SET Distribution Draft Discussion

Marius Scurtescu, Google

IETF98 Chicago

March 2017

What is SET Distribution?

Defines how a SET transmitter (aka issuer) delivers events to a receiver using HTTPs.

https://tools.ietf.org/html/draft-hunt-secevent-distribution

Slide Colors

⬜ In Spec

clarification

🟨 In Spec

needs work

🟥 Removed from Spec

🟩 Potentially will be added to spec

Data vs Control Plane

- Data plane for SETs
  - from transmitter to receiver
- Control plane for status, configuration and management
  - from receiver to transmitter

Some events can be seen as commands and vice versa: user enrollment, user opt-out.

For simplicity, the control plane could be merged into bi-directional data plane

- no clear error messages
- receiver may not be able to process commands immediately

Control Plane Operations

- Stream state and current configuration
- Stream management
  - update stream status (force **verify** state for example)
  - create stream
    - One vs multiple streams between same transmitter and receiver
    - receiver specified filter based on event type
- User enrollment

Control Plane Authorization

- control plane is one or more REST endpoints
- the caller must be identified and authorized

Proposal to use OAuth 2 access token:

- Transmitter IdP
    - transmitter identified by issuer
- Receiver RP, has IdP issued client id and secret
    - receiver identified by client id
- No user, client credential grant or similar must be used

Using SCIM for Control Plane

Streams defined as SCIM resources based on RFC 7644.

Pros:

- sophisticated error handling
- mature libraries

Cons:

- complexity
- SET Distribution spec either not self sufficient or very large

Batch Mode

- deliver multiple SETs in one HTTP POST
- complicates error response
- not clear that there is a real need
- each transport method should look at batch mode

Discovery - Transmitter

- Could provide well known based on issuer
- Attributes:
  - issuer
  - supported delivery methods
  - control plane endpoint URL
  - other endpoint URLs, based on delivery methods
  - supported events
  - signature JWK URL

Discovery - Receiver

- no well known base, must document full URL
- attributes
  - client id
  - supported delivery methods
  - data plane endpoint URL
  - other endpoint URLs, based on delivery methods
  - supported event types
  - encryption JWK URL

Uni vs Bi-Directional Streams

- in many cases both parties act as transmitter and receiver
  - for authorization both act mutually as IdP and RP
- for simplicity always look at the uni-directional case

User Opt-Out

- security implications, privacy vs security
  - RISC: attackers should not be able to use opt-out
- for bi-directional connections the user might expect to see opt-out state on both sides
- challenging user experience
  - opt-out of all connections or only specific ones?
  - opt-out of both directions or only one?
  - opt-out delay
  - opt back in

Distribution Methods

- the spec requires only HTTP POST
- other methods
  - polling
  - XMPP
  - Kafka
  - WebSocket
  - proprietary
- registration mechanism

What do you need?