things-to-consider-when-joining-incommon

InCommon’s “common framework” creates multilateral trust among all federation Participants, facilitated by the Federation Operator, to exchange identity information in a secure manner. Service Providers trust Identity Providers to provide accurate information, and Identity Providers trust Service Providers not to misuse the information they receive. Community Members trust both Identity Providers and Service Providers to respect their privacy, making use of their identity information only as needed, according to legal and institutional policy. Trusted Relationships for Access Management: The InCommon Model provides a comprehensive introduction to this framework, including definitions of many of the terms used in this document.

InCommon’s Participants (member institutions) operate Identity Providers (IdPs - network-accessible services that authenticate users and provide identity information, according to local policy, about Service Providers’ current users) and Service Providers (SPs - network-accessible services that rely on information from IdPs for the purpose of making access decisions and/or personalizing the user’s experience). In order to facilitate this exchange, the Federation provides information about all IdPs and SPs, and the Participants that operate them, to all Participants. This creates a three-way flow of trust and information:

Your Identity-Related Policies and Practices

When you join the InCommon Federation, you will be agreeing to comply with various requirements related to InCommon's multilateral trust framework, including:

- Deployment of conformant software
- Use of common syntax and semantics for Identity Assertions
- Provision of accurate information for the Trust Registry
- Provision of accurate contact information
- Respect for intellectual property rights
- Respect for privacy of identity information
- Adherence to Baseline Expectations for the mature, secure, and privacy-protecting operation of your institution’s IdPs and SPs, and that those IdPs and SPs are duly registered with InCommon.

Now is a good time for a quick review your policies, practices, and software in light of your current requirements and those of the federation. This review will likely involve various areas of your institution, potentially affecting technology, policy, and operations.

If you will be registering an IdP in InCommon, you will particularly want to review your Identity and Access Management (IAM) program, the business processes and technology platforms that your institution uses to manage the life-cycle of identity information your institution maintains about members of its community to control access to online services. If your institution is like many others, that IAM program is the result of many years of often-informal evolution, so this is a good opportunity for some clean up.