

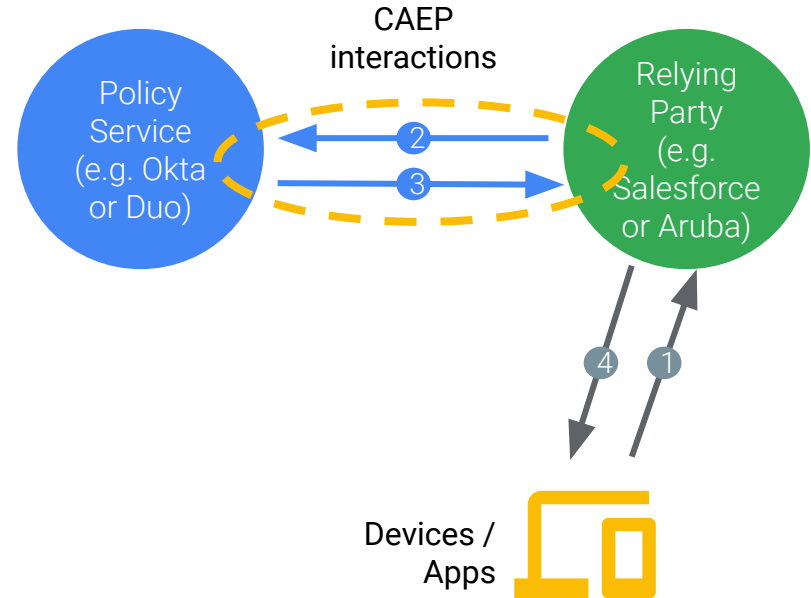
Shared Signals and Events

Spring 2020 Update
to the

OpenID Foundation Workshop

What is SSE?

- Synchronize distributed state relating to shared principals
 - Users
 - Authentication
 - Devices
- Using a publish and subscribe method
- Based on OpenID RISC Profile
- Incorporates events and concepts from “Continuous Access Evaluation Protocol” (CAEP)



Events since Fall 2019

- OpenID RISC Working Group re-constituted as Shared Signals and Events
- Workshop in Microsoft in Nov 2019
- Workshop in Cisco in Feb 2020
- Results from Workshop:
 - New Event types identified
 - New Subject types identified
 - Changes to RISC Profile outlined
- Spec development in progress
 - First draft shared with WG
- Microsoft CAE implementation

Microsoft CAE Implementation

- References CAEP work in announcement
- Enables two services (Teams and Exchange Online) to obtain updates from Azure AD:
 - User Account is deleted or disabled
 - Password for a user is changed or reset
 - MFA is enabled for the user
 - Admin explicitly revokes all Refresh Tokens for a user
 - Elevated user risk detected by Azure AD Identity Protection
- Interest in converging using standards in the future

Outline of Changes to SSE Spec

- Event Properties
 - Additional Claim in SSE SETs to indicate optional detail about the event.
 - May be event-specific, so not included in Subject Type fields.
- Subject Principals
 - Entities managed by Transmitters and Receivers
 - Referenced by Subjects in SSE events.
 - Subject Principal Administrative Groupings (SPAGs) represent collections of Subject Principals
- Transmitter Status Changes
 - Status may be queried and updated for specific SPAGs

Work to be Done

- Add CAEP Events Spec
- Discuss and finalize SSE Profile Spec
- Discuss and finalize Use-Cases Spec
- Virtual Workshop Planned for June 4-5