



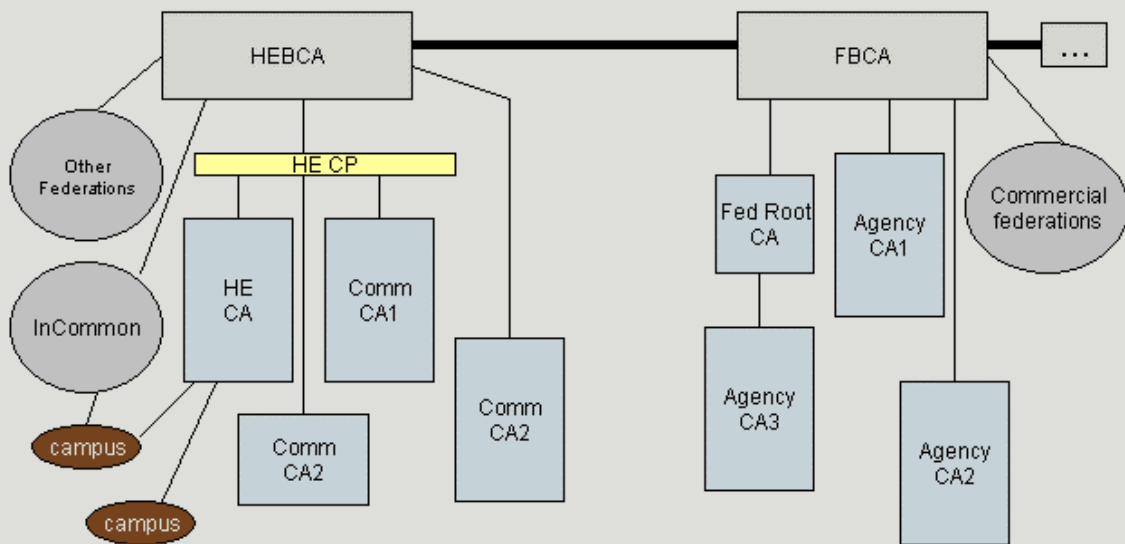
Federations

- *Federations – the good, the bad and the unknown*
- *Types of federations*
- *What federations need to exist*
- *Federating software*
- *Federations today*
- *Federations in Higher Education*
- *Issues and next steps*

- *They are very similar*
 - Both imply trust models
 - Federations are an enterprise-enterprise PKI
 - Local authentication may well be end-entity certs
 - Name-space control is a critical issue
- *And they are very different*
 - End user authentication a local decision
 - Flat set of relationships; little hierarchy
 - Focus as much on privacy as security
 - Web Services only right now: no other apps, no encryption
 - We get to define...

Overall Trust Fabric

Trust diagram





What are federations?

- *Associations of enterprises that come together to exchange information about their users and resources in order to enable collaborations and transactions*
- *Built on the premise of*
 - Initially “Authenticate locally, act globally”
 - Now, “Enroll and authenticate and attribute locally, act federally.”
- *Federation provides only modest operational support and consistency in how members communicate with each other*
- *Enterprises (and users) retain control over what attributes are released to a resource; the resources retain control (though they may delegate) over the authorization decision.*
- *Over time, this will all change...*



The good

- *Very flexible – easy to establish and operate; can work for 2 or 2000 members*
- *Very customizable – tailored to fit the precise membership*
- *Address the whole problem space – security, data schema, privacy, security, transport – of inter-realm collaborations*
- *Are simple to install and operate, both for enterprises and for end-users*



The bad

- *They aren't real, yet*
- *They don't do everything*
- *Are web services based right now*
- *Will hit scaling walls in several dimensions; we don't see clear answers yet...*



The unknown

- *The scaling walls*
- *How reality will unfold*
- *The convergence of the various federating software solutions*
- *Users' willingness to manage their privacy and security*

Three Types of federation

- *Internal federations are occurring among the many subsidiaries of large companies, especially for those companies with more dynamic aggregations.*
- *Private federations occur among enterprises, typically within a market sector, that want to facilitate a specific set of transactions and interactions. Many will be bi-lateral, short-term or otherwise constrained.*
- *Public federations address more free-standing, long-term, general-purpose requirements, and need to be more open about rules of engagement. Public federations face significant scaling issues and may not be able to leverage contractual relationships that private federations can.*



Requirements for federations

- *Federation operations*
- *Federating software*
 - Exchange assertions
 - Link and unlink identities
- *Federation data schema*
- *Federation privacy and security requirements*

- *Liberty Alliance*

- V 1.1 of their functional specs; 2.0 under discussion
- Federation itself is out of scope (see PingID et al)
- Semi-open source under development
- Current work only on linked identities

- *Shibboleth*

- V1.1 released; 2.0 under discussion
- Most standards-based (though Liberty has said that they will turn their enhancements into standards organizations)
- Pure open source
- Current work is attribute release focused.

- *WS-**

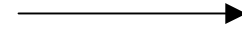
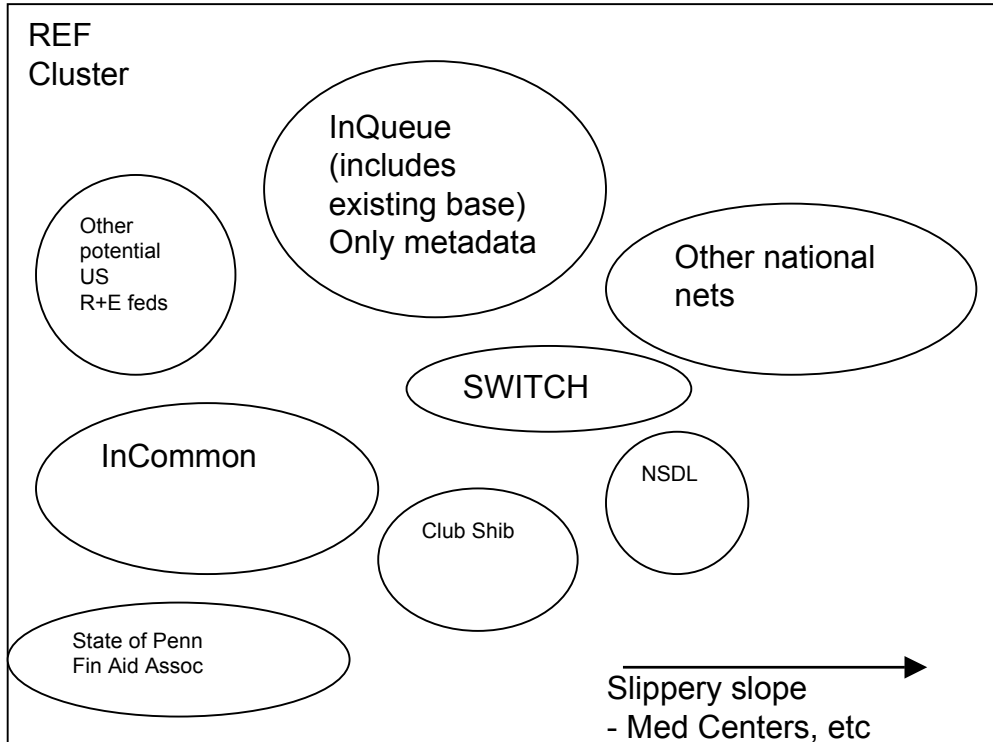
- *Work by Microsoft, with participation from IBM and BEA et al*
- *Complex framework, consisting of 9 areas, which can form a whole cloth solution to the problem space, but which need to closely interact with each other to do so.*
- *Several of the specifications areas still unreleased*
- *Standards process very unclear; significant IPR issues exist*
- *No implementations yet; indeed a lofty set of abstractions that will need considerable convention and detail to resolve into a working instantiation*
- *Can Shibboleth/InCommon be a working instantiation within WS-*? Good question. Once MS has all the areas defined, if someone wants to see whether the existent Shib/InCommon (or Shib/someotherfed) fits into WS-*, we'd certainly be curious...*



Shibboleth-based federations

- *InQueue*
 - *InCommon*
 - *Club Shib*
 - *SWITCH*
 - *NSDL*
-
- *State networks*
 - *Medical networks*
 - *Financial aid networks*
 - *Life-long learning communities*

The Research and Education Federation Space



Other clusters



InCommon Activities

- *Current*
 - Process applications for admission into origin list or for being a target
 - Manage central WAYF and distribution of Club Shib feed (members and their keys)
 - Member services – information, key revocation; no tech support
- *Longer term...*



Trust pivot points in federations

- *In response to real business drivers and feasible technologies*
 - increase the strengths of*
 - Campus/enterprise identification, authentication practices
 - Federation operations, auditing thereof
 - Campus middleware infrastructure in support of Shib (including directories, attribute authorities and other Shib components) and auditing thereof
 - Relying party middleware infrastructure in support of Shib
 - Moving in general from self-certification to external certification



Process the last six months

- *Breadth of interest in Shib leads to design team discussions and last minute externalization of trust components*
- *Discussions in FOO*
- *Conversations in the halls of lots of meetings*
- *Most recently, discussions with European and Australian middleware folks*
- *Internal Internet2 planning of storefront, operations, naming*