

**INCOMMON FEDERATION:
FEDERATION OPERATING POLICIES AND PRACTICES
2007 October 15**

Table of Contents

1	ROLE OF THE INCOMMON FEDERATION ORGANIZATION	2
2	ORGANIZATIONAL STRUCTURE	2
2.1	MANAGEMENT	2
2.2	COMMITTEES	2
2.3	MEETINGS	3
2.4	OFFICES AND RECORDS	3
2.5	PERSONNEL	3
3	POLICIES, REQUIREMENTS, AND STANDARDS	3
4	APPLICATION FOR PARTICIPATION IN INCOMMON	4
4.1	ELIGIBILITY CRITERIA	4
4.2	SUBMITTING AN APPLICATION	5
4.3	APPROVING AN APPLICANT	5
5	PARTICIPATION FEES	5
6	REGISTRATION: IDENTIFICATION AND AUTHENTICATION OF TRUSTED OFFICERS	5
7	REGISTRATION AND MANAGEMENT OF PARTICIPANT POLICIES, SYSTEMS, AND TECHNICAL COMPONENTS	5
7.1	TYPES OF REGISTERED SYSTEMS: IDENTITY PROVIDERS AND SERVICE PROVIDERS	5
7.2	RELATIONSHIP OF SYSTEMS TO PARTICIPANT	6
7.3	REQUIRED INFORMATION COMPONENTS	6
7.3.1	<i>Participant Operating Practices</i>	6
7.3.2	<i>Metadata</i>	6
7.3.3	<i>Digital Certificates for Federation Participant service platforms</i>	7
7.3.3.1	Signing	7
7.3.3.2	Expiration	7
7.3.3.3	Revocation	7
8	DISPUTE RESOLUTION PROCEDURE	7
8.1	DISPUTES AMONG PARTICIPANTS	7
8.2	DISPUTES BETWEEN PARTICIPANT(S) AND THE FEDERATION	7
9	OPERATIONS	8
9.1	OPERATIONAL ASSURANCE LEVEL	8
9.2	COMMUNICATIONS AND SUPPORT	8
9.3	FEDERATION TECHNICAL INFRASTRUCTURE	9
9.3.1	<i>Where Are You From (WAYF)</i>	9
9.3.2	<i>Metadata Distribution</i>	9
9.3.3	<i>Participant Administrative Interface</i>	9
9.3.4	<i>Certification Authority (CA)</i>	9
9.3.5	<i>Suspension of Federation Services</i>	9
9.4	DISASTER RECOVERY	10
10	PARTICIPATION STATUS: RENEWAL, WITHDRAWAL AND TERMINATION, AND SUSPENSION	10
10.1	RENEWAL	10
10.2	WITHDRAWAL AND TERMINATION	10
10.3	SUSPENSION OF PARTICIPANTS' SERVICES	10
11	FURTHER RISK ASSESSMENT	10

This document describes at a high level how the InCommon support organization is structured and how it operates in accordance with the Limited Liability Company Agreement of InCommon ("Company Agreement") and Bylaws of the InCommon LLC ("Bylaws") to support the entire InCommon Federation ("Federation"). Specific details and logistics are left to the discretion of the InCommon Operations Manager ("OM").

InCommon Federation Participants ("Participants") should review this document to help assess what potential risks, if any, might be incurred by their participation in the Federation. By reviewing the policies and practices of the Federation, Participants and potential participants can evaluate the level of assurance of the Federation's services to ensure trustworthy operations and determine whether they meet a Participant's minimum requirements. Complete evaluation of the entire Federation's infrastructure and level of assurance is out of scope for this document and would need to include evaluation of all relevant Participants' policies and practices. Please contact the InCommon office for clarification or additional information regarding this document or other Federation matters.

1 Role of the InCommon Federation Organization

The InCommon, LLC Bylaws define the mission of InCommon and its Federation and the principles and governance structure under which the Federation operates. This Federation Operating Policies and Practices document (FOPP) outlines the activities undertaken by InCommon on behalf of its Federation Participants.

The administrative and operational functions of InCommon are carried out under direction of the OM in accordance with the Company Agreement. These responsibilities include development of the Federation participant community, processing applications, identifying and authenticating eligible organizations and their trusted officers, processing participant metadata, overseeing the operation of InCommon service platforms, dispute resolution, termination processes, accounting and billing, and other duties as assigned by the InCommon Steering Committee or the officers of the InCommon LLC.

2 Organizational Structure

2.1 Management

Responsibility for management of the business and affairs of the InCommon LLC is vested with the InCommon Steering Committee ("Steering Committee") as described in the Company Agreement. Specific authority may be delegated by the Steering Committee to appointed subcommittees of the Steering Committee or the OM.

The Steering Committee approves this FOPP as an accurate reflection of InCommon Federation operations. Any change to this FOPP will be communicated to each Participant Administrator via email within 15 business days of the change being approved by the Steering Committee.

2.2 Committees

The Steering Committee may designate subordinate or advisory committees to make decisions, develop position papers, and/or provide advice on particular matters of importance to the Federation as outlined in the Bylaws. 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. Other committees may be formed as detailed in the Bylaws. Current committees are listed on the InCommon website.

2.3 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 confidential personnel or financial matters, are available to Federation Participants upon request.

Advisory and other committees meet as needed, typically by conference call. Minutes need not be kept.

2.4 Offices and Records

The InCommon Federation office's contact information is:

InCommon
c/o Internet2
1000 Oakbrook Dr, Suite 300
Ann Arbor, MI 48104
Email address: incommon-admin@incommonfederation.org
Telephone: 734-913-4250
Website: <http://www.incommonfederation.org>

All records of InCommon are managed by this office.

2.5 Personnel

The InCommon LLC minimally requires 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's support organization. Operational functions are staffed and performed by Internet2.

Internet2 hires and manages personnel who provide legal, administrative, communications, operational, and other support to the OM.

3 Policies, Requirements, and Standards

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

- Limited Liability Company Agreement of InCommon
- Bylaws of the InCommon LLC
- InCommon Federation: Federation Operating Policies and Practices (this document)

- InCommon Federation: Participation Agreement
- InCommon Federation: Common Identity Attributes
- InCommon Federation: Participant Operational Practices

Additional documents, guidelines, and other papers are also available on the InCommon website.

4 Application for Participation in InCommon

Organizations that wish to participate in the InCommon Federation must be eligible under the requirements defined below.

4.1 Eligibility Criteria

The InCommon Federation currently has two classes of participants: (1) Higher Education (accredited post-secondary institutions and their central offices) and (2) their Sponsored Partners.

To qualify in the first category, an organization must be:

- A two- or four-year degree-granting institution that is accredited by an agency on the U.S. Department of Education's list of recognized Regional Accrediting Agencies as listed on the InCommon website (URL found in section 2.4); or
- A state higher education system office or other central coordinating office which either governs or manages a collection of accredited, degree-granting institutions. The entity must be commissioned, established, or recognized by a local, state, or national government to perform this activity or must be a cooperative venture organized by and for the benefit of higher education institutions for the above purposes. Documentation substantiating these criteria may be required, and determinations will be made on a case by case basis.

A Sponsored Partner is any entity that is sponsored for participation in the Federation by a participating category 1 organization. A Sponsored Partner typically provides online resources, research data, informational, or other services to the sponsoring higher education organization. A sponsorship letter must be received by InCommon from the sponsoring category 1 Participant's designated Executive, either by email or postal mail. For details see the InCommon website.

The InCommon Steering committee may choose to set eligibility criteria for additional types of organizations or may vote on the approval of any applying organization under special circumstances (see 4.3).

Distributed university or corporate systems are expected to require independent universities or businesses to become separate Participants in the InCommon Federation. Examples of such distributed systems include state-wide university systems and large conglomerate corporations where each university or business unit is authorized to commit to and enter into legal agreements on behalf of its own organizational entity. Federations and other complex membership systems will be eligible for InCommon Federation participation on a case by case basis.

4.2 Submitting an Application

Interested organizations may apply for participation by submitting an online application or by submitting a signed Participation Agreement for review. InCommon may request additional information concerning the nature or qualifications of the applying organization.

4.3 Approving an Applicant

Any eligibility questions will be referred to the OM. The OM will determine if the application requires Steering Committee approval.

The Steering Committee may request that additional information be supplied by the applicant. If the Steering Committee deems the applicant eligible, the OM will continue with application processing. In the case that neither the OM nor the Steering Committee approves an applicant, InCommon will notify the applicant of this result in a timely manner.

The applicant will be accepted for participation when two original, signed copies of the Participation Agreement have been received by the InCommon office and have been countersigned by InCommon.

5 Participation Fees

InCommon fees are established by the Steering Committee on a cost-recovery basis and reviewed annually. The Registration fee covers the cost of determining the eligibility of the applicant and the identification and authentication of its trusted officers. Payment by credit card is due upon submission. Annual Participation fees are invoiced, based on a calendar year from January 1 to December 31, and are not prorated. No fees are refundable. The current fee schedule is available on the InCommon website.

6 Registration: Identification and Authentication of Trusted Officers

InCommon verifies the identity of all individuals who fill the Participant's trusted roles of Executive and Administrator (see the InCommon online Glossary for definitions). By constructing an independently verifiable, out-of-band communication path with these officers, the Registration Authority establishes a relatively strong level of assurance that the person is who he or she declares. Details on the registry process are available on the InCommon website.

7 Registration and Management of Participant Policies, Systems, and Technical Components

The Participant's trusted Administrator will be given credentials to manage Federation Participant data and requests in a secure manner.

7.1 Types of Registered Systems: Identity Providers and Service Providers

Within the Federation, both classes of participants may offer services as Identity Provider for its user community, Service Provider to a participant organization's user community, or both. For instance, a Higher Education Institution serving primarily as an Identity Provider might also make online information or services available to

other InCommon participants. Likewise, a Sponsored Partner that is primarily a provider of online services also might act as an Identity Provider.

Participants register identity management systems and/or service provider systems using the InCommon participant administrative interface. Higher Education Institutions and Sponsored Partners receive an initial quota for each system type and can purchase more as needed, subject to certain restrictions, as outlined in the Participation Agreement and Fee Schedule available on the InCommon website.

7.2 Relationship of Systems to Participant

Any identity management system or service provider system registered by a Participant must be under the management hierarchy of the Participant organization. The Participant is responsible for the actions of any system registered with the Federation. Participants may only register third party systems that operate services under contract to Participant and for which Participant will be responsible, in accordance with the provisions of the Participation Agreement. Such third party systems might, for example, include outsourced identity management services.

7.3 Required Information Components

7.3.1 Participant Operating Practices

A fundamental expectation of Federation Participants is that they provide authoritative and accurate attribute assertions to other participants and that participants receiving an attribute assertion protect it and respect any privacy constraints placed on it by the Federation or the source of that information.

To support this goal, each Participant must describe its relevant operations in a Participant Operating Practices (POP) statement and share this POP with Federation Participants. The template POP is available on the InCommon website. In some cases, multiple systems can be described in one POP. A current version of the POP must always be available to the Federation and Participant Administrators. InCommon does not review such Participant Operating Practices against any criteria of performance. The POP is a self-asserted declaration by each Participant of its current practices. More information about POP requirements is available on the InCommon website.

7.3.2 Metadata

A Participant Administrator registers its Identity Provider and Service Provider systems through the participant administrative interface by describing components of its systems. The data are collected and digitally signed by InCommon. Secure, up-to-date, trusted information about all Participants and their systems is a core service of the Federation. InCommon will make reasonable efforts to verify submitted data, and will act in accordance with the practices outlined in the InCommon Operations reference, available on the InCommon website.

Metadata may be removed or modified by Participant Administrators through the participant administrative interface. Changes to metadata are updated within one Internet2 business day following the submission. Under special circumstances, Participant Executives or Administrators may make removal requests via e-mail or telephone as listed on the InCommon website. InCommon will verify these requests using trusted communication channels before processing any removal requests.

Transmission of Federation metadata to Participants is not initiated by InCommon. Instead, Participants are expected to retrieve Federation metadata on a regular basis.

7.3.3 Digital Certificates for Federation Participant service platforms

7.3.3.1 Signing

Certificate Signing Requests are submitted via the participant administrative interface. Certificates are signed in accordance with the InCommon Federation Certification Authority Server Certificate Profile found in the InCommon Certificate Practices Statement.

7.3.3.2 Expiration

Certificates normally are valid for one (1) year. The Participant will be notified by InCommon prior to the expiration of its certificates. The Participant is responsible for submitting certificate requests to update the validity of its certificates.

7.3.3.3 Revocation

The InCommon CA revokes certificates upon request by Participant Executives or Administrators. Certificates are revoked and a new CRL is issued within one Internet2 business day of the verification of the request. Details on the Certificate revocation policy and practices are available on the website.

8 Dispute Resolution procedure

Should disputes regarding Federation services or the use of those services arise among Participants or between a Participant and InCommon, the following procedure is intended to affect a 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's issues and the resolution of those will be communicated to Federation Participants by email or protected website, unless non-publication is requested by any of the disputing Participants.

8.1 Disputes Among Participants

Participants are expected to make every reasonable effort to settle disputes among themselves, especially if contractual issues among the Participants are involved. If circumstances warrant, (for example, if the dispute centers on the interpretation of Attribute values or the implementation of standards) InCommon 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 other operational staff or advisors. The Referee will then document in writing a proposed solution and submit it to the disputing parties for comment. The Referee then will submit a final draft to the Steering Committee.

8.2 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 Participant(s).

The Negotiator will gather all the facts and rationales for the dispute and, as necessary, seek advice from any Federation advisors 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, after reviewing the report, may ask for additional information or request the Negotiator to take into account further considerations and prepare a modified recommendation. Resolution of the dispute must be approved by affirmative vote of a quorum of the Steering Committee as defined in the Bylaws. If the Steering Committee is unable to affirm a resolution, the status quo is maintained. The OM shall report the Steering Committee's final action to the disputing Participant(s) in writing as soon thereafter as is 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 as stated in the Participation Agreement.

9 Operations

The operation and performance of the Federation infrastructure are paramount to maintaining its trust fabric. InCommon supports certain operational services, including the operation of a certification authority for digital certificate life-cycle management, the secure collection and distribution of participant metadata, a registration authority to identity-proof and credential Participant organizations and officers, communications and outreach, and a Help Desk. As the Federation gains more experience with federated identity and access management and as requirements for higher assurance levels emerge, the InCommon Federation's operations will evolve to meet new functional criteria.

9.1 Operational Assurance Level

Complete procedures were developed detailing InCommon's central operations. Information security industry standards and practices¹ were used to establish the necessary level of assurance. These operations and procedures were approved by a technical advisory group of Internet2 Middleware Architects. A public listing of these procedures can be found on the InCommon website.

9.2 Communications and Support

All InCommon operating documents and Participant Operating Practices statements are made accessible via the InCommon website.

InCommon provides a Help Desk for Participant administrative and technical support. The Help Desk is staffed during normal Internet2 business hours as described on the InCommon website. InCommon also supports a community electronic mailing list for building community involvement and partnerships. Any

¹ RFC 2527, RFC 3647, The American Bar Association PKI Assessment Guidelines, *The Computer Security Handbook 4th edition*, *Planning for PKI: Best Practices Guide for Deploying Public Key Infrastructure* by Housley and Polk, The Federal Bridge Certification Authority Certification Policy, and others.

end users who inadvertently contact the Federation Help Desk will be referred to their home organization for support in online access to other Participants.

Software guidelines are provided or referenced on the website, along with deployment guides, attribute policies, testing facilities, and other federation-specific information for the operation of Identity Providers and Service Providers in the Federation.

9.3 Federation Technical Infrastructure

InCommon is responsible for the secure operation of a number of technology platforms including: a Shibboleth "Where Are You From" (WAYF) server; a Metadata distribution service; a participant administrative interface; a Certification Authority; and other necessary infrastructure. Operation of the technical infrastructure is described in greater detail in the technical documents available on the InCommon website.

9.3.1 Where Are You From (WAYF)

The WAYF, an optional user interface component, is responsible for allowing users to specify their appropriate Identity Provider for the services they intend to use on-line. Upon selecting an Identity Provider, the user is redirected to the Identity Provider's log in service to authenticate. InCommon operates a redundant WAYF service and Web page on which all Identity Providers are listed.

9.3.2 Metadata Distribution

InCommon digitally signs and makes available to Participants metadata submitted by all Participants for interoperation of Identity Provider and Service Provider systems. The metadata is maintained on redundant servers.

9.3.3 Participant Administrative Interface

Federation Participant Administrators use the Participant Administrative Interface to securely manage the data relevant to their organization's participation in the Federation. The particular tasks include submitting certificate signing requests, Participant Operating Practices, and submitting or modifying Participant metadata.

9.3.4 Certification Authority (CA)

InCommon operates an X.509 CA from which it issues server certificates for use within the Federation. Redundant Certificate Revocation Lists (CRL) are made available and are updated every 30 days or within one Internet2 business day of a verified certificate revocation request, whichever is sooner.

9.3.5 Suspension of Federation Services

If InCommon suspects compromise of any of its service components, it may take immediate action to remedy the situation or verify non-compromise, including taking components out of service for a limited time for diagnosis and repair. The OM always will endeavor to minimize interruption or inconvenience to Participants. Any critical compromise will be communicated to Participants in a timely manner.

9.4 Disaster Recovery

InCommon disaster recovery practices ensure the minimum interruption of availability of Federation services in the event of a disaster. This includes providing redundant hardware and secure data backups. Public versions of disaster recovery practices are available on the InCommon website.

10 Participation Status: Renewal, Withdrawal and Termination, and Suspension

10.1 Renewal

Renewal of Participation is automatic as long as the Participant remains in good standing and pays its fees in a timely manner.

10.2 Withdrawal and Termination

Participant may withdraw from the Federation at any time upon written notice to the InCommon office in accordance with the Participation Agreement.

Termination by InCommon or Participant is governed by the Term provisions of the Participation Agreement.

In all cases of Withdrawal or Termination, the Participant will be removed from the metadata.

10.3 Suspension of Participants' Services

A Participant may request the suspension of any Federation services in the case of Administrator credential compromise, participant key compromise, or other security compromise within the Participant's systems. This request may be made via e-mail or telephone from the Executive or Administrator and will be verified by InCommon using trusted communication channels. Suspension may include processes such as revoking credentials, removing or modifying metadata, or revoking certificates.

If InCommon suspects any compromise or negligence on the part of a Participant, it will make reasonable efforts to contact Participant to verify Participant's status. For example, a non-responsive Administrator's account may be suspended for the security and safety of Participant's metadata if InCommon suspects an Administrator is no longer active and its repeated attempts at contact go unanswered.

11 Further Risk Assessment

For additional information highlighting some of the ways in which operation of the Federation might incur risk to Participants, please read the risk assessment paper found on the InCommon website.