IdP Discovery

Discovery during authentication is a unique-to-federation problem caused by the need for user selection of an authentication source. Within a single domain, authentication sources are often combined by "stacking", in which credentials are played against multiple back-ends in some combination. This doesn't work across domains because it would expose user credentials to authentication systems controlled by unrelated organizations. As a result, the authentication source has to be selected before credentials are supplied, either explicitly through user choice, or by deriving something from a user identifier.

See also the Shibboleth topic on IdPDiscovery.

- Workarounds
  - Initiating at the IdP
  - Per-IdP URLs (e.g. Google)
  - Assume one IdP, "click here if you're a weirdo" in its login UI
- Models
  - SP/Embedded
  - Centralized/Shared
    - SP-centric vs. federation/IdP centric
  - Proxying
- Common UI "trigger" for consistency
- Maintaining the "story" through discovery and login
  - http://wiki.oasis-open.org/security/SAML2MetadataUI
- Shared hints, friend or foe?
- Boarding Process
  - Limiting discovery to IdPs expected to be viable.