Authorization

It's a truism among the security-minded that authentication is not a substitute for authorization. Federation brings that point home with a vengeance because there is often a loss of control over who can actually authenticate to an IdP, as compared to an authentication service under the control of the same organization that owns a service. That authentication is no guarantee of user-appropriateness becomes inevitable with federation.

Federated applications can assume literally nothing about an authenticated user unless they're prepared to negotiate in detail with partners on a continual basis; in return those same partners would generally be wise to refuse any constraints on their ability to operate their identity management systems as they see fit, lest they be hamstrung by their partners.

Instead, federated applications (and indeed all applications) must rely on the Attributes they are able to obtain about the users that authenticate to them. These attributes might include identifiers that allow applications to explicitly provision and recognize individual users and grant them locally-maintained rights. This is a common, though limiting, pattern: local authorization with distributed authentication.

But attributes may express, in addition or instead, a user's relationship with the authenticating organization, membership in Groups, or posession of roles or entitlements that signify permission to access application resources. In such cases, authorization may be delegated or distributed to the authenticating organization, or even across additional organizations. This is a relatively common pattern when the authorization policy is simple (typically all or nothing) and applies to large numbers of users at multiple organizations. It is less common as policies become more complex and fine-grained.

- Local vs. Distributed Authorization
- Groups vs. Roles vs. Entitlements
- Authorization Without Identity
- Incident Response and Blacklisting
- Blocking Authentication of Unauthorized Users
- Implications of Federation on Authorization Services?
    - XACML: Friend or Foe?