Google Cloud

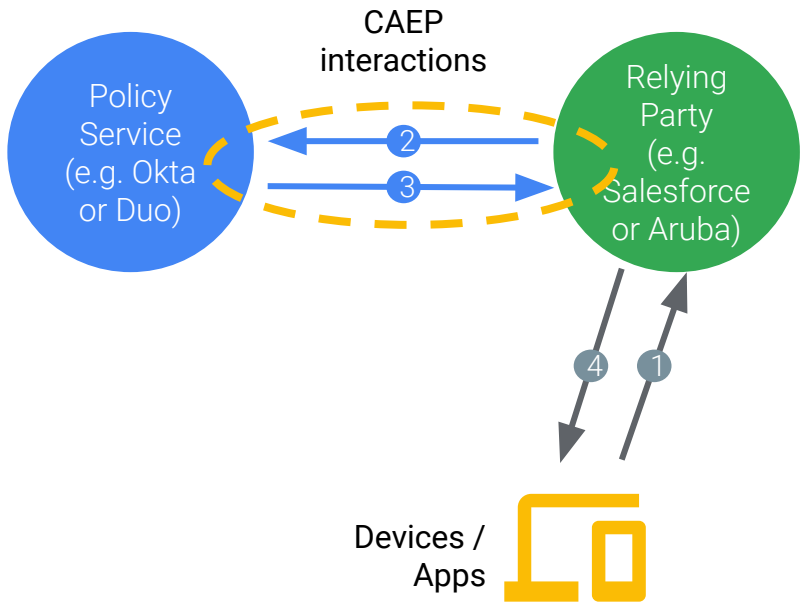
Shared Signals and Events

Atul Tulshibagwale (Google)

Spring 2020 Update

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)



Why Shared Signals and Events

Continuous Access Evaluation

- Enterprises migrating to a perimeter-free “zero-trust” architecture
- Attack focus shifting from network penetration to endpoint compromise
- Every access needs to be evaluated “in context” - User identity, device, location, client-app, user behavior, etc.
- Current authentication technology needs to catch up

Why Shared Signals and Events

RISC

- Attackers often target multiple accounts across service providers for a single individual
    - A single weak link can create a cascade of account takeovers
- RISC enables providers to prevent attackers from compromising linked accounts
- RISC helps enables coordination in restoring accounts in the event of compromise

RISC + CAEP Better Together

- Both concerns are ultimately about determining access to online resources
  - CAEP provides finer-grained routine information
  - RISC enables taking drastic action swiftly in response to account compromise
- Both protocols use similar asynchronous publish-and-subscribe mechanisms
  - Leverage the same set of underlying principles and standards
- Systems that implement these protocols are likely to overlap
  - Can benefit from uniformity in formats and features

Progress Since Fall 2019

- OpenID RISC Working Group re-constituted as Shared Signals and Events
- Workshop in Microsoft in Nov 2019
  - Attended by Google, Microsoft, Cisco, Thales, Sailpoint,
- Workshop in Cisco in Feb 2020
- Results from Workshop:
  - New Event types identified
  - Changes to RISC Profile outlined
- Spec development in progress
  - First draft shared with WG
- Microsoft's CAE announcement

Microsoft CAE Announcement

- 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
  - 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

- Subject Principals and SPAGs
  - 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
  - Authorization per SPAG update request

Outline of Changes to SSE Spec - Contd.

- Event Properties
  - Additional optional claim in SSE SETs to specify detail about the event
- Other Changes
  - Versioning
  - “Accepted” 202 responses to some requests

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
    - Register here