Security Events Draft Proposals

Phil Hunt, Oracle
Marius Scurtescu, Google
IETF97 Seoul
Security Events Working Group
November 2016

Drafts

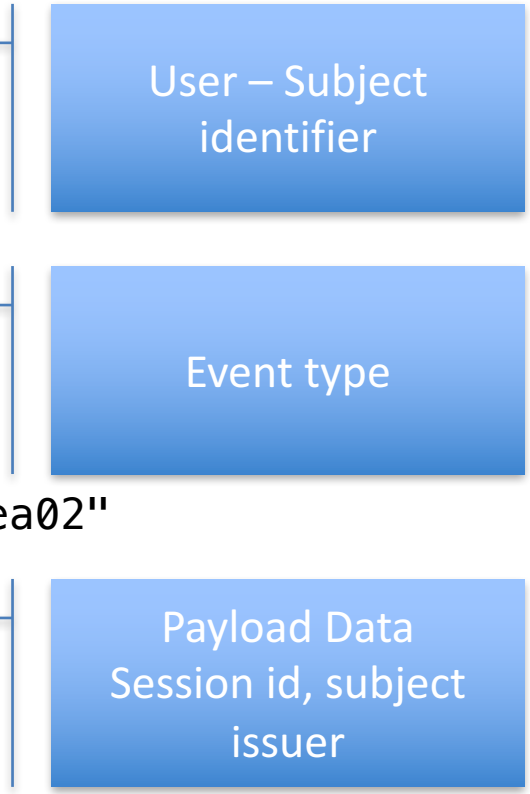
- SET Token
  - https://tools.ietf.org/html/draft-hunt-idevent-token-06
  - Profiles RFC 7519 JWT Token
- SET Distribution
  - https://tools.ietf.org/html/draft-hunt-idevent-distribution-01
  - Control-plane
    - SCIM used to manage/operate pub sub relationships (profile of RFC7644/43 SCIM)
  - Data Plane
    - Simple assured delivery method using HTTP POST
    - Registry for defining new methods

The SET Token

- Profile of JWT token
  - Reuses key attributes: jti, iat, iss, aud, nbf, sub
  - New attributes
    - events – a list of URIs declaring the type of event
    - txn – a unique identifier for the originating transaction
    - event objects – a JSON attribute whose name is the event URI and whose value is a JSON object containing one or more event specific attributes
- May use JWS and JWE to sign and encrypt

Example OpenID Logout SET

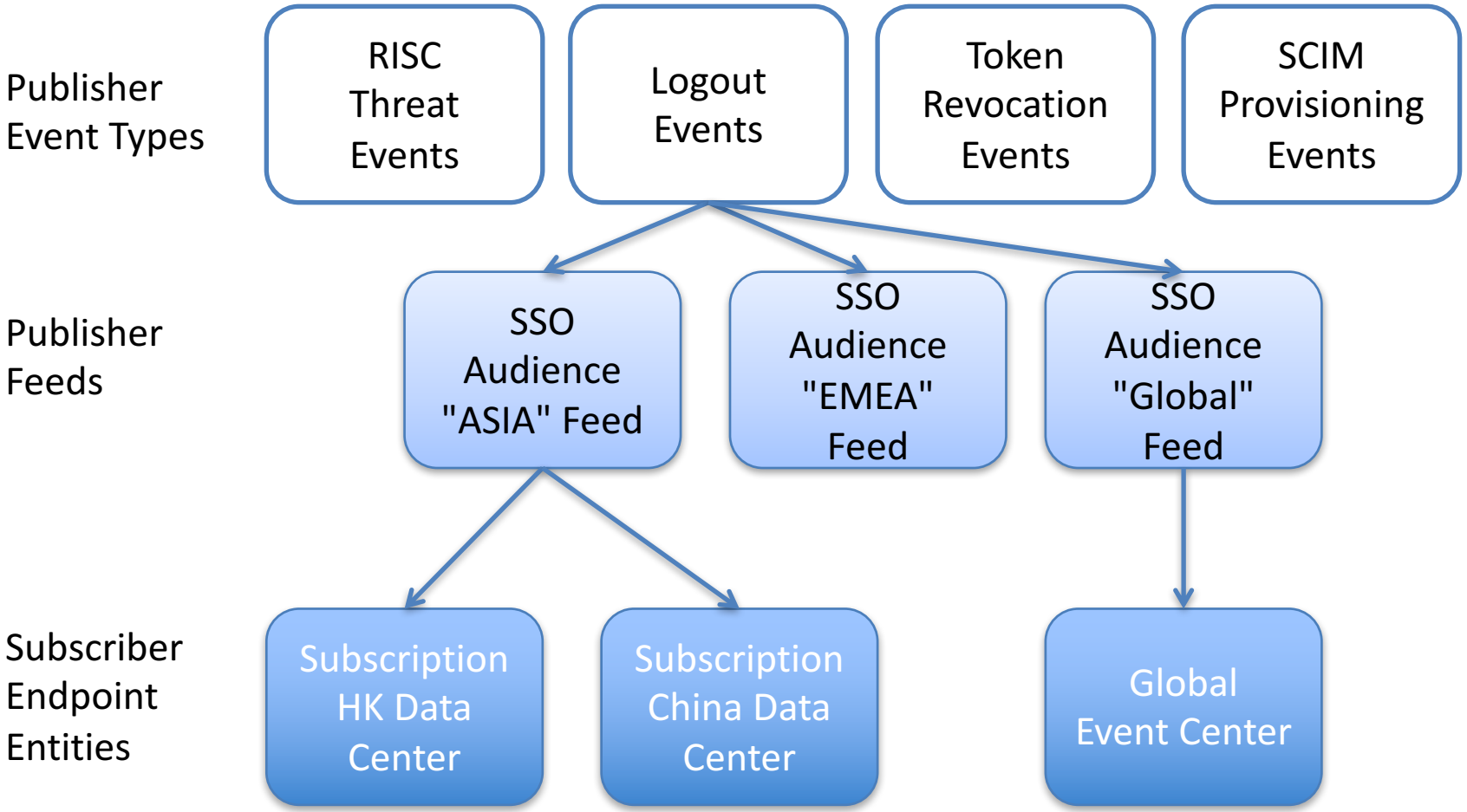

```
{
   "iss": "https://server.example.com",
   "aud": "https://rp.example.com",
   "jti": "3d0c3cf797584bd193bd0fb1bd4e7d30",
   "iat": 1458668180,
   "exp": 1458668580,
   "sub": "248289761001",
   "events": [
     "https://specs.openid.net/logout"
   ],
   "https://specs.openid.net/logout": {
     "iss": "https://token.example.com",
     "sid": "08a5019c-17e1-4977-8f42-65a12843ea02"
   }
 }
```

SET Delivery

- Initial draft will contain HTTPS POST (webcallback) method
  - Each HTTPS POST delivers 1 message
  - HTTP Status 202 Response is used to confirm receipt
  - Error response JSON for Status 400 errors relating to JWT processing/validation

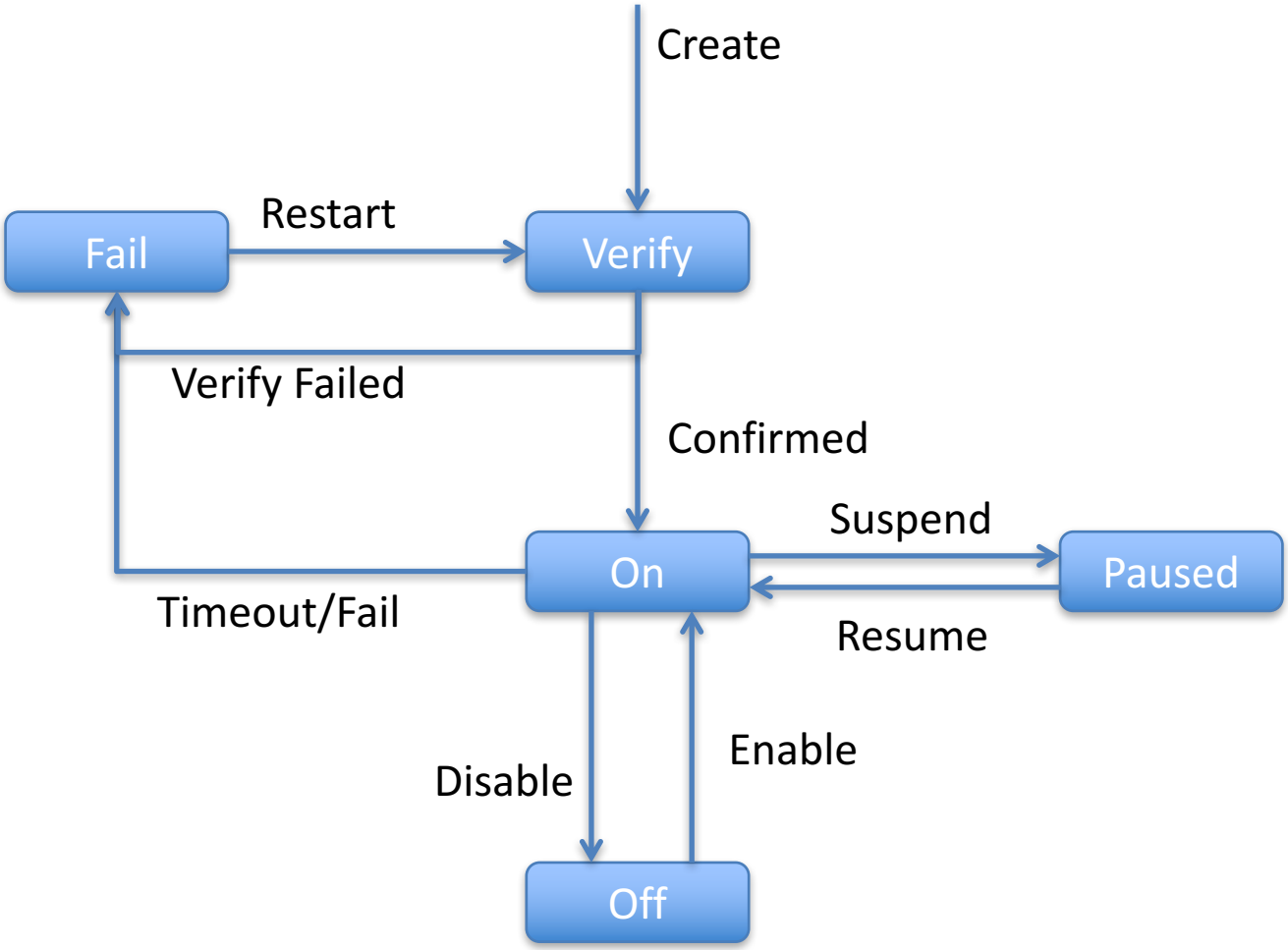
Feeds & Subscriptions



Subscriptions

- SCIM represents the "control-plane" for managing events
- Used to manage a subscription for a particular subscribing client end-point
- Represents a single event transmission "path"
- Indicates delivery method, endpoints, feed status, JWT config (eg keys), operational params (eg intervals)

Subscription State



Example Subscription Inquiry

```
GET /Subscriptions/767aad7853d240debc8e3c962051c1c0
Host: example.com
Accept: application/scim+json
Authorization: Bearer h480djs93hd8

HTTP/1.1 200 OK
Content-Type: application/scim+json
Location:
 https://example.com/v2/Subscriptions/767aad7853d240debc8e3c962051c1c0

{
  "schemas":["urn:ietf:params:scim:schemas:event:2.0:Subscription"],
  "id":"767aad7853d240debc8e3c962051c1c0",
  "feedName":"OIDCLogoutFeed",
  "feedUri":
    "https://example.com/v2/Feeds/88bc00de776d49d5b535ede882d98f74",
  "methodUri":"urn:ietf:params:set:method:HTTP:webCallback",
  "deliveryUri":"https://notify.examplerp.com/Events",
  "aud":"https://sets.myexamplerp.com",
  "subStatus":"pending",
  "maxDeliveryTime":3600,
  "minDeliveryInterval":0,
  "description":"Logout events from oidc.example.com",
}
```

Defines the content

Current operational status

Pausing a Subscription (SCIM PUT)

```
PUT /Subscriptions/767aad7853d240debc8e3c962051c1c0
Host: example.com
Accept: application/scim+json
Content-Type: application/scim+json
Authorization: Bearer h480djs93hd8

{

"schemas":["urn:ietf:params:scim:schemas:event:2.0:Subscription"],
 "id":"767aad7853d240debc8e3c962051c1c0",
 "feedName":"OIDCLogoutFeed",
 "feedUri":

"https://example.com/v2/Feeds/88bc00de776d49d5b535ede882d98f74",
 "methodUri":"urn:ietf:params:set:method:HTTP:webCallback"
 "deliveryUri":"https://notify.examplerp.com/Ev
 "aud":"https://sets.myexamplerp.com",
 "subStatus":"paused",
}
```

Subscriber requests subscription to pause

Note: Can also be completed with SCIM PATCH

Verifying a Subscription

- Confirms correct endpoint config
- Co-ordinate the start of feed / DevOps Co-ord
- Confirm clients acceptance of subscription
  - Prevent unauthorized subscription
  - DoS Prevention
- Sends a test event (a verify/ping) that confirms configuration of endpoints
  - Can be used to periodically verify operation when usage is infrequent

Verification SET

SET Verification Token

```
{
  "jti": "4d3559ec67504aaba65d40b0363faad8",
  "events":["[[this RFC URL]]#verify"],
  "iat": 1458496404,
  "iss": "https://scim.example.com",
  "exp": 1458497000,
  "aud":[
   "https://scim.example.com/Feeds/98d52461fa5bbc879593b7754",
   "https://scim.example.com/Feeds/5d7604516b1d08641d7676ee7"
  ],
  "[[this RFC URL]]#verify":{
    "confirmChallenge":"ca2179f4-8936-479a-a76d-5486e2baacd7"
  }
}
```

On receipt, receiver responds with…

```
HTTP/1.1 200 OK
Content-Type: application/json
{
  "challengeResponse":"ca2179f4-8936-479a-a76d-5486e2baacd7"
}
```

Discussion

- SET Token
  - Proposal from Justin to optimize payload
    - e.g. as JSON object of events

```
"events”: {
        "urn:ietf:params:scim:event:passwordReset":{
          "id":"44f6142df96bd6ab61e7521d9"
        },
        "
 },
```

- SET Distribution
  - Useful to list Feeds for discovery purposes?
  - Subscription management
    - Is verify useful?
  - Proposal from Tony to not restrict subscription management to SET based events
    - E.g. allow extension for management of STIX/TAXII and other XML forms