings and, except for sensitive matters involving personnel, are available to Federation Participants for review and comment.

Advisory Committees meet as needed, typically by conference call. Minutes need

not be kept. The work product(s) of Advisory Committees are provided to the Steering Committee and made available to Federation Participants unless they involve sensitive personnel matters.

#### **4 Policies, Requirements and Standards**

The Steering Committee approves all policies, requirements and standards that apply to the InCommon Federation Organization and/or Participants. Current governing documents, available from the Federation office above and on the website, include:

- Overview of the InCommon Federation
- InCommon Federation: Federation Operating Practices and Procedures (this document)
- InCommon Federation: Participant Agreement
- InCommon Federation: Common Identity Attributes
- InCommon Federation: Participant Operating Practices

Advisory documents and other white papers may be made available on the Federation web site: <http://www.incommonfederation.org/>.

#### **5 Participant Applications**

Organizations that wish to participate in the InCommon Federation must complete a Participation Application. Potential Participants should review the Participation Agreement and any other Federation documents that may be required in order to evaluate the potential risks and rewards of participation.

##### **5.1 Who can apply**

Currently any 2- or 4-year degree-granting institution of higher education that is regionally accredited by an agency on the U.S. Department of Education's list of Regional Institutional Accrediting Agencies may apply for Participation as a Higher Education Institution.

Any organization may apply as a Sponsored Partner but must submit with its application a letter of endorsement from an InCommon Higher Education participant. This requirement is intended to ensure that Sponsored Partners are of value to the Federation's higher education community.

##### **5.2 Submitting an Application**

The Application must be accessed online, on the InCommon Federation website, completed, and submitted with the required payment of the application fee by credit card. The Federation office may request additional information concerning the nature or qualifications of the applicant organization. The Federation office also might request a statement on letterhead identifying the official(s) of the organization eligible to enter into legally binding contractual agreements.

Other procedures will be developed as additional types of classes of organizations

are made eligible for Participation.

### **5.3 Approving an applicant**

Questions of eligibility arising out of the processing of applications will be referred to the OM. The OM will determine when to refer the application to the Steering Committee. If there are ambiguities, or if the Steering Committee so directs, the application may be submitted to the Membership Committee (CMPP) for advice.

The Steering Committee may request additional information from or discussion with the applicant. If the Steering Committee approves the applicant, the OM will continue with the application processing. In the case that neither the Steering Committee nor OM approves an applicant, the OM will notify the applicant of the rejection in a timely manner.

Finally, the applicant will be approved for participation when a paper copy of the signed, executed Participation Agreement has been received by the InCommon office. In the case of a Sponsored Partner applicant, an additional sponsorship note must be received from an InCommon Higher Education Institution participant, either by email or postal mail.

### **5.4 Applicant's acceptance**

Once accepted for participation, the applicant will be invoiced any required fees and will submit a list of the second level Internet domain names (e.g., berkeley.edu) under which their management systems will be registered. The Participant will also be given, via postal mail or by telephone, a unique userid and password, which will be used to register identity management systems and/or resource provider IDs. This userid/password pair should not be shared; additional credentials can be provided if necessary.

### **5.5 Renewal**

Renewal of Participation is automatic as long as the Participant remains in good standing and pays their Annual Participation Fees in a timely manner. All identity management and resource management registrations are maintained as long as the Participant is in good standing.

### **5.6 Termination**

Participant can withdraw from the Federation at any time upon written notice to the Federation office. In addition, the Steering Committee may terminate any organization's participation if it determines that that Participant is no longer qualified or has failed to observe its commitments to the Federation.

When a Participant leaves the Federation, all registrations of identity management systems and resource provider IDs are removed from the metadata but not deleted from our records. No other organization will be able to use those identifiers without the explicit written authorization of the organization with which they were previously associated.

## **6 Registration of Identity Management and Resource Provider Systems**

Participants can register identity management systems and/or resource provider systems on-line using the credentials issued by InCommon to the Administrative Contact. Higher Education Institutions and Sponsored Partners receive an initial quota for each system type and can purchase more if needed, subject to certain restrictions.

### **6.1 Required Relationship to Participant**

Any identity management system or resource provider system registered by a Participant must be under the management hierarchy of Participant's organization. Participant is responsible for the actions of any system registered under their Participation Agreement. Participant may not register third party systems.

University systems or distributed corporations where each campus or business unit is only loosely managed by the parent organization are expected to require each campus or business unit to become a separate Participant in the InCommon Federation. One factor in determining whether this applies is whether there is a single identity management system serving all campuses in the university system or all locations of the distributed corporation. Each major location that operates its own identity management system or independently manages access to its own resources should join the InCommon Federation as a Participant. Ultimately, the decision will reside with your Executive Liaison, who will be contacted during the application process.

### **6.2 Required Information**

Each system registered must be described in a Participant Operating Practices (POP) statement. In some cases, multiple systems can be described in one POP. In either case, the URL for the POP must be submitted to the InCommon Federation during the application process.

Each registration must include PKI certificate signing requests (CSRs) for the Handle Service and the Attribute Authority, which will be used in issuing the InCommon certificates.

## **7 Routine Operations**

In addition to the above functions and responsibilities, the Federation shall support certain operational services, including:

### **7.1 Communication and Outreach**

All Federation operating documents, Participant Operating Practices statements, and the minutes of the Steering Committee meetings shall be posted to a website maintained by the Federation.

Participants are required to submit to the Federation, within 14 days of any substantive change, a new copy of their Participant Operating Practices statement. Within 2 working days, the Federation will notify the Participants of the existence of

the revised/new statement.

## **7.2 Metadata distribution and other trusted electronic communications**

All communication of trusted information concerning an identity management system or resource provider system **must** be digitally signed using the certificates issued as a result of system registration.

## **7.3 InCommon Federation Technical Infrastructure**

The Federation is responsible for operation of a number of technology platforms including a Web server, a WAYF server, and a certificate authority (CA). Operation of the technical infrastructure is described generally in the following documents, which are available on the InCommon website:

- Internet2\_InCommon\_Federation\_Infrastructure\_Technical\_Reference
- Internet2\_InCommon\_Technical\_Operations\_steps
- Internet2\_InCommon\_Technical\_Operation\_Hours
- InCommon\_Federation\_Disaster\_Recovery\_Procedures

## **7.4 Operation of the InCommon CA**

The Federation operates its own x.509 certificate authority (CA) from which it issues “server certificates” for use within the Federation. Details of InCommon CA operation are available in the following documents, available on the InCommon website:

- Internet2\_InCommon\_CA\_PKI-Lite\_CP
- Internet2\_InCommon\_CA\_PKI-Lite\_CPS
- Internet2\_InCommon\_Certificate\_Authority\_for\_the\_InCommon\_Federation\_System\_Technical\_Reference
- InCommon\_CA\_Audit\_Log
- CA\_Disaster\_Recovery\_Procedure
- Internet2\_InCommon\_CA\_Disaster\_Recovery\_from\_root\_key\_compromise

## **7.5 Operation of the InCommon WAYF servers**

The Federation operates a redundant WAYF server in which all Credential Providers are listed. This does not preclude a Resource Provider from operating their own WAYF server listing only those Credential Providers with which it has an operating agreement.

Operation of the Federation WAYF is described in the Technical Infrastructure documents listed above.

## **7.6 Dispute Resolution procedure**

Should disputes regarding Federation services or the use of those services arise among Participants or between a Participant and the Federation, the following

procedure should be used to come to resolution. This procedure will evolve as the Federation gains more experience with the types of disputes that may occur.

Upon resolution, a brief description of the dispute issues and the resolution of those will be posted to the members-only section of the Federation website.

#### 7.6.1 Disputes Among Participants

Participants should make every reasonable effort to settle disputes among themselves, especially if contractual issues are involved. If circumstances warrant, for example, the dispute centers on the interpretation of Attribute values, or the implementation of standards, then the Federation may be asked to act as referee in helping the Participants come to resolution.

The OM will serve as the Referee in working with Participants. The Referee will gather as much information as possible from each disputing party and then, if necessary, ask for additional information or advice from the Federation staff or advisors. The Referee then will offer a proposed solution to the disputing parties.

If this process fails to reach consensus among the parties, then the dispute may be escalated to a Dispute Between Participant(s) and the Federation.

#### 7.6.2 Disputes Between Participant(s) and the Federation

Any Participant may submit a written Notice of Dispute to the OM regarding any aspect of the operation or services supported by the Federation. The OM will make certain that sufficient information exists to define the dispute and then shall inform the Chair of the Steering Committee. The Chair will appoint one of the Steering Committee Members to serve as Negotiator with the disputing party(s).

The Negotiator will gather all the facts and rationales for the dispute and, as necessary, seek advice from the Federation advisors and/or other relevant parties. The Negotiator will prepare a written report, which shall include a recommended resolution of the dispute. The report shall be submitted to the Chair of the Steering Committee within 30 days of the appointment of the Negotiator unless delayed by the required fact finding.

The Chair shall bring the report to a quorum of the Steering Committee. The Committee may ask for additional information or a modified recommendation after reviewing the report. Resolution of the dispute must be approved by affirmative vote of a quorum of the Steering Committee as defined in the Federation Charter. If the Steering Committee is unable to affirm a resolution, the status quo is maintained. The OM shall report the Steering Committee's action to the disputing party(s) in writing as soon thereafter as practical. If any disputing party believes it cannot accept the outcome of this process, its only recourse would be to discontinue participation in the Federation.



## **Appendix A: Risk Assessment of the InCommon Federation Organization**

Participants in the Federation place a certain amount of trust in the Federation Organization to perform correctly and reliably the support functions that it provides. It is also the case that Participants place a great deal of trust in each other as the source of attribute information or a trusted repository of subject information. In some cases, mitigation of Participant-to-Participant risk will require explicit agreements or contracts. The discussion below highlights some of the ways in which operation of the Federation might incur risk to Participants and what measures might be taken to mitigate those risks.

### **1. Misrepresentation by a Participant organization**

The Federation depends upon organizations to identify individuals who are empowered to represent the legal and business interests of the organization. The signatory to the Participant Agreement is assumed to be such a person, and the Federation assumes that this signatory can represent the management of identity services and resource managers within the same organization.

Vetting of these relationships is relatively weak at the current time (see above). If a Participant provides incorrect information to the Federation, and another Participant relies on that information, (e.g., the commitment to abide by Federation rules and the Participant Agreement) and something goes wrong, the relying party may not be able to recover damages.

### **2. Incorrect or corrupted metadata**

Participants provide their own metadata to the Federation, but the Federation must aggregate that information and provide it reliably and accurately to all other Participants. There is a very small and remote chance that such information might become corrupted or misplaced in the process of relaying it to Federation Participants. This might result in incorrect attribute release to Resource Providers or the inability of a potential user to be redirected to an appropriate Attribute Authority (identity management system).

### **3. Incorrect public key for Participant**

The Federation issues two key pairs to each service platform registered by Participants. This enables rapid switchover to a second key pair in case the first becomes compromised. In this case, the Participant must notify the Federation and it will update the metadata to reflect the different public key.

Distribution of this revised metadata might be delayed or even mis-configured. This would cause temporary loss of functionality for the affected Participant.

### **4. Mis-configuration or malfunction of the InCommon WAYF**

The InCommon WAYF is a critical component of the Shibboleth service. It has been

designed for high availability but its database might be accidentally corrupted or inconsistent among the redundant platforms. This would cause temporary inconvenience for users who might not be able to find their Credential Provider or might be redirected to an incorrect Credential Provider.

5. Failure to notify Participants of changes in the FOPP or in Participants' POPs

The Federation Operational Practices and Procedures statement and the Participant Operational Practices statements form the basis, in part, of trust among Federation Participants. The Federation has a critical role in ensuring that these statements are available to all Participants and are correct and current. Failure to do so might inadvertently cause a relying party to make a decision about trust in another party that it would not have otherwise made.

Great care has gone into the development and implementation of the operational processes which are described in the technical documents (see 7.3 and 7.4). However, a number of functions of the initial Federation may not be as robust as some potential applications require. The Federation is committed to improving all of its services to Participants as it learns more about the actual operation and needs of the Federation.