RISC F2F

May 4, 2017

Agenda

- Events Base URI
- Events
- Opt-out
- RISC Profile Spec
- Use Cases
- ~~Distribution Spec~~

Events Base URI

- http://schemas.openid.net/**event**/risc/event-type/account-deleted
  vs
  http://schemas.openid.net/risc/**event-type**/account-deleted
- component for SET namespace: event, secevent, set, security-event
- component for profile: risc
- component for URI type, "event type": event, event-type

Events Base URI - OAuth Events

- Profile group for all OAuth based profiles
- http://schemas.openid.net/**event**/oauth/

Events - *revoked

- sessions_revoked
  - IdP revoked one or more sessions for this user due to security reasons
- ~~session_revoked~~
  - session or device identifier?
    - what would the semantics be for this event?
    - Id Token revocation?
- tokens_revoked
  - IdP revoked **all** tokens for this user **and** client, based on user action
- token_revoked
  - explicitly by client using revocation API
  - by IdP due to inactivity, or similar policy
- client_secret_revoked
  - client secret compromised
  - applies to all subjects

Events - Hijacking

- account_locked
  - account locked, needs recovery flow
- ~~account_reverification_requested~~ account_password_change_required
  - account not locked, but user will be prompted to change password, special notification sent
- account_at_risk
  - account not locked, **unusual** activity through login or recovery
- ~~account_recovered~~ account_unlocked
  - user went through recovery and account is back in good standing
  - this is not for the "forgot password" case
- do we need a password change event?
  - not clear what it can be used for
  - password_change_user
    - user chose to change password, was not forced to
  - password_chage_admin

Events - Account Deleted

- account_deleted
- *account_undeleted*
- *account_purged*

Events - Abuse

- abuse event cannot be communicated in event
- bot created accounts should have a distinct event

Events - Generic Account Disabled?

- account_disabled
  - reason: hijacking, abuse, delete, bot, admin
- account_reenabled

Events - Identifier Change

- also similar event is Identifier Recycled

Events - Other?

Opt-out

- Opt-out at transmitter
- User interaction questions:
  - Global or per receiver
  - Uni or bidirectional

Possible events:

- opt-out-initiated
- opt-out-cancelled
- opt-out-effective
- opt-in

OAuth profile group level event?

RISC Profile Spec

- OpenID RISC specific spec
- One or two specs
  - list of events
  - other RISC specific URIs and additions
    - aud prefix URI
    - subject enrollment RISC specific attributes
      - email
      - email_verified
      - phone_number
      - phone_number_verified
    - OAuth profile group level?

Use Cases

- RISC Use Cases

Distribution Spec - Data Plane

- rough agreement on delivery methods
  - push: HTTP POST, single event
  - pull: HTTP GET with POST for confirmation, multiple events
- HTTP level authentication

Distribution Spec - Control Plane

- early requirements
  - assumptions
    - one stream per transmitter and receiver
      - receiver identified by set of credentials
  - basic control plane operations
    - stream status
    - subject add and remove
    - verify event request
  - plain REST vs SCIM
    - writing proposal for both then we will compare