Strengthening Keycloak Security

An Introduction to the Shared Signals Framework

Thomas Darimont
Identity Tailor GmbH

Thomas Darimont

- Managing Director | Identity Tailor GmbH
- Digital Identities ❤️ Standards
- Open Source Enthusiast
- Spring Team Alumni
- Official Keycloak Maintainer
- OpenID Foundation Certification Team
- IDPro Certified
- Java User Group Saarland Organizer

@thomasdarimont
thomas@identity-tailor.de

Overview

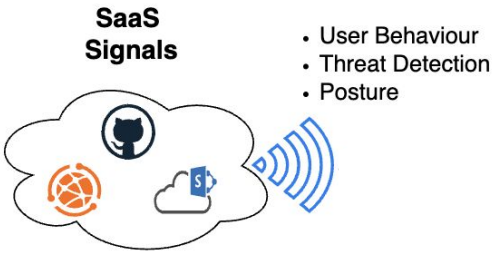
Shared Signals Working Group
OpenID Foundation

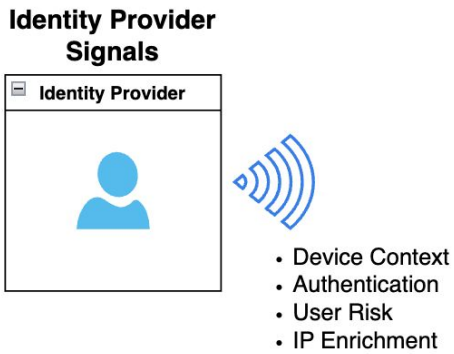
The **OpenID Shared Signals Framework (SSF)** provides a **standardized approach** for identity systems to **communicate events** in a **trusted way** between parties to **improve security and user experience**.

Goals

- Enable ***real-time*** communication of ***critical security events***
- *Reduce complexity* by *standardizing* ***event formats*** and ***delivery mechanisms***
- Enhance ***interoperability*** across ***identity systems***

Enhancing SaaS Security with SSF





Credits to AppOmni / Okta

SSF Usage Examples

- **Real-Time Session Revocation**
  Revoke sessions instantly when risk conditions change, ensuring real-time access control.

- **Compromised Account Alert**
  Notify Keycloak when an IdP detects account compromise, triggering security measures.

- **Automated User Deprovisioning**
  Sync user lifecycle events to revoke access upon termination, preventing orphaned accounts.

SSF Building Blocks

- **Transmitter**

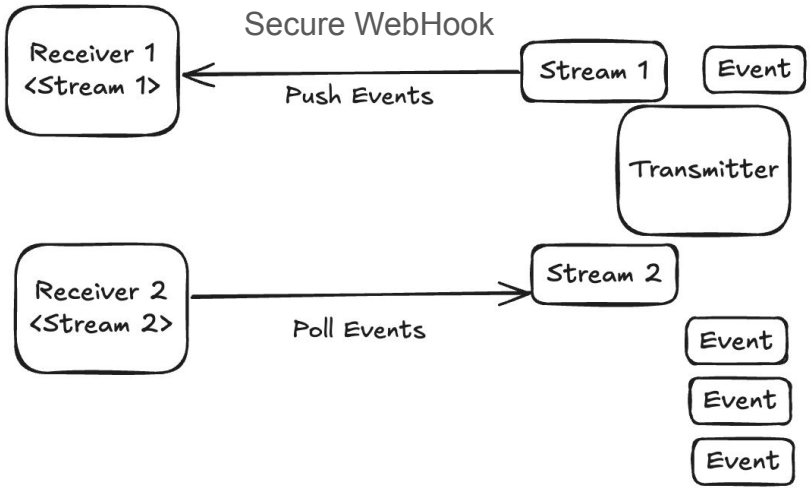
  System generating and emitting an Security event, e.g. an Identity Provider.

- **Receiver**

  System consuming the event, e.g., a Service Provider.

- **Stream**

  Logical *subscription* for a set of events managed by a *Receiver*, but stored on a *Transmitter*



Event and Subject Format

SET (Security Event Token) RFC 8417

- A **JSON Web Token (JWT)** based **format** for conveying **security-related events**.
- Includes event type, event payload, subject identifier, and metadata.
- Signed by SSF Transmitter for Non-repudiation and Integrity Protection

Subject Identifiers RFC 9493

- A standardized way to **identify entities** across systems.
- Can be a **person**, **device**, **group** or **organization**, etc.
- Types of Subject Identifiers: `iss_sub`, `email`, `phone_number`, `opaque`, etc.

ENCODED VALUE

JSON WEB TOKEN (JWT) COPY CLEAR

Valid JWT

Fix public key input errors to verify signature.


```
eyJhbGciOiJSUzI1NiIsImtpZCI6IjllMjJlMjc2LWQzYTQtNGE2OS1hZDA4LWQyNmNmNWI0
Y2ExOSIsInR5cCI6InNlY2V2ZW50K2p3dCJ9.eyJhdWQiOiJodHRwczovL3Rkd29ya3Nob3B
zLm5ncm9rLmRldi9hdXRoL3JlYWxtcy9zc2YtZGVtbyIsImV2ZW50cyI6eyJodHRwczovL3N
jaGVtYXMub3BlbmlkLm5ldC9zZWNldmVudC9jYWVwL2V2ZW50LXR5cGUvc2Vzc2lvbi1yZXZ
va2VkIjp7ImV2ZW50X3RpbWVzdGFtcCI6MTczODYyMTQzOCwic3ViamVjdCI6eyJlbWFpbCI
6InRlc3RlckBsb2NhbC50ZXN0IiwiZm9ybWF0IjoiZW1haWwifX19LCJpYXQiOjE3Mzg2MjE
0MzgsImlzcyI6Imh0dHBzOi8vc3NmLmNhZXAuZGV2LyIsImp0aSI6IlkyWmxaV05tWmpjdFp
XRmlNUzAwT0RRMUxXSTJNMlF0TVRjeFlqY3pNMkppTlRjMCIsInN1Yl9pZCI6eyJlbWFpbCI
6InRlc3RlckBsb2NhbC50ZXN0IiwiZm9ybWF0IjoiZW1haWwifX0.Xy71Z-
jdELCbXFWAzaTb298XtRCQCZhyFX8qp9DXLYGBbQet6k-
xbZDAz5B8CtlapMf5ogBAb7nGep-Gs0L1T-
KfdtkTpCLYKrfsStBnmeB1b7sXrshLtEsqhTvL_3CtQHOPUewGAp0z9wMH_M23b4ldzTQDnD
Ywx6oPiyS2TQt3G_k8R0FnmOhqLs9o3RLW1rvSdPdxkmVnxu9mK56CfT8A7EZCC--
aqWwCC4lqj_kizC8sp1C2ezjohrhkkZvz3lvQUh2O9Ij81E_bWOZf4cvvfwegL8yTl96z7tV
KH1DS1rO9R4w4WyiMFLMeXWa_3vwpK5g6QSpMdFtqRR2nIg
```


DECODED HEADER

JSON CLAIMS TABLE COPY


```
{
  "alg": "RS256",
  "kid": "9e22e276-d3a4-4a69-ad08-d26cf5b4ca19",
  "typ": "secevent+jwt"
}
```


DECODED PAYLOAD

JSON CLAIMS TABLE COPY


```
{
  "aud": "https://tdworkshops.ngrok.dev/auth/realms/ssf-demo",
  "events": {
    "https://schemas.openid.net/secevent/caep/event-type/session-revoked": {
      "event_timestamp": 1738621438,
      "subject": {
        "email": "tester@local.test",
        "format": "email"
      }
    }
  },
  "iat": 1738621438,
  "iss": "https://ssf.caep.dev/",
  "jti": "Y2ZlZWNmZjctZWFiMS00ODQ1LWI2M2QtMTcxYjczM2JiOTc0",
  "sub_id": {
    "email": "tester@local.test",
    "format": "email"
  }
}
```


Security Event Token Example

Event Profiles: CAEP, RISC

Event Profile = A set of event definitions

CAEP (Continuous Access Evaluation Protocol) 1.0 - draft 03

- **SSF profile** that enables **continuous monitoring** and **evaluation of access decisions**.
- Example events: session-revoked, token-claims-changed, risk-level-changed

RISC (Risk and Incident Sharing and Coordination) 1.0 - draft 02

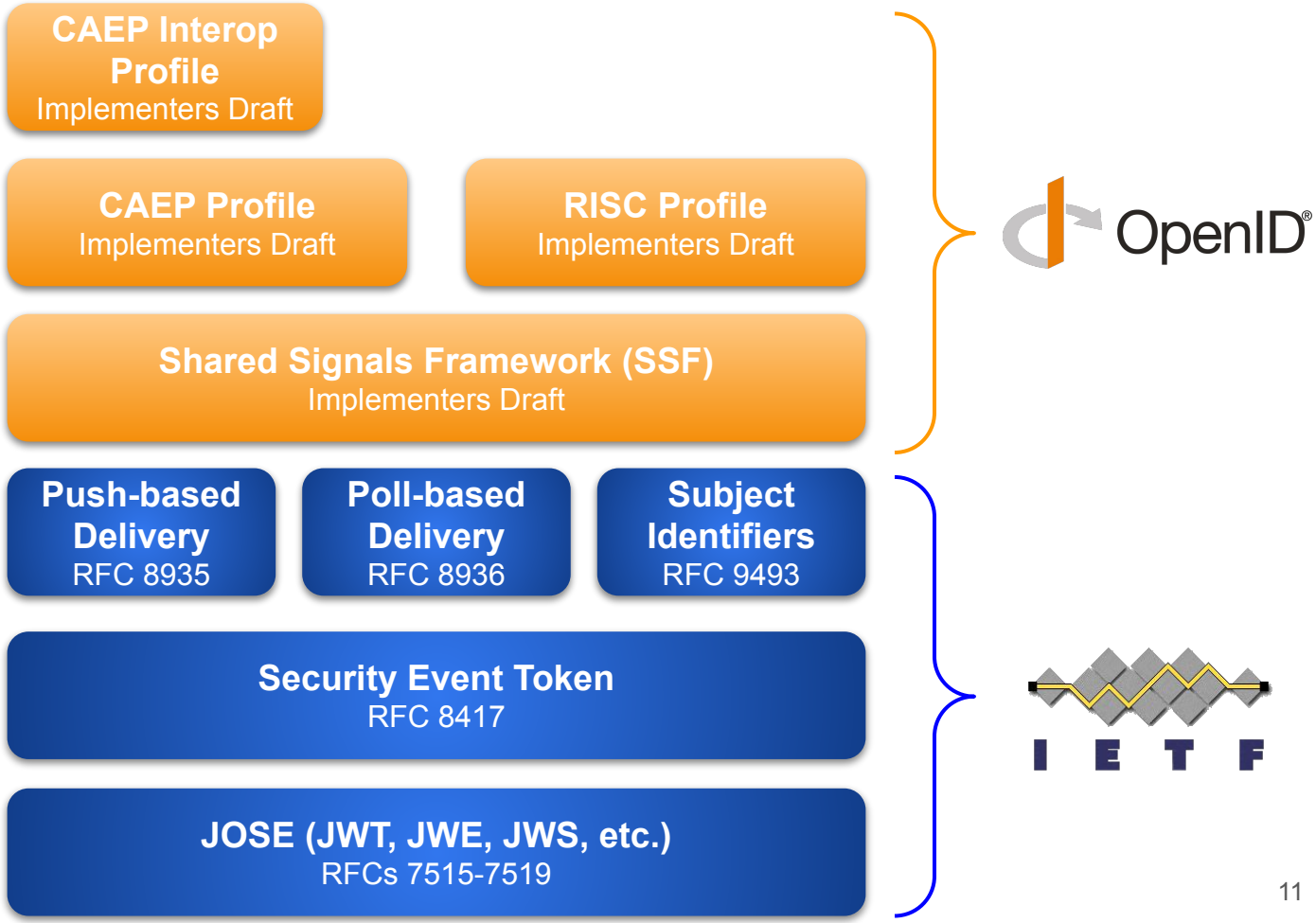
- **SSF profile** focused on disaster mitigation and is related to **security risks and incidents**.
- Example events: credential-compromised, credential-change-required, account-disabled, etc.

SET Delivery Options: Push and Poll

- **Push Model RFC 8935**
  - Push-Based Security Event Token (SET) Delivery Using HTTP
  - Transmitter sends events to **Push-endpoint on Receiver** via HTTP POST
  - Enables **Real-Time Event Delivery**

- **Poll Model RFC 8936**
  - Poll-Based Security Event Token (SET) Delivery Using HTTP
  - Receiver periodically fetches events from the **Transmitter's Poll-endpoint**.
  - Enables **Async Event Delivery**

SSF Protocol Stack



SSF Summary

Risk Incident Sharing and Coordination (RISC)

Account Security Events

- Account disabled
- Account suspended
- Credentials Compromised
- …

Continuous Access Evaluation Protocol (CEAP)

Session Management Events

- Session Revoked
- Token Claims Changed
- Risk Level Changed
- …

SCIM Events

Entity Provisioning Events

- Account Created
- Account Updated
- Account Deleted
- …

Shared Signals Framework

- Asynchronous Publish/Subscribe Webhook Framework
- Stream of Security Event Tokens (SETs) - JWT format
- Subject identification (e.g. User, Group, Org, Tenant)
- Event Stream Management
- Push & Poll Delivery/Transport with Acknowledgement

Credits Sailpoint

Relationship between SSF and SCIM

- **SCIM (System for Cross-domain Identity Management)**
  - Standard for managing identity information across domains.
  - Events in SCIM (e.g., user creation, deletion, suspension) complement SSF Events.
- **Key Difference**
  - **SCIM** focuses on ***User Lifecycle Management***
  - **SSF** (CAEP, RISC) addresses **security** and risk-related ***event sharing***.
- **Integration with SSF**
  - SSF as transport layer for SCIM Events for sharing lifecycle events.
  - SCIM Profile for Security Event Tokens IETF Draft

Shared Signals Framework Adopters (*)

- AppOmni
- caep.dev
- Cisco
- Delinea
- Google
- IBM
- Jamf
- Okta **
- Omnissa
- SailPoint
- Saviynt
- SGNL
- Thales
- WinMagic
- Apple **

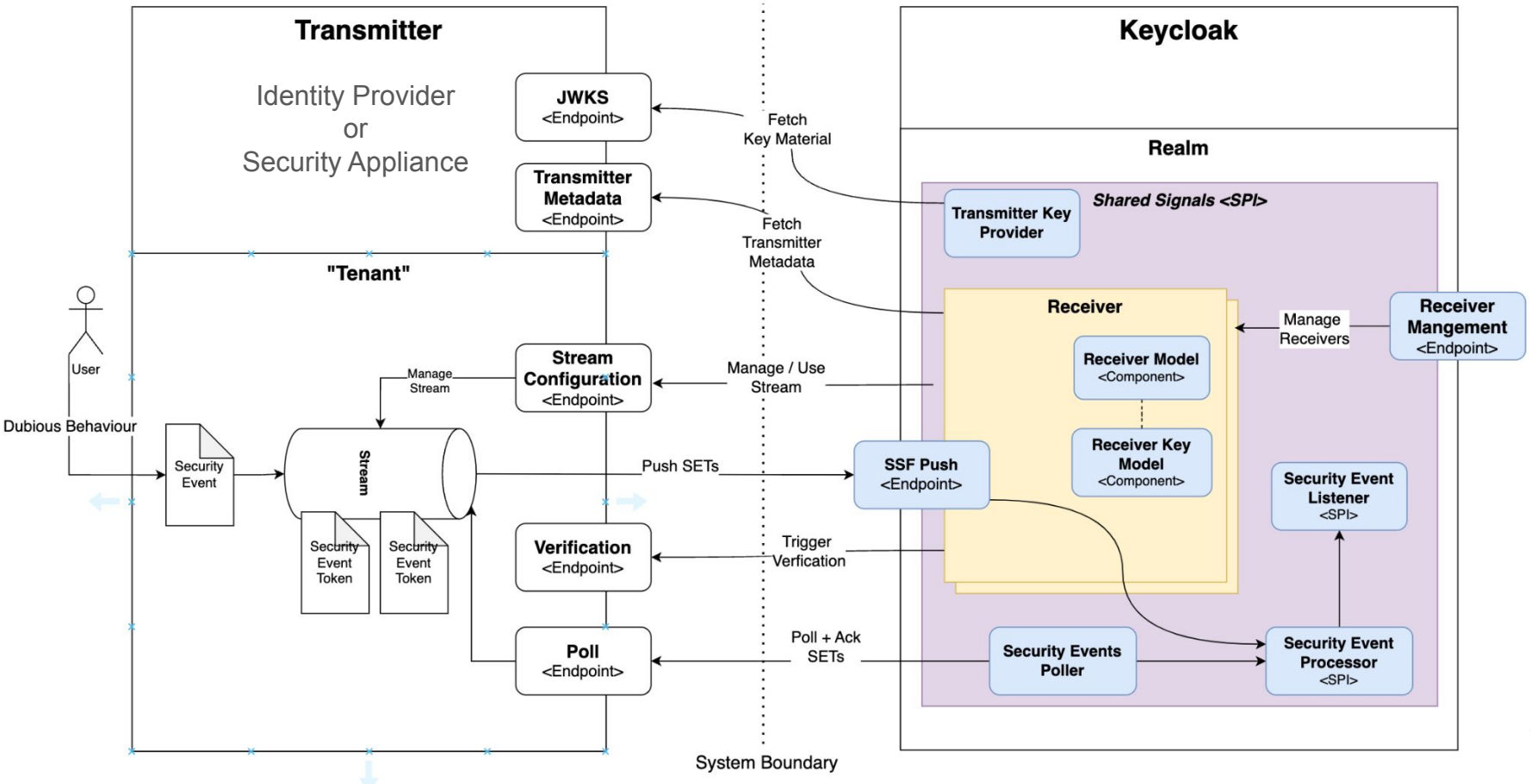
*) based on Participation survey at Gartner IAM SSF Interop Event January 2025 or **) Product Documentation

SSF Support for Keycloak

- **Keycloak as SSF Transmitter**
  - Keycloak could emit CAEP/RISC events to interested parties (IdP Broker, SaaS apps)
  - Keycloak could notify “child” Identity providers about account changes, suspension
  - Challenges ****
    i. Stream Management and Scalable Event Storage
    ii. Polling / Push Infrastructure

- **Keycloak as SSF Receiver** **(This Talk)**
  - Keycloak can receive / fetch CAEP/RISC/SCIM events from trusted parties
  - Identity Providers could propagate Session revocations, Account removal/suspension
  - Challenges ***
    i. SSF Stream Management Client
    ii. Event Ingestion and Event-Handling Infrastructure

Architecture: Keycloak as SSF Receiver



Keycloak Shared Signals Framework Extension Demo

Repository with PoC: https://github.com/identitytailor/keycloak-ssf-support

caep.dev

Transmitter Receiver Learn Developer NEW About Register

Brought to you by sgnl

caep.dev is a service that enables Shared Signals Framework developers to test their Transmitters and Receivers. It implements the SSF draft specification and the CAEP draft specification required to operate the Transmitter and Receiver.

Register for a caep.dev access token

Start Transmitting

Use the Transmitter to generate and send CAEP events to your Receiver

Start Receiving

Use the Receiver to collect events from your Transmitters

New: Join the discussion and track or report issues on GitHub!

Shared Signals Framework (SSF) Summary

- **SSF** standardizes real-time event delivery for identity systems.
- ***Continuous Access Evaluation*** and ***Compromised Account Mitigation*** demonstrate its practical impact.
- **SET**, **RISC**, and **CAEP**, along with flexible and **secure delivery mechanisms**, can enable robust event sharing.
- **SSF** and **SCIM** can **work together** to improve both identity lifecycle management and security operations.
- **SSF Receiver Support** can be **added as an extension** to **Keycloak**

Question

“Would SSF support add valuable to your Keycloak based Environments?”

- As a Keycloak Extension?
- As part of Keycloak?
- As a separate Appliance?

Thank you!

Questions?

Feedback?

❤️

OpenID®

Contact: thomas@identity-tailor.de

Event Profiles: CAEP, RISC

CAEP (Continuous Access Evaluation Protocol) 1.0 - draft 03

- **SSF profile** that enables **continuous monitoring** and **evaluation of access decisions**.
- Example events: session-revoked, token-claims-changed, risk-level-changed

CAEP Interoperability Profile 1.0 - draft ID01

- **CAEP profile** that enables **interoperability between** connected **parties**
- Limits options for transmitters and receivers

RISC (Risk and Incident Sharing and Coordination) 1.0 - draft 02

- **SSF profile** focused on disaster mitigation and is related to **security risks and incidents**.
- Example events: credential-compromise, credential-change-required, account-disabled, etc.