

Account Linking

Basic Requirements

- Persistent identifier bound to a credential
- May (should?) be unidirectional
- May be backed by a private key

Examples of Identifiers

- Private keys/fingerprints
- Certificate issuer/serial
- SAML "persistent" (or other) identifiers
- Infocard "PPID" claim
- OpenID

Processes

- Runtime creation of new accounts
 - May include additional attributes from IdP or other sources, including end user
- Runtime linking of existing accounts
 - Generally requires establishment of ownership of account via local authentication, knowledge-based challenge, additional attributes from IdP or other sources
- Batch feeds (SPML?)

Issues

- Correlation of activity when identifiers are omnidirectional
- Reassignment of identifiers
- Lack of standards around UI, particularly canonical "login to SP, login to IdP" use case
- "Unlinking", particularly recovering access to local account once local credential is long forgotten
- Granting access to a new user before a link exists