Interfederation Tools Comparison

Method	Description	Pros	Cons
Proxy IdP	A gateway that sits at the boarder between two federations. It has both an IdP and SP "side". The IdP side of the gateway must be included in the metadata of the "external" federation (e.g. InCommon), with the SP side included in the metadata of the federation that owns the Proxy (e.g. a regional federation). A user authenticating to an external federation's service (e.g. InCommon SP) would be redirected to the Proxy IdP, which in turn would relay the user to their "home" institution's authentication source to login.	• Less time consuming to connect to CAS, AD, etc. • Potentially less work if you don't already have SAML IdPs • Might be beneficial for K-12 use case (likely not running IdPs) • Useful for Hub & Spoke model • SimpleSAMLphp IdP is recommended for this, since it has OOTB multi-protocol capability (can connect to many different types of authentication mechanisms and directories/ databases)	• Not as straightforward as MDA • Might be difficult to establish "trust" from a policy and business perspective with SPs from an external federation, since the authentication sources behind the proxy are not part of the same federation. • IdP Proxy has a number of little "gotchas" that can make implementation difficult - (Tom Scavo)
Metadata Aggregator (MDA)	A metadata aggregator is a tool used to process the metadata of IdPs and SPs and create a composite aggregate Metadata (MD) file for a particular federation or subset of a federation. A regional federation might generate its own MD file (which would include its own members and possibly some InCommon entities) and then "Publish" a subset metadata aggregate for InCommon to regularly include in its MD (all regional participants that want to be InCommon "members").	• If you already have SAML, the MDA is a straightforward way to go from a technical perspective • If you need MD from an external federation (InCommon) anyway, then MDA might be a better solution using Publish & Subscribe • Could still "hide" members using MDA – just don't Publish them to external federation • More tested tech • Less complicated once established	• Requires SAML Metadata from IdP and SP entities to process • If organizations are not already running IdPs, then not a suitable solution

Mark Scheible, MCNC – 05Apr2013