Device Recovery in WebAuthn

Utilize Online Recovery Storage

Alex Takakuwa, University of Washington

Online Recovery Storage

- Use Transfer Access style delegations
  - Chains of signatures from the original private key to the new private key
  - Chain of hardware attestations from the original device to the new device
- Store information about each registration (with Online Recovery Storage) including registered public keys/key handles for each Relying Party
  - Also store a Transfer Access style delegation to a “backup device”
  - Can encrypt storage with a privacy wrapping key to preserve non-linkabililty
  - Note: Recovery storage doesn’t have to have access to private keys.
  - This should happen after each registration, but does not necessarily require user action.
- Recovery:
  - Backup device creates delegations to the new device for each site.
  - New device delivers these chains to Relying Parties.

User Experience: Online Recovery Storage

- Setup:
  - User acquires and manages a backup device. (This can be pysical device(s) or a software service)
  - User “activates” each new authenticator once by syncing with the backup device
    - User can also activate a new device by syncing with an existing device
- Recovery:
  - User buys a new device, sets up a secure channel with the backup device and “restores” from a previous device. These devices will need access to the Online Recovery Storage
- Authentication:
  - Same as normal
- Device Upgrade
  - Same as in Transfer Access

Caveats

- Requires available online recovery storage during each **registration** and **recovery**
  - Note that during registration, the user is already necessarily online.
- Requires authenticators that can access the internet in some way
  - Old phones would work well as backups authenticators
- May require backup devices/authenticators with UI so that users can select which devices they would like to restore, should users want this option

More Information on Recovery from Device Loss

https://docs.google.com/document/d/1tRLbXYLb9Z65QqhOX7v9D-aq_RUODyn5oALpCXj46K8/edit?usp=sharing