Security Event Tokens, Subject Identifiers, and SSE/CAEP/RISC Java implementation

Matt Domsch, VP & Engineering Fellow

Specs

- Security Event Tokens – RFC 8417
- Subject Identifiers – Internet Draft RFC
- Shared Signals & Events – OpenID Foundation WG
  - Includes RISC, CAEP, and Oauth event profiles

SailPoint

Shared Signals and Events

Goal

Enable the sharing of security events, state changes, and other signals between related and/or dependent systems in order to:

• Manage access to resources and enforce access control restrictions across distributed services operating in a dynamic environment.

• Prevent malicious actors from leveraging compromises of accounts, devices, services, endpoints, or other principals or resources to gain unauthorized access to additional systems or resources.

• Enable users, administrators, and service providers to coordinate in order to detect and respond to incidents.

- Google
- AWS
- Microsoft
- Thales
- SailPoint
- SecureAuth
- Oracle
- Prove
- Tesla
- UK Foreign & Commonwealth Office
- Coinbase
- Vericlouds
- VMWare
- OneLogin
- Duo
- Okta
- Verizon Media
- RSA
- Intuit
- Ping Identity
- Blackberry

SailPoint

Interesting Events

- User account is disabled/deleted in their directory
- User changes their password in their directory
- Access request is granted
- User changes their email address
- A phone company re-assigns a previously issued phone number to a new customer
- A user's credentials are found to have been leaked onto the Dark Web
- A device makes impossible travel to a new continent
- A bank recognizes fraudulent transaction attempts

Reactions

- Revoke the user's active application sessions
- Make the user re-authenticate to continue using their active application sessions
- Upgrade a user's active application session permissions
- Unlink the phone number from the previous customer record
- Force users through a password reset flow on next login

In use today!

- Google Identity Cross-Account Protection
- Microsoft Azure Active Directory Continuous Access Evaluation
- Login.gov
- SailPoint Java library @ GitHub sailpoint-oss/openid-sse-model

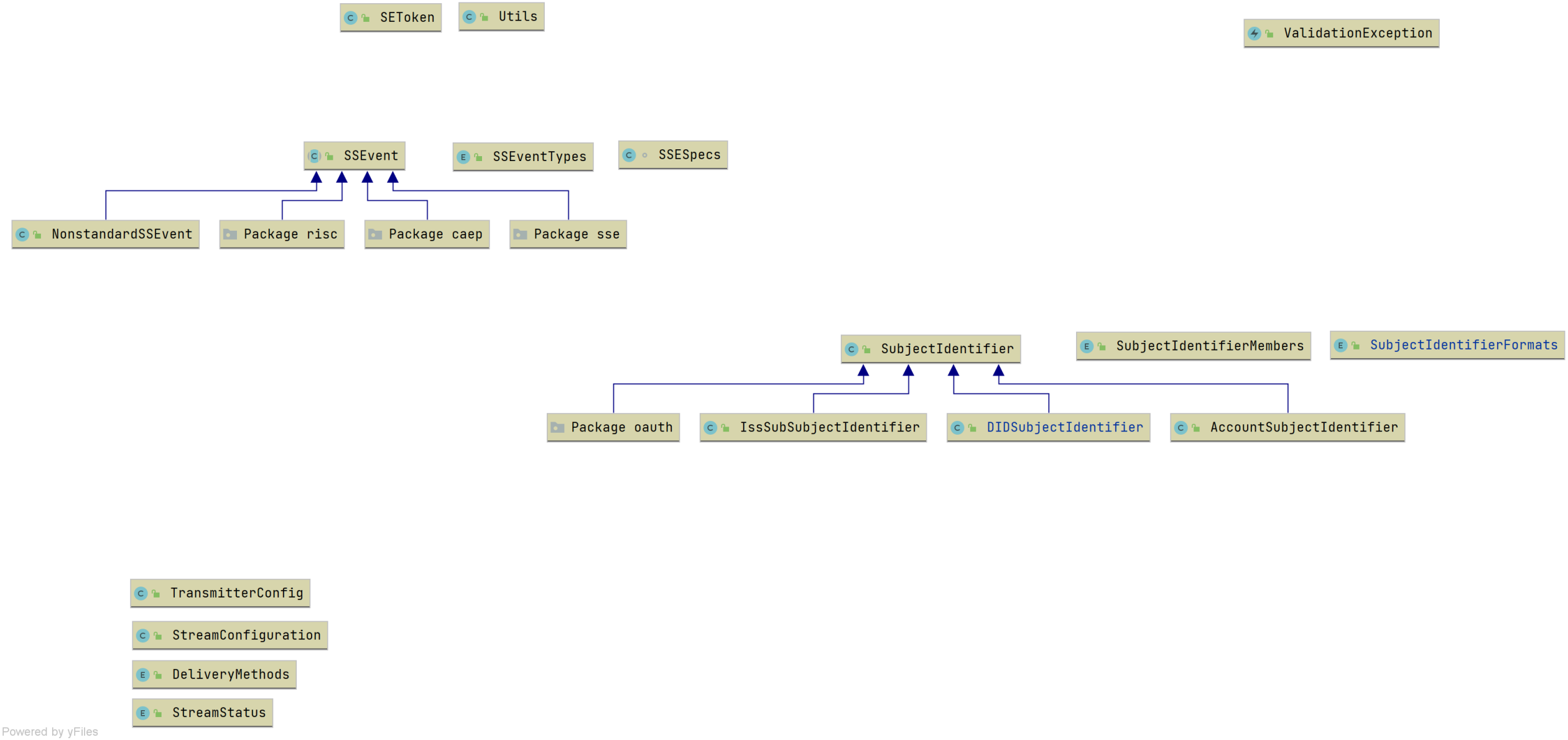
SailPoint

OpenID-SSE-model

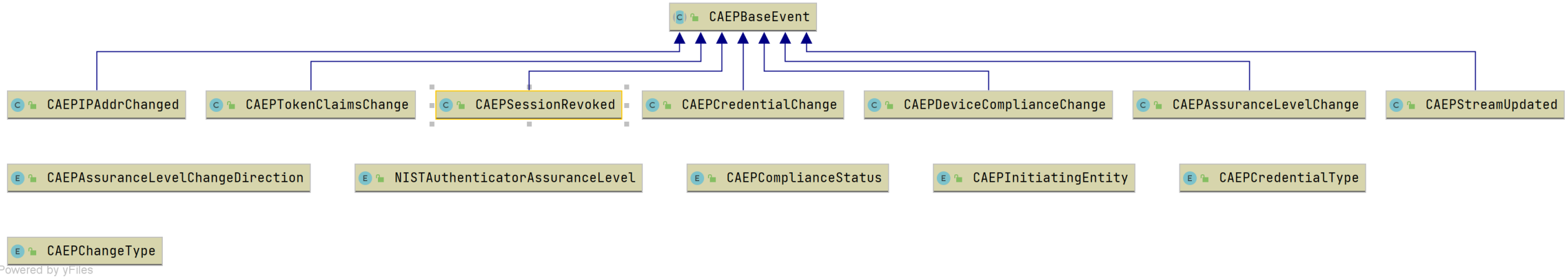
- Open Source (Apache 2) Java Library
- Builds on Nimbus-JOSE-JWT (JWTClaimsSet, JSONObject)
- Security Event Tokens (SETs)
- Shared Signals & Events
- CAEP & RISC profile events
- Builders for every event type
- Parsers with event-specific validation

SailPoint

```java
@Test
public void Figure5() throws ParseException, ValidationException {
    SubjectIdentifier subj = new SubjectIdentifier.Builder()
            .format(SubjectIdentifierFormats.EMAIL)
            .email("foo@example.com")
            .build();

    RISCAccountEnabled evt = new RISCAccountEnabled.Builder()
            .subject(subj)
            .build();

    JWTClaimsSet set = new JWTClaimsSet.Builder()
            .issuer("https://idp.example.com/")
            .jwtID("756E69717565206964656E746966696572")
            .issueTime(DateUtils.fromSecondsSinceEpoch( time: 1520364019))
            .audience("636C69656E745F6964")
            .claim(SEToken.EVENTS_CLAIM, evt)
            .build();

    final String figure_text = "{\n" +
            "  \"iss\": \"https://idp.example.com/\",\n" +
            "  \"jti\": \"756E69717565206964656E746966696572\",\n" +
            "  \"iat\": 1520364019,\n" +
            "  \"aud\": \"636C69656E745F6964\",\n" +
            "  \"events\": {\n" +
            "    \"https://schemas.openid.net/secevent/risc/event-type/account-enabled\": {\n" +
            "      \"subject\": {\n" +
            "        \"format\": \"email\",\n" +
            "        \"email\": \"foo@example.com\"\n" +
            "      }\n" +
            "    }\n" +
            "  }\n" +
            "}";

    final JSONObject figureJson = new JSONObject(JSONObjectUtils.parse(figure_text));
    final JSONObject setJson = new JSONObject(set.toJSONObject());
    assertEquals(figureJson, setJson);
    evt.validate();

    JWTClaimsSet parsedSet = SEToken.parse(figure_text);
}
```



CAEP Package classes



Thank You