

InCommon organizations control their exchanges based on scalable technology. Identity providers authenticate their own members and manage privacy levels. Resource providers authorize access based on agreed upon qualifications. The InCommon trust fabric enables federated identity management.

Security, privacy, and scalable access controls.

Trusted collaboration, InCommon.

The InCommon Federation leverages standards-based Shibboleth and PKI technologies to create access solutions that are easier on both the end user and the administrator.

Imagine this:

A visiting researcher needs access to the visiting campus's wireless network, his own remote database, professional journals, federal grant administration, and remote field instruments. With a single sign on to his home institution, the researcher can access all of the above at varying levels of privacy and authorization.

Thanks to InCommon participation.

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

InCommon™

To learn more, visit <http://www.incommonfederation.org> or contact us at incommon-info@incommonfederation.org

Participation in InCommon is open to two- and four-year degree-granting academic institutions in the United States and their resource partners.

InCommon LLC is operated by Internet2® and managed by an independent Steering Committee representing the higher education and research community.

InCommon™

www.incommonfederation.org

The **InCommon** Federation

Protected Resources
Secure Exchanges
Scalable Technology
Optional Privacy Protection

Through **InCommon**

Researchers
Faculty & Staff
Students

can

Collaborate
Share
Discover

a world of resources

Scientific Research
Government Services
Journals
Media
Everything Imaginable

Why InCommon?

- InCommon confirms every participating organization and the identity of their representatives.
- InCommon administers a certificate authority (CA) to create a level of assurance based on the identity proofing of the organization for trusted communication between participants.
- InCommon requires participants to share information about operational practices and privacy policies to ensure transparent collaboration.
- InCommon participants use the Shibboleth® software system for attribute exchange.

“By participating in InCommon, we can manage each customer’s account via a standardized format, which removes the need for us and our customers to repeat integration work for each new contract. Instead of being in the username and password business, we’re now able to focus on our core competencies as a resource provider.”

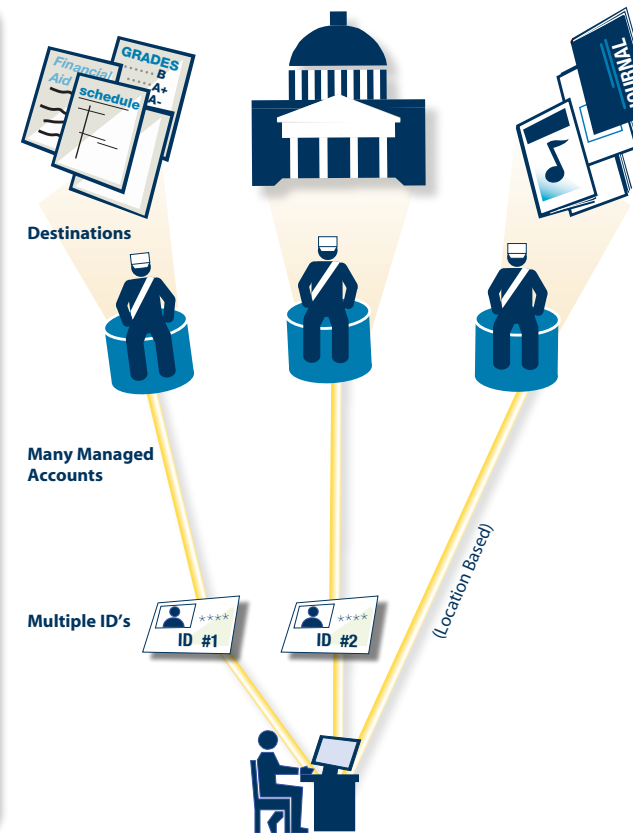
Joep Verheggen – Director Elsevier ScienceDirect

End User Benefits

- Users no longer have to manage an array of accounts and passwords.
- Users identify themselves locally with their home institution, then pass only relevant and necessary attributes to the resource, maintaining privacy as necessary.
- Single sign-on reduces opportunities for accounts to be compromised and also allows users to access any number of resources while signing on only once.

Without InCommon

- ▶ Users have many accounts to access different resources.
- ▶ Access is based on a user’s identity or location.
- ▶ Time spent managing accounts instead of resources.
- ▶ Lack of uniform standards among partners.
- ▶ Collaborations don’t happen because sharing is too difficult or insecure.
- ▶ Adding new resources and users may require significant work.



With InCommon

- ▶ Users have a single point of signing on to access different resources.
- ▶ Fewer user accounts to manage.
- ▶ Fine-grained control over the release of identities and other user information.
- ▶ Standards-based and open source.
- ▶ New resource providers and users can be integrated quickly.
- ▶ Access is based on information attributes, not identity or location.



“InCommon is reducing the need for our researchers, students, and educators to maintain multiple, password-protected accounts for each of our resource provider partners. At the same time, InCommon also protects the privacy of our community by empowering us with the ability to control what information about our community can be revealed externally.”

Gary Augustson – Vice Provost for Information Technology at Penn State

Administrator Benefits

- Fewer user accounts for resources to manage; reduced help desk cost for organizations.
- Fine-grained control over the release of identities and other user information.
- Uniform infrastructure allows new users and new resource providers to be quickly integrated, both on and off campus.
- Economies of scale are realized by federating to extend the capabilities of existing identity-management and resource services.
- Standards-based and open source, with an extensible vocabulary.
- Federation managed trust infrastructure.
- Easier inter-domain integration.
- Enable personalization, without releasing identity.

“The NISO MetaSearch Authentication and Access committee has extensively evaluated the available access control methods. Shibboleth and InCommon provide the most desirable model to pursue giving the complete control necessary for fine-grained access management.”

Mike Teets – Chair NISO Metasearch Initiative, Authentication Access Committee