Device Recovery in WebAuthn

Copying Private Key Material

Alex Takakuwa, University of Washington

Copy Private Key Material

- Copy necessary information to reconstruct the private key
  - Ex: Random Seed
  - Ex: Wrapping Key

User Experience: Copy Private Key Material

- Setup:
  - User acquires device capable of copying keys. Users must understand that this type of initialization should not occur agian. The user should use recovery or device upgrade in the future.
- Recovery:
  - User retrieves another valid device, sets up a secure channel, and uses that to duplicate the keys.
- Authentication:
  - Same as normal
- Device Upgrade
  - Same as recovery

Caveats

- Revocation is potentially unsolved. We have some methods proposed that rely on trusitng the authenticators to update counters, but revoking access from a single device is difficult.
- Relying Party can’t validate new hardware
- Authenticators must implement secure key copy.
- If copying a random seed, authenticators need to implement operations to derive keys from that seed
- If copying a wrapping key, Relying Parties need to store wrapped keys.

More Information on Recovery from Device Loss

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