Shared Signals and Events

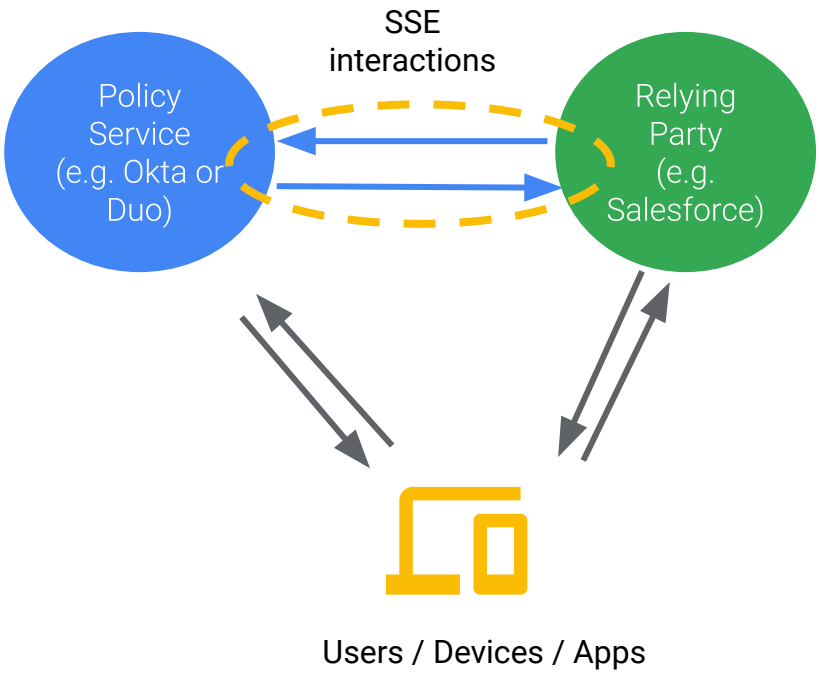
Fall 2020 Update

Atul Tulshibagwale (Google)

Tim Cappalli (Microsoft)

What is SSE?

- Synchronize distributed state relating to shared principals
  - Users
  - Authentication
  - Devices
  - ...more in future
- Profile of Security Event Tokens (SETs)
- Using an asynchronous publish and subscribe method



Applications of Shared Signals and Events

Continuous Access Evaluation Protocol (CAEP)

- Conveys state changes relating to access to resources
- Enables peers to tune access to updated state
- Event types include:
  - Credential change
  - Token claims change
  - Level of Assurance change
  - Device compliance change

RISC

- Enables providers to prevent attackers from compromising linked accounts
- RISC helps enables coordination in restoring accounts in the event of compromise
- Event types include:
  - Account purged
  - Credential change required
  - Identifier recycled

Progress Since Spring 2020

- First draft of SSE Profile of SETs spec published in May
- Virtual Workshop hosted by Google in June
    - Attended by Google, Microsoft, Cisco, Thales, Sailpoint, VMWare, Intuit, Target and others
- Results from Workshop:
    - Go forward on draft spec
    - Start work on CAEP Event types spec
- Re-worked spec to depend on IETF SecEvents Subject Identifiers draft

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

CAEP Event Type Examples

- Current Event Types
  - **Session Revoked**
  - **Token Claims Change** (ex: location or IP address change)
  - **Credential Change** (ex: user added a FIDO2 authenticator)
  - **Device Compliance Change** (ex: device was compliant and is now not compliant)
  - **Assurance Level Change** (ex: LoA increased or decreased for a user or device)
- Event types do not mandate specific subject identifiers
- Custom claims allowed between transmitter and receiver

[Example] Session Revoked: User + Device


```
{
    "iss": "https://login.microsoftonline.com/e69e17d9-8a93-4156-bed8-71036f23080d/",
    "jti": "24c63fb56e5a2d77a6b512616ca9fa24",
    "iat": 1600976590,
    "aud": "https://events.workspace.google.com/caep",
    "events": {
        "https://schemas.openid.net/secevent/caep/event-type/session-revoked": {
            "subject_type": "user-device",
            "user": {
                "subject_type": "iss-sub",
                "iss":
"https://login.microsoftonline.com/e69e17d9-8a93-4156-bed8-71036f23080d/",
                "sub": "jane.smith@example.com"
            },
            "device": {
                "subject_type": "iss-sub",
                "iss":
"https://login.microsoftonline.com/e69e17d9-8a93-4156-bed8-71036f23080d/",
                "sub": "e9297990-14d2-42ec-a4a9-4036db86509a"
            }
        },
        "initiating_entity": "policy",
        "reason_admin": "Policy Violation: C076E82F",
        "reason_user": "Your device is no longer compliant.",
        "tenant_id": "123456789",
        "event_timestamp": 1600975810
    }
}
```