“Pushpull” delivery of SETs

Atul Tulshibagwale
LinkedIn, GitHub: @tulshi

SGNL

Aaron Parecki
LinkedIn: @aaronparecki
GitHub: @aaronpk

Okta

Apoorva Deshpande
LinkedIn, GitHub: @appsdesh

Okta

Background

The secevent WG was active from Sep 2016 through June 2023

RFC 9493 **Subject Identifiers for Security Event Tokens**	18 pages Errata	2023-12
RFC 8935 **Push-Based Security Event Token (SET) Delivery Using HTTP**	15 pages	2020-11
RFC 8936 **Poll-Based Security Event Token (SET) Delivery Using HTTP**	16 pages	2020-11
RFC 8417 **Security Event Token (SET)**	28 pages Errata	2018-07

Push Delivery (RFC 8935)

Sender delivers a single event

```
POST /Events HTTP/1.1
Host: notify.rp.example.com
Accept: application/json
Content-Type: application/secevent+jwt

eyJ0eXAiOiJzZWNldmVudCtqd3QiLCJhbGciOiJIUzI1NiJ9Cg.
eyJpc3MiOiJodHRwczovL2lkcC5leGFtcGxlLmNvbS8iLCJqdGkiOiI3NTZFNjk
3MTc1NjUyMDY5NjQ2NTZFNzQ2OTY2Njk2NTcyIiwiaWF0IjoxNTA4MTg0ODQ1LC
JhdWQiOiI2MzZDNjk2NTZFNzQ1RjY5NjQiLCJldmVudHMiOnsiaHR0cHM6Ly9zY
2hlbWFzLm9wZW5pZC5uZXQvc2VjZXZlbnQvcmlzYy9ldmVudC10eXBlL2FjY291
bnQtZGlzYWJsZWQiOnsic3ViamVjdCI6eyJzdWJqZWN0X3R5cGUiOiJpc3Mtc3V
iIiwiaXNzIjoiaHR0cHM6Ly9pZHAuZXhhbXBsZS5jb20vIiwic3ViIjoiNzM3NT
YyNkE2NTYzNzQifSwicmVhc29uIjoiaGlqYWNraW5nIn19fQ.
Y4rXxMD406P2edv00cr9Wf3_XwNtLjB9n-jTqN1_lLc
```

Poll Delivery (RFC 8936)

```
POST /Events HTTP/1.1
Host: notify.idp.example.com
Content-Type: application/json

{
   "returnImmediately": true,
   "ack": ["3d0c3cf797584bd193bd0fb1bd4e7d30"]
}
```

Receiver asks for events and acknowledges previously received event

```
HTTP/1.1 200 OK
Content-Type: application/json

{
 "sets":
  {
   "eyJqdGkiOiI0ZDM1NTllYzY3NTA0YWFiYTY1ZDQwYjAzNjNmYWFkOCIsImlhdC
    L3NjaW0uZXhhbXBsZS5jb20vVXNlcnMvNDRmNjE0MmRmOTZiZDZhYjYxZTc1Mj
    FkOSIsImF0dHJpYnV0ZXMiOlsiaWQiLCJuYW1lIiwidXNlck5hbWUiLCJwYXN",
   "eyJqdGkiOiIzZDBjM2NmNzk3NTg0YmQxOTNiZDBmYjFiZDRlN2QzMCIsImlhdC
    I6MTQ1ODQ5NjAyNSwiaXNzIjoiaHR0cHM6Ly9zY2ltLmV4YW1wbGUuY29tIiwi
    dvcmRSZXNldCI6eyJpZCI6IjQ0ZjYxNDJkZjk2YmQ2YWI2MWU3NTIxZDkifSwi
    aHR0cHM6Ly9leGFtcGxlLmNvbS9zY2ltL2V2ZW50L3Bhc3N3b3JkUmVzZXRFeH
    QiOnsicmVzZXRBdHRlbXB0cyI6NX19fQ."
  }
}
```

Sender delivers new event in HTTP response

Pushpull Delivery: Communication Object

- Common JSON object that contains (all optional):
  - Multiple SETs to transfer to the recipient
  - An array of previous SETs to be acknowledged
  - Multiple error objects
- Similar to a HTTP Response in “Delivery Poll” (RFC8936)


```
{
  "sets": {
    "4d3559ec67504aaba65d40b0363faad8":
          "eyJ … d29yZCYWlscyJdfX19.",
    "3d0c3cf797584bd193bd0fb1bd4e7d30":
          "eyJ … QiOnsicmVzZXRBdl."
  },
  "ack": [
    "f52901c4-3996-11ef-9454-0242ac120002",
    "0636e274-3987-a1c3-3149-0215ac132142",
    "d563c724-79a0-4ff0-ba41-657fa5e2cb11"
  ],
  "setErrs": {
    "5c436b19-0958-4367-b408-2dd542606d3b" : {
      "err": "invalid subject",
      "description": "subject format not
supported"
    }
  }
}
```

Pushpull Delivery: Transport options

- Always a Communication Object
- HTTP Request Response binding
  - Requests can have an additional “maxResponseEvents” field
- WebSocket binding
  - WebSocket Subprotocol: `pushpull`
  - Communication Object is the Payload data
- Any initiator can request upgrade to WebSocket, and they must use WebSocket if handshake succeeds

Developments since IETF 122

- Combined "Pushpull" with "Multi-SET Push Delivery" - new draft is still called "Pushpull"
- Feedback received on:
  - Multi-SET Push
  - Pushpull
- Feedback response provided

Feedback Points

- Multi-SET Push
  - “Incremental work without significant engineering advantages”
  - Creates interoperability disadvantage

- Pushpull
  - Idea is not new. Another proposal here: “Symmetric SET Transfer Protocol” (expired 2018)
    - Some differences, but largely the same
  - Incremental work without significant engineering advantages
  - Creates interoperability disadvantage

Feedback response

- SSTP - merge authors
  - Pushpull seems to be a superset of SSTP

- “Incremental work” response:
  - No async acknowledgement of pushed events
  - No way to detect “zombie streams”
  - Efficiency improvement

- Interoperability disadvantage
  - Nascent adoption of these specs at this time - SSF is the biggest adopter

Efficiency improvement requirement

- Requirement: Implement cloud ITDR
  - Send CAEP "session established" and "session presented" events periodically for each active user.
  - Millions of active users at each app, tens of apps, assume period is 1 minute.
  - Push is convenient for lightweight Transmitters - no HTTP server required.
  - Single push per connection would be too expensive

- Single bidirectional stream instead of two unidirectional streams reduces overhead, simplifies architecture.

- Vision: SSF becomes the HTTP of asynchronous communication