SCIM Events Update

draft-ietf-scim-events-01

IETF 116, Yokohama
SCIM Working Group Meeting

March 28, 2023

Phil Hunt

Nancy Cam-Winget

Background

- SCIM Events defines a series of events that can be expressed in Security Event Token format per RFC8417
- A SET (RFC8417) is:
  - A type of JWT which may be signed and encrypted
  - Is passed as a statement that an event occurred at a specific time (toe) which may be distinct from the time the SET was issued (iat)
  - A SET is a signal which allows for independent action (see OpenID Shared Signals)
- SETs may be transferred by any method supported by JWT but in particular:
  - RFC8935 HTTP Push-Based SET Delivery
  - RFC8936 HTTP Poll-Based SET Delivery
  - RFC8935/8936 support real-time, verified transfer including ACK and recovery

Working Group Draft 01

- Added privacy, security, and IANA sections
- Moved use-case information to appendix
- Revised to align better with https://openid.net/wg/sharedsignals/
  - Added support for draft-ietf-secevent-subject-identifiers-16 (in final publication review)
- Section 2 defines 4 classes of events:
  - Feed Events – Adding and removing subjects from a stream of events
  - Provisioning Events – Mimic SCIM operations (same format as SCIM BULK)
  - Signal Events – High-level events such as password reset or auth change
  - Async Events – Method for confirming a long-running SCIM operation is complete (future)

Draft 01 - Continued

- Section 3 discusses event delivery and recovery
  - Discussed how and when to use JWT Plain text (alg=none), JWS signing, and JWE encryption in SCIM scenarios
- Provides clarification on the context events are exchanged
  - Addresses concerns raised such as "RFC8935,8936 have no recovery method"
  - RFC8935/8936 SET transfer typically happens between domains
    - Inter-domain recovery *not the same* as Node recovery or cluster replication
    - Push/Poll RFCs define a minimum (but not limited) recovery to ensure information is transferred, secured, and acknowledged.
    - Because of scale requirements (publishers with 1000s or 100Ks of clients) the SECEVENTS WG decided that event issuers are not responsible for maintaining event history indefinitely. Receiving domains are responsible for their own recovery once they ack an event.

Privacy and Security Considerations

- Security Considerations build on the security considerations of
  - RFC8417 Security Event Tokens
  - RFC8935/8936 HTTP Transfer of SET Tokens
  - Details requirements for timeliness and recovery
  - Less may be more when it comes to high-rate change resources like groups
- Privacy Considerations
  - Builds on 8417,8935,8936 as above
  - The ability to share information is based on either:
    - A common administrative domain (e.g., where there is one owner of the data)
    - A co-operative relationship where parties or individuals have decided to exchange information based on agreement or consent (this is why the Add/Remove Feed events)

IANA Issue

- RFC8417 (Security Event Token) defines the "events" claim as a set of URI attributes with a JSON object "payload"

```
"events":{
   "urn:ietf:params:event:SCIM:feed:add": {}
}
```

- While the events claim was defined, no event registry was defined
- Should we:
  - Establish the Event registry (for all uses) for urn:ietf:params:event: …
  - Use the SCIM Schema registry urn:ietf:params:SCIM:event …
    - Likely need to establish a new sub-registry for events
  - Just register specific URIs with IANA (not sure we can do this)

Implementations

- i2scim.io uses a slight variation of events for replication purposes
  - Plan to publish a draft compliant version shortly
  - Plan to support event transfer and consumption via shared signals framework (see below)
- Open Source Projects
  - Cisco DUO Shared Signals demo implements RFC8935/8936 and OpenID Shared Signals Exchange Framework - sharedsignals.guide
  - I2gosignals (to be released) implements shared signals