Background Information for Regional / InCommon Collaboration

(8/29/2013)

This document provides background information for discussion of potential partnerships between InCommon and regional networks.

We start with some basic information on federation participants and the trust relations among them and then explore the specifics of the Federation Administrations functions.

Trust Relationships within a Federation

There are multiple types of participants in an identity federation. For the purposes of this discussion the federation participants are:

- IdP Operator (IdPO) - An organization that provides identity information to SP Operators. An Identity Provider (IdP) is the network-connected service operated by the IdPO to deliver that identity information to Service Providers.
- SP Operator (SPO) - An organization that provides services within a federation. A Service Provider (SP) is the network-connected service operated the SPO to deliver those services.
- Federation Administration (FA) - An organization that administers a federation. One of the FA's primary responsibilities is to maintain and distribute Metadata, one or more files containing information about the IdPs, IdPOs, SPs, and SPOs in the federation.

The trust relationships are multiple:

- SP Operators trust
  - Federation Administrations to correctly vet and certify IdP Operators,
  - Federation Administrations to maintain and distribute metadata containing service end-points, certifications, and other information about IdP Operators, and
  - IdP Operators to provide correct identity information.
  - IdP Operators to scope the audience receiving credentials to the appropriate group
- IdP Operators trust
  - Federation Administrations to correctly vet and certify SP Operators,
  - Federation Administrations to maintain and distribute metadata containing service end-points, certifications, and other information about SP Operators, and
  - SP Operators not to misuse or mismanage the identity information they receive.
- Federation Administrations trust
  - IdP and SP Operators to reveal correct information about their policies and practices, and
  - When inter-federating, other Federation Administrations to reveal correct information about their policies and practices

  - When inter-federating, other Federation Administrations to maintain and distribute metadata containing service end-points, certifications, and other information about SP and IdP Operators.

There are multiple levels of trust in each of these categories, affected by many factors. For example,

- Organizational maturity
- Legal regulatory domain
- Contractual agreements and remedies
- Risk mitigation
- Technology deployed
- Process controls
- Independent audit

Federation Functions

As indicated above, minimally, federations are responsible for trustworthy operation of the following functions:

- Collection, maintenance and distribution of metadata
- Vetting and certifying IdP Operators and SP Operators
- Baseline behavioral guarantees for participants

These represent the federation's primary purpose of integrating identity providers and service providers and are, therefore, represent our primary opportunities for partnership. They are discussed in greater detail below, as well as other functions performed by InCommon.

Maintenance and Distribution of Metadata

The federation is responsible for maintenance and distribution of metadata containing information about all SPs and IdPs registered in the federation. This information includes:

- service end-points
- certifications
- contact information
- user interface elements (logos, support addresses, *etc.*) for use by discovery services

Vetting and Certifying IdP Operators and SP Operators

There are multiple compliance standards that have been established by InCommon for IdP Operators and SP Operators, for example:

- Baseline requirements for all InCommon participants. These are specified in the Participant Agreement and the Participant Operating Practices statement. (See the Appendix: InCommon Participant Agreement Requirements for further information.)
- Additional requirements for IdP Operators that opt to be certified for the InCommon

Bronze or Silver assurance profiles. These requirements are specified in the Identity Assurance Assessment Framework and the Identity Assurance Profiles.

- Additional requirements for SP Operators that opt to be certified for one of the InCommon Service Categories, such as the Research & Scholarship Category.

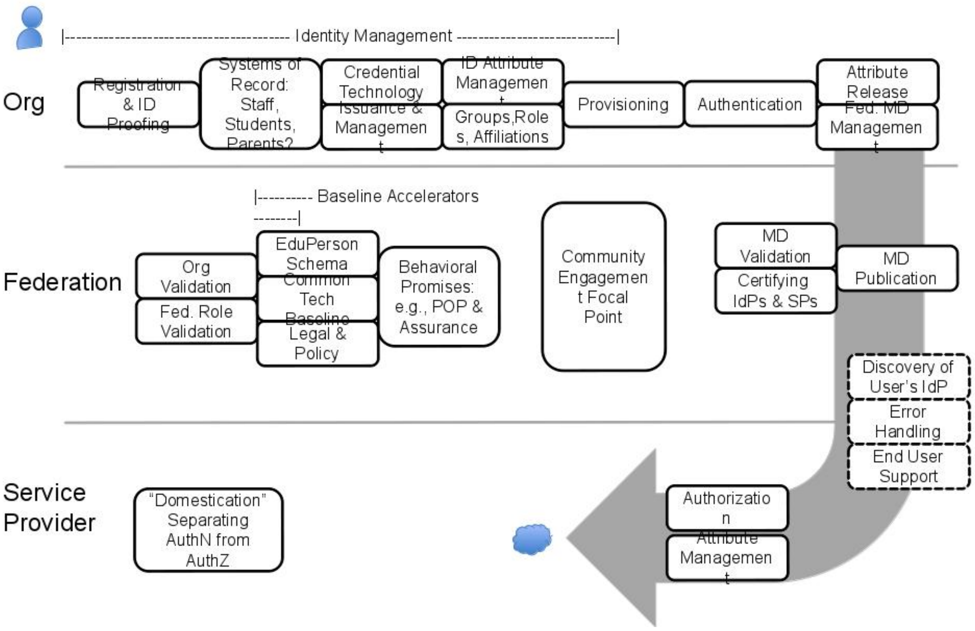
Other Functions

InCommon provides other functions that do not materially contribute to trust, but are drivers for scale and interoperability.

- Schema adoption. A commonly agreed upon set of attributes must be adopted as the lingua franca for access decisions.
- Discovery Service. A centrally managed Discovery Service (DS) can be an important scale enabler to enable end users to select the IdP that will identify them to the SP. SPs often incorporate their own discovery services that are tailored to their user community; the InCommon DS is provided as a federation-wide default.
- Error Handling Service. While SPs are encouraged to implement authentication error handling services that are tailored to their specific needs, a default error handling service is provided for InCommon for SPs that have not done this.
- Dispute Resolution. InCommon participants are encouraged to resolve disputes among themselves. InCommon can, however, facilitate resolutions. Ultimately, where a dispute affects the federation overall, the Steering Committee is the final arbiter.
- Technical Interoperability Standards. InCommon publishes and references schemas, software guidelines, profiles and other technical standards for interoperability within the federation.
- IdP Solutions: Gateways to Other Authentication Frameworks. InCommon is working on gateways to Google and other “social” services to support campus relationships with more distant stakeholders, such as Parents or lifelong learning Students.
- Tags. Categorizing or certifying SPs and IdPs according to groups of characteristics allows for more scalable approaches to attribute bundling and automated attribute release.

The following diagram illustrates the identity and access ecosystem of actors and systems within a federated transaction.

End-to-End Federated Business Models: the Solutions Marketplace


|-- Identity Management -----------------------------|
Org
Registration & ID Proofing
Systems of Record: Staff, Students, Parents?
Credential Technology
Issuance & Management
ID Attribute Management
Groups,Roles, Affiliations
Provisioning
Authentication
Attribute Release
Fed. MD Management
|---------- Baseline Accelerators --------|
Federation
Org Validation
Fed. Role Validation
EduPerson Schema
Common Tech Baseline
Legal & Policy
Behavioral Promises: e.g., POP & Assurance
Community Engagement Focal Point
MD Validation
Certifying IdPs & SPs
MD Publication
Discovery of User's IdP
Error Handling
End User Support
Service Provider
"Domestication" Separating AuthN from AuthZ
Authorization
Attribute Management