InCommon Assurance Program

PROVIDING A FRAMEWORK OF TRUST FOR THE SAFE SHARING OF ONLINE RESOURCES

What is the Identity Assurance Program?

The Identity Assurance Program awards certifications to qualifying campuses and research organizations that support InCommon requirements for consistent management of digital identities.

Why is it Needed?

Service Providers incur a risk of compromise when making resources available via federated identity and access management. Higher-risk applications (such as those involving financial or medical data) require a greater level of trust for another party's authentication and identity management system.

Service Providers: Service Providers reduce risk by requiring Identity Providers to adopt a set of standard identity and electronic credential practices that meet the service risk requirements. Services related to financial aid and federal research grants, for instance, will require that Identity Providers prove they are certified for a particular practice set in order to access the federated service.

Identity Providers: Supporting a standard set of assurance practices, and especially those that contribute to a higher confidence in identity, enables Identity Providers to access services that require greater security because of data sensitivity (such as medical or financial records), or because of the impact to the service or the provider's business (such as a critical IT system running in the cloud).

Which Assurance Profiles are Available?

InCommon has published two sets of practices, or profiles: Bronze and Silver. These profiles align with the U.S. government's NIST levels of assurance level 1 and level 2, respectively. Bronze has a security level that slightly exceeds the confidence associated with a common Internet identity. Silver has a security level appropriate for financial transactions.

Which Service Providers Use These Profiles?

InCommon is recognized as a Trust Framework Provider through the Federal Identity, Credential, and Access Management Program. As a result, Bronze and Silver will be available for use with identified federal services. However, as with federation itself, Identity Assurance is useful across the academy, including research and administrative-related services:

- The National Institutes of Health will introduce several Silver-requiring services in 2012, including federated grant submission
- CI Logon will use Silver to access research services such as Open Science Grid.
- Research virtual organizations, like LIGO, will offer Silver services to their project members in 2012.
- The National Student Clearinghouse will use Silver for access to private and federal loan reports.

Find out more at www.incommon.org/assurance

BENEFITS

Increases Confidence; Reduces Risk – Service Providers have increased confidence because standards-based identity practices ensure that their risk requirements are met.

Saves Time When Adding New Customers Service Providers can rely on community-accepted standards in assessing Identity Provider systems, eliminating the burden of individual campus assessments. This will greatly reduce the time required to add new certified Identity Providers.

Access to Higher-Value Services – Financial (and other) services that require greater confidence in an identity will be available to certified identity providers.

RESOURCES

To see these documents, go to www.incommon.org/assurance.

Identity Assurance Profiles: This document defines the specific requirements that Identity Providers must meet to be eligible for certification for Bronze or Silver

Identity Assurance Assessment Framework: This document describes the identity assurance trust model that InCommon has adopted, including a functional model for Identity Provider operations and a certification model.

InCommon®

PROVIDING A FRAMEWORK OF TRUST FOR THE SAFE SHARING OF ONLINE RESOURCES.

What is InCommon?

InCommon serves the U.S. education and research communities, supporting a common framework of trust services for the safe sharing of online resources. InCommon operates the InCommon Federation—the U.S. trust federation for research and education—and the community-driven InCommon Certificate Service.

The InCommon Certificate Service

InCommon® CERTIFICATES

The InCommon Certificate Service provides unlimited SSL certificates (including extended validation certificates), client (personal) certificates, and code signing certificates for one fixed annual fee. This program offers a true site license and truly unlimited certificates for all of the domains you own or control (.edu, .net, .com, .org, etc.). This program is open to any institution of higher education in the U.S.

The InCommon Federation

InCommon® FEDERATION

The InCommon Federation enables scalable, trusted collaborations among its community of participants.

InCommon Federation participants adopt common policies and processes, and use standards-based technology for authentication and authorization. This allows identity providers to have fine-grained control over the release of user information, while service providers maintain access control to their online resources. The result is a secure and privacy-protecting method for providing individuals with single sign-on access to protected or licensed online resources. Service providers no longer need to maintain user accounts or deal with password management.

Through federated identity management, researchers, faculty, students, and staff enjoy single sign-on access that allows them to:

- Manage research accounts and grants at the National Institutes of Health and the National Science Foundation.
- Participate in collaboration groups and virtual organizations within and outside of the campus walls.
- Gain access to key information resources, like library databases and financial aid information from the National Student Clearinghouse.

InCommon Federation Benefits

- Standardized format reduces or removes the need to repeat integration work for each new resource.
- One username and password for many services, done in a secure and privacy-preserving way. This results in less confused users (who will have fewer accounts to juggle), fewer password reset requests, and fewer support calls.
- Access decisions and user privacy controls are decided on a case-by-case basis for each resource, providing higher security and more granular control.
- Reduced account management overhead for service providers.

About InCommon

InCommon is operated by Internet2 Participation is separate and distinct from membership in Internet2. Certificate service subscribers must be an InCommon participant or join InCommon.

Who Can Join InCommon?

Any accredited two- or four-year higher education institution can join InCommon. Higher education participants can sponsor their online service providers.

HOW DOES IDENTITY FEDERATION WORK?