Security Event Token (SET)

draft-ietf-secevent-token

Phil Hunt
IETF100, Singapore
November 2017
Agenda

- Background
- Current Status
- Draft 03 Updates
- Discussion:
  - Post 03 "Event" Simplification Proposal
Background

- **Security Event Token**
  - In a RESTful context, it is a simple statement of state change
    - Does not typically convey history (why)
    - Is not a command (receiver decides action)
    - Contains an event type and subject information
  - Useful as a signal/trigger between federated entities (across security domains)

- **Timeline**
  - Nov 2015 IETF94 (Tokyo) – Informal agreement to draft proposal
  - Apr 2016 IETF95 (Buenos Aires) – Informal BoF at SCIM WG
    - 3 IDs presented (Token, Distribution, Example SCIM Profile)
  - Nov 2016 IETF97 (Seoul) – First SECEVENT Meeting
SET Examples

- **SCIM (RESTful provisioning)**
  - A trigger to inform clients of independent state changes made by other RESTful clients in a system.

- **OAuth / OIDC (Authorization and Federation)**
  - Ability to revoke tokens and/or sessions

- **RISC (Risk Incident Sharing and Coordination)**
  - Ability to share events based on risk analysis

- **HEART (Health Relationship Trust)**
  - Ability to share consent events

* All areas were proposing using JWTs in similar ways
Draft Status Review

- Completed WGLC
- Current version draft-ietf-secevent-token-03
  - Addresses WGLC feedback from 02
  - Most responses "Good-to-go as is"
- History
  - 4 WG drafts
  - 8 ID drafts (since March 2016)
- Functionally stable
Draft 03 Updates

● Editorial
  ● Corrected old term "subscriber" to "Event Receiver"
  ● WGLC Feedback proposing updates from
    ● Nat Sakimura
    ● Annabelle Backman
    ● Marius Scurtescu
    ● Others – Good to go

● Definitions
  ● Clarified Event Receiver is a JWT recipient
  ● Replaced use of "nbf" with "toe" (time of event)*
DISCUSSION
Post 03 – Annabelle's Event Simplification Proposal

- Proposal to allow only one event
  - https://www.ietf.org/mail-archive/web/id-event/current/msg00710.html
  - Make "events" singular / simple
  - Extensions TBD by Event Profiler

```
A JSON object containing an "event_type" member whose value is a URI representing a type of event defined in a Profiling Specification. The object MAY otherwise be empty, or MAY contain additional members as described by the Profiling Specification.
```
Annabelle's Proposed SET

```
{
  "jti":  "4d3559ec67504aaba65d40b0363faad8",
  "iat":  1458496404,
  "iss":  "https://scim.example.com",
  "aud":  [  
    "https://scim.example.com/Feeds/98d52461fa5bbc879593b7754",
    "https://scim.example.com/Feeds/5d7604516b1d08641d7676ee7"
  ],
  "event":  {  
    "event_type":  "urn:ietf:params:scim:event:create",
    "ref":  "https://scim.example.com/Users/44f6142df96bd6ab61e7521d9",
    "attributes":  ["id", "name", "userName", "password", "emails"]
  }
}
```
Proposal Justification

- 1 Event is simple
  - Event receivers may not be able to make sense of multiple payloads; more information may be confusing
  - Processing multiple payloads could be complex

- Related Comment:
  - JSON attribute name "events" suggests multiple logical events are allowed
    - However, repeat URI's are not allowed (can't repeat a JSON attribute name)
  - Normative language specifies 1 logical event despite name
  - "events" values can convey multiple aspects of same event
03 Draft Reflects Previous Consensus

- Multiple payloads provide multiple benefits
  - Versioning – specs do not version like code
  - Payloads mean namespaces do not need to be registered (collision free)
  - Ad-hoc spec development allowed (via use of URIs payloads)
  - Utility profiles can be defined to simplify profiles
    - E.g. Subject addressing using multiple identifier types
    - Localized transmitter/receiver extensions (non-standard)
  - Concern: Independent profiles may causes event overlaps
    - That's ok: When profiles overlap, both events may be sent to give full picture if receiver understands both event URI types.

- Performance:
  - Signing a single SET for a transaction is less costly
  - Multi-SET would require multi-part new signalling protocol
    - Rcvr: Have I received everything related to this event?
Multi-Event Venn

Event issued based on provisioning

SCIM Password-Reset

Profile A
What if the count of resets matters to the receivers?

Can that be conveyed separately?
Multi-Event Venn

- This RISC event is similar but is not specific to passwords.
- It suggests the event is triggered by risk analysis rather than user-action.
Multi-Event Venn

- Event issued based on provisioning
- Event issued based on risk analysis

Profile A
- SCIM Password-Reset
- SCIM ResetCount 5

Profile B
- RISC Account-Credential-Change-Required

Was it a risk because of high count?

- Received together, the receiver has more information than A or B alone.
Password Reset - Compare

• 3 payloads processed same way
• receiver infers meaning (robust)

Event payload has normative attributes

Event payload has normative attributes

3 payloads processed same way
• receiver infers meaning (robust)
Observations

- A single SET currently conveys the whole picture
  - Each piece adds value
- If receivers may only understand one type
  - They are free to ignore pieces they don't care about
- Forcing single payload may cause
  - More similar event definitions each with specialization
  - No standard extension support if at all
- Outcomes:
  - Profiles would need to be reviewed to avoid overlap OR,
  - Multi-SET signalling to inform receivers a SET has multiple distinct SET messages to form a logical event
Authors' Recommendation

- Do not adopt – change fundamentally different from past consensus
  - Simple single "event" payload increases overall complexity
    - Nested JSON, possible attribute name conflicts
    - Delivery signalling protocol for multiple-SET delivery (txn not enough)
  - Alters/drops foundational features (more than "breaking")
  - May lead to requirement for event registry
  - Would incur substantial re-write
  - Not an issue for receivers that only understand one event uri type
    - Can ignore event URIs that are not understood
    - Transmitters not obliged to include unwanted event data