Project Terminology

Terminology Used in InC-Quilt Federation Documentation/Discussions

Term	Definition
Delegated Administration (Scenario)	This model keeps the existing InCommon technical infrastructure and Regionals assume some administrative responsibilities and may provide some level of assistance or technical support to K-12 or Community Colleges to bring up an Identity Provider (IdP) or Service Provider (SP) for their constituent's institution.
Sub-Federation (Scenario)	The sub-federation scenario implies that the Regional will help manage their own federation of IdPs and SPs and register their participant's metadata with InCommon. InCommon Operations (or a Regional delegated administrator) will create an aggregate of the Regional federation entities, plus some number of InCommon entities (likely SPs) for use by the Regional federation participants. Some number of Regional entities may also be published in the default InCommon MD aggregate, shared with all InCommon members.
Interfederation (Scenario)	The Interfederation model implies that there exists a separate (possibly existing) federation that wants to interoperate with InCommon. This could be a state university or community college system, K-12 school districts, healthcare facilities, libraries, museums or other Community Anchor Institutions. Some of these may not fit the current business model of InCommon, but need to interact with each other, existing InCommon SPs or other peer organizations in other states /federations. This model can be established using either the Metadata Aggregator (MDA) tool or possibly a Proxy IdP – depending on the use cases of the (local /state/Regional) federation.
Federation	A federation supports a common framework for trusted shared management of access to on-line resources. Identity Providers can give their users single sign-on convenience and privacy protection, while online Service Providers control access to their protected resources. A federation, through its trust agreements and federating software, allows identity providers to manage user privacy and information exchange. Service providers no longer need to provision identity accounts, instead leveraging the identity provider's identity system. (Definition from InCommon site)
Federation Operator	A federation operator (such as InCommon) manages the services offered by a Federation including entering into contracts with IdPs, SPs, and vendors, operating a service infrastructure supporting real-time transactions with participants, acting as the Registration Authority of the federation, overseeing compliance audits of certain Federation participants (such as the InCommon Silver Assurance program) and maintains records, documents and other resources of the Federation.
InCommon	The Research and Education (R&E) Federation Operator for the United States.
InCommon Affiliate	InCommon Affiliates provide software, support, integration, and other identity services for higher education and their sponsored partners. The InCommon Affiliate Program connects higher education institutions and their partners with organizations that provide implementation and integration products or services related to identity and access management.
Metadata (MD)	Metadata (MD) refers to a configuration data file used to provision an SP or IdP to communicate with each other. Typically it exists in XML form, at least for publishing and interchange.
Metadata Aggregator (MDA)	A metadata aggregator is a tool used to process the metadata of IdPs and SPs and create a composite aggregate MD file for a particular federation or subset of a federation.
Proxy IdP/SP	A gateway IdP that sits at the boarder between two federations. The Proxy IdP must be included in the metadata of the "external" federation, with the "SP" side of the Proxy in the metadata of the federation that owns the Proxy. Proxy IdPs based on SimpleSAMLphp can connect to many different types of Authentication and directories/databases residing in the federation it is protecting.
Identity Provider (IdP)	An Identity Provider (IdP) is a federation entity that provides authentication and attributes for the users of the organization that owns it.
Service Provider (SP)	A Service Provider (SP) protects a resource from access by unauthorized users. It requires a SAML assertion from an IdP that contains information attributes about a user, as well as an acknowledgement of their successful authentication. This SAML assertion is evaluated to determine whether to provide the user access to the protected resource.
Registration Authority (RA)	A federation Registration Authority (RA) performs identity proofing and vetting for federation applicant organizations, to verify the identities of its executive and federation administrator representatives.
POP (Participant Operational Practices)	A document filled out by an InCommon member (those running IdPs and/or SPs) that answers questions pertaining to how expected federation behaviors are performed at the member institution. These include how credentials are issued, how user attributes are managed, etc.
Net+ Services	"Above the net" services offered by Internet2. See: http://www.internet2.edu/netplus/