InCommon is a formal federation of organizations creating a common framework for exchanging trusted identity information in support of research and education collaborations and sharing of protected resources. The community of InCommon participants defines, promulgates, and supports an agreed-upon set of policies and standards built upon original work and multiple industry developments.

Campuses

“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, Penn State

Best Practices

“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

Resources

“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

About Shibboleth

Shibboleth leverages campus identity and access management infrastructures to authenticate individuals and then sends information about them to the resource site, enabling the resource provider to make an informed authorization decision.

http://shibboleth.internet2.edu

The InCommon Federation:

Without InCommon

Resource providers spend a great deal of time and support managing user accounts.

Partnerships lack standards-based practices for easy, scalable integration.

Lack of fine-grained access and security controls leaves all but the broadest sharing opportunities unattained.

Users bear the burden of multiple username accounts and passwords.

Users are constrained by IP addresses and must be onsite to gain access.

Users give away privacy to gain access.