M. Scurtescu
Google
A. Backman
Amazon
P. Hunt
Oracle
J. Bradley
Yubico
February 1, 2018

RISC profile of IETF Security Events
risc-secevent-00

Abstract

This spec is a general profile for IETF Security Events [SECEVENT] and it defines:

- Subject Identifiers
- a configuration information discovery method for Transmitters
- a Management API for Event Streams

This spec also directly profiles several IETF Security Events drafts:

- Security Event Token (SET) [SET]
- SET Token Delivery Using HTTP [DELIVERY]

Table of Contents

1. Introduction

1.1. Notational Conventions

The key words "MUST", "MUST NOT", "REQUIRED", "SHALL", "SHALL NOT", "SHOULD", "SHOULD NOT", "RECOMMENDED", "MAY", and "OPTIONAL" in this document are to be interpreted as described in [RFC2119].

2. Subject Identifiers

The RISC profile defines a structure called a Subject Identifier: a JSON [RFC7159] object containing a set of claims that collectively uniquely identify a subject, according to a simple schema called a Subject Identifier Type. Every Subject Identifier MUST contain a "subject_type" claim, whose value MUST be a name that uniquely identifies the Subject Identifier Type of the Subject Identifier. Any remaining claims within the Subject Identifier MUST be interpreted according to the definition of the Subject Identifier Type. A Subject Identifier MUST conform to the Subject Identifier Type identified by its "subject_type" claim, and MUST NOT contain any claims not defined by its Subject Identifier Type.

```
{
  "subject_type": "email",
  "email": "foo@example.com"
}
```

A Subject Identifier that identifies a subject by email address.

Figure 1: Example: Email Subject Identifier

```
{
  "subject_type": "iss-sub",
  "iss": "https://issuer.example.com/",
  "sub": "abc1234"
}
```

A Subject Identifier that identifies a subject by an identifier provided by an issuer.

Figure 2: Example: Issuer and Subject Subject Identifier

2.1. Subject Identifier Types

A Subject Identifier Type is a light-weight schema that describes a set of claims that uniquely identifies a subject. Every Subject Identifier Type MUST have a unique name registered in the IANA "Security Event Subject Identifier Types" registry established by Section 6.1. A Subject Identifier Type MAY contain more claims than are strictly necessary to uniquely identify a subject, however a

Subject Identifier MUST contain all of the claims required by its type (See Privacy Considerations).

The following Subject Identifier Types are registered in the IANA "Security Event Subject Identifier Types" registry established by Section 6.1.

2.1.1. Email Subject Identifier Type

The Email Subject Identifier Type describes a subject by email address. Subject Identifiers of this type MUST contain an "email" claim whose value is a string containing the email address of the subject. The "email" claim MUST NOT be null or empty. The Email Subject Identifier Type is identified by the name "email".

2.1.2. Phone Number Subject Identifier Type

The Phone Number Subject Identifier Type describes a subject by telephone number. Subject Identifiers of this type MUST contain a "phone" claim whose value is a string containing the full telephone number of the subject, including international dialing prefix, formatted according to E.164 [E164]. The "phone" claim MUST NOT be null or empty. The Phone Number Subject Identifier Type is identified by the name "phone".

2.1.3. Issuer and Subject Subject Identifier Type

The Issuer and Subject Subject Identifier Type describes a subject by an issuer and a subject. Subject Identifiers of this type MUST contain an "iss" claim whose value identifies the issuer, and a "sub" claim whose value identifies the subject with respect to the issuer. These claims MUST follow the formats of the "iss" claim and "sub" claim defined by [RFC7519], respectively. Both the "iss" claim and the "sub" claim MUST NOT be null or empty. The Issuer and Subject Subject Identifier Type is identified by the name "iss-sub".

2.1.4. ID Token Claims Subject Identifier Type

The ID Token Claims Subject Identifier Type describes a subject by a subset of the claims from an ID token. Subject Identifiers of this type MUST contain at least one of the following claims:

email
: An "email" claim, as defined in [IDTOKEN].

phone_number
: An "phone_number" claim, as defined in [IDTOKEN].

sub
A "sub" claim, as defined in [RFC7519].

If the Subject Identifier contains a "sub" claim, it MUST also contain an "iss" claim, as defined in [RFC7519]. The ID Token Claims Subject Identifier Type is identified by the name "id-token-claims".

3. Transmitter Configuration Discovery

This section defines a mechanism for Receivers to obtain Transmitter configuration information.

3.1. Transmitter Configuration Metadata

Transmitters have metadata describing their configuration:

issuer REQUIRED. URL using the https scheme with no query or fragment component that the Transmitter asserts as its Issuer Identifier. This MUST be identical to the iss Claim value in Security Event Tokens issued from this Transmitter.

jwks_uri REQUIRED. URL of the Transmitter's JSON Web Key Set [RFC7517] document. This contains the signing key(s) the Receiver uses to validate signatures from the Transmitter.

delivery_methods_supported RECOMMENDED. List of supported delivery method URIs.

configuration_endpoint OPTIONAL. The URL of the Configuration Endpoint.

status_endpoint OPTIONAL. The URL of the Status Endpoint.

add_subject_endpoint OPTIONAL. The URL of the Add Subject Endpoint.

remove_subject_endpoint OPTIONAL. The URL of the Remove Subject Endpoint.

verification_endpoint OPTIONAL. The URL of the Verification Endpoint.

3.2. Obtaining Transmitter Configuration Information

Using the Issuer as documented by the Transmitter, the Transmitter Configuration Information can be retrieved.

Transmitters supporting Discovery MUST make a JSON document available at the path formed by concatenating the string "/.well-known/risc-

configuration" to the Issuer. The syntax and semantics of ".well-known" are defined in [RFC5785] and apply to the Issuer value when it contains no path component. "risc-configuration" MUST point to a JSON document compliant with this specification and MUST be returned using the "application/json" content type.

3.2.1. Transmitter Configuration Request

A Transmitter Configuration Document MUST be queried using an HTTP "GET" request at the previously specified path.

The Receiver would make the following request to the Issuer "https://tr.example.com" to obtain its Configuration information, since the Issuer contains no path component:

```
GET /.well-known/risc-configuration HTTP/1.1
Host: tr.example.com
```

Figure 3: Example: Transmitter Configuration Request (without path)

If the Issuer value contains a path component, any terminating "/" MUST be removed before appending "/.well-known/risc-configuration". The Receiver would make the following request to the Issuer "https://tr.example.com/issuer1" to obtain its Configuration information, since the Issuer contains a path component:

```
GET /issuer1/.well-known/risc-configuration HTTP/1.1
Host: tr.example.com
```

Figure 4: Example: Transmitter Configuration Request (with path)

Using path components enables supporting multiple issuers per host. This is required in some multi-tenant hosting configurations. This use of ".well-known" is for supporting multiple issuers per host; unlike its use in [RFC5785], it does not provide general information about the host.

3.2.2. Transmitter Configuration Response

The response is a set of Claims about the Transmitter’s configuration, including all necessary endpoints and public key location information. A successful response MUST use the 200 OK HTTP status code and return a JSON object using the "application/json" content type that contains a set of Claims as its members that are a subset of the Metadata values defined in Section 3.1. Other Claims MAY also be returned.

Claims that return multiple values are represented as JSON arrays. Claims with zero elements MUST be omitted from the response.

An error response uses the applicable HTTP status code value.

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

{
  "issuer":
    "https://tr.example.com",
  "jwks_uri":
    "https://tr.example.com/jwks.json",
  "delivery_methods_supported": [
    "http://schemas.openid.net/secevent/risc/delivery-method/push",
    "http://schemas.openid.net/secevent/risc/delivery-method/poll"],
  "configuration_endpoint":
    "https://tr.example.com/risc/mgmt/stream",
  "status_endpoint":
    "https://tr.example.com/risc/mgmt/status",
  "add_subject_endpoint":
    "https://tr.example.com/risc/mgmt/subject:add",
  "remove_subject_endpoint":
    "https://tr.example.com/risc/mgmt/subject:remove",
  "verification_endpoint":
    "https://tr.example.com/risc/mgmt/verification",
}
```

Figure 5: Example: Transmitter Configuration Response

3.2.3. Transmitter Configuration Validation

If any of the validation procedures defined in this specification fail, any operations requiring the information that failed to correctly validate MUST be aborted and the information that failed to validate MUST NOT be used.

The "issuer" value returned MUST be identical to the Issuer URL that was directly used to retrieve the configuration information. This MUST also be identical to the "iss" Claim value in Security Event Tokens issued from this Transmitter.

4. Management API for SET Event Streams

This section defines an HTTP API to be implemented by Event Transmitters and that can be used by Event Receivers to query the Event Stream status, to add and remove subjects and to trigger verification.

This section is based on Management API for SET Event Streams [MGMTAPI].

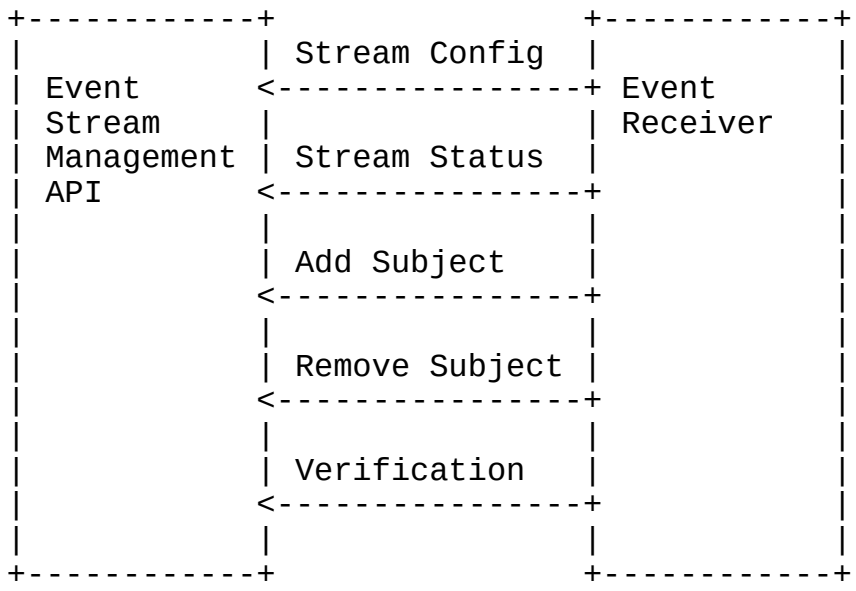

Figure 6: Event Stream Management API

4.1. Event Stream Management

Event Receivers manage how they receive events, and the subjects about which they want to receive events over an Event Stream by making HTTP requests to endpoints in the Event Stream Management API.

The Event Stream Management API is implemented by the Event Transmitter and consists of the following endpoints:

Configuration Endpoint
: An endpoint used to read the Event Stream’s current configuration.

Status Endpoint
: An endpoint used to read the Event Stream’s current status.

Add Subject Endpoint
: An endpoint used to add subjects to an Event Stream.

Remove Subject Endpoint
: An endpoint used to remove subjects from an Event Stream.

Verification Endpoint
: An endpoint used to request the Event Transmitter transmit a Verification Event over the Event Stream.

An Event Transmitter MAY use the same URLs as endpoints for multiple streams, provided that the Event Transmitter has some mechanism through which they can identify the applicable Event Stream for any given request, e.g. from authentication credentials. The definition of such mechanisms is outside the scope of this specification.

4.1.1. Stream Status

4.1.1.1. Reading a Stream's Status

An Event Receiver checks the current status of an event stream by making an HTTP GET request to the stream's Status Endpoint. On receiving a valid request the Event Transmitter responds with a 200 OK response containing a JSON [RFC7159] object with a single attribute "status", whose string value MUST have one of the following values:

enabled
: The transmitter will transmit events over the stream, according to the stream's configured delivery method.

paused
: The transmitter will not transmit events over the stream. The transmitter will hold any events it would have transmitted while paused, and will transmit them when the stream's status becomes "enabled".

disabled
: The transmitter will not transmit events over the stream, and will not hold any events for later transmission.

The following is a non-normative example request to check an event stream's status:

```
GET /set/status HTTP/1.1
Host: transmitter.example.com
Authorization: Bearer eyJ0b2tlbiI6ImV4YW1wbGUifQo=
```

Figure 7: Example: Check Stream Status Request

The following is a non-normative example response:

```
HTTP/1.1 200 OK
Content-Type: application/json; charset=UTF-8
Cache-Control: no-store
Pragma: no-cache

{
  "status": "enabled"
}
```

Figure 8: Example: Check Stream Status Response

4.1.1.2. Updating a Stream’s Status

An Event Receiver updates the current status of a stream by making an HTTP POST request to the Status Endpoint. The POST body contains a JSON [RFC7159] representation of the updated status. On receiving a valid request the Event Transmitter responds with a "200 OK" response containing a JSON [RFC7159] representation of the updated stream status in the body.

The following is a non-normative example request to update an Event Stream’s status:

```
POST /set/status HTTP/1.1
Host: transmitter.example.com
Authorization: Bearer eyJ0b2tlbiI6ImV4YW1wbGUifQo=

{
  "status": "paused",
}
```

Figure 9: Example: Update Stream Status Request

The following is a non-normative example response:

```
HTTP/1.1 200 OK
Content-Type: application/json; charset=UTF-8
Cache-Control: no-store
Pragma: no-cache

{
  "status": "paused",
}
```

Figure 10: Example: Update Stream Status Response

Errors are signaled with HTTP staus codes as follows:

Code	Description
400	if the request body cannot be parsed or if the request is otherwise invalid
401	if authorization failed or it is missing
403	if the Event Receiver is not allowed to update the stream status

Table 1: Update Stream Configuration Errors

4.1.2. Stream Configuration

An Event Stream's configuration is represented as a JSON [RFC7159] object with the following properties:

aud
: A string containing an audience claim as defined in JSON Web Token (JWT) [RFC7519] that identifies the Event Receiver for the Event Stream. This property cannot be updated.

events_supported
: OPTIONAL. An array of URIs identifying the set of events supported by the Transmitter for this Receiver. If omitted, Event Transmitters SHOULD make this set available to the Event Receiver via some other means (e.g. publishing it in online documentation).

events_requested
: OPTIONAL. An array of URIs identifying the set of events that the Receiver requested. A Receiver should request only the events that it understands and it can act on. This is configurabel by the Receuver.

events_delivered
: OPTIONAL. An array of URIs which is the intersection of "events_supported" and "events_requested". These evebts MAY be delivered over the Event Stream.

delivery
: A JSON object containing a set of name/value pairs specifying configuration parameters for the SET delivery method. The actual delivery method is identified by the special key "method" with the value being a URI as defined in Section 5.2.1.

min_verification_interval

An integer indicating the minimum amount of time in seconds that must pass in between verification requests. If an Event Receiver submits verification requests more frequently than this, the Event Transmitter MAY respond with a 429 status code. An Event Transmitter SHOULD NOT respond with a 429 status code if an Event Receiver is not exceeding this frequency.

subject_type The Subject Identifier Type that the Receiver wants for the events. If not set then the Transmitter might decide to use a type that discloses more information than necessary.

4.1.2.1. Reading a Stream's Configuration

An Event Receiver gets the current configuration of a stream by making an HTTP GET request to the Configuration Endpoint. On receiving a valid request the Event Transmitter responds with a "200 OK" response containing a JSON [RFC7159] representation of the stream's configuration in the body.

The following is a non-normative example request to read an Event Stream's configuration:

```
GET /set/stream HTTP/1.1
Host: transmitter.example.com
Authorization: Bearer eyJ0b2tlbiI6ImV4YW1wbGUifQo=
```

Figure 11: Example: Read Stream Configuration Request

The following is a non-normative example response:

```
HTTP/1.1 200 OK
Content-Type: application/json; charset=UTF-8
Cache-Control: no-store
Pragma: no-cache

{
  "aud": "http://www.example.com",
  "delivery": {
    "delivery_method":
      "http://schemas.openid.net/secevent/risc/delivery-method/push",
    "url": "https://receiver.example.com/events",
  },
  "events_supported": [
    "urn:example:secevent:events:type_1",
    "urn:example:secevent:events:type_2",
    "urn:example:secevent:events:type_3",
  ],
  "events_requested": [
    "urn:example:secevent:events:type_2",
    "urn:example:secevent:events:type_3",
    "urn:example:secevent:events:type_4",
  ],
  "events_delivered": [
    "urn:example:secevent:events:type_2",
    "urn:example:secevent:events:type_3",
  ],
  "min_verification_interval": 60,
}
```

Figure 12: Example: Read Stream Configuration Response

Errors are signaled with HTTP staus codes as follows:

Code	Description
401	if authorization failed or it is missing
403	if the Event Receiver is not allowed to read the stream configuration
404	if there is no Event Stream configured for this Event Receiver

Table 2: Read Stream Configuration Errors

4.1.2.2. Updating a Stream’s Configuration

An Event Receiver updates the current configuration of a stream by making an HTTP POST request to the Configuration Endpoint. The POST body contains a JSON [RFC7159] representation of the updated configuration. On receiving a valid request the Event Transmitter responds with a "200 OK" response containing a JSON [RFC7159] representation of the updated stream configuration in the body.

The full set of editable properties must be present in the POST body, not only the ones that are specifically intended to be changed. Missing properties SHOULD be interpreted as requested to be deleted. Event Receivers should read the configuration first, modify the JSON [RFC7159] representation, then make an update request.

Properties that cannot be updated MAY be present, but they MUST match the expected value.

The following is a non-normative example request to update an Event Stream’s configuration:

```
POST /set/stream HTTP/1.1
Host: transmitter.example.com
Authorization: Bearer eyJ0b2tlbiI6ImV4YW1wbGUifQo=

{
  "aud": "http://www.example.com",
  "delivery": {
    "delivery_method":
      "http://schemas.openid.net/secevent/risc/delivery-method/push",
    "url": "https://receiver.example.com/events",
  },
  "events_requested": [
    "urn:example:secevent:events:type_2",
    "urn:example:secevent:events:type_3",
    "urn:example:secevent:events:type_4",
  ],
}
```

Figure 13: Example: Update Stream Configuration Request

The following is a non-normative example response:

```
HTTP/1.1 200 OK
Content-Type: application/json; charset=UTF-8
Cache-Control: no-store
Pragma: no-cache

{
  "aud": "http://www.example.com",
  "delivery": {
    "delivery_method":
      "http://schemas.openid.net/secevent/risc/delivery-method/push",
    "url": "https://receiver.example.com/events",
  },
  "events_supported": [
    "urn:example:secevent:events:type_1",
    "urn:example:secevent:events:type_2",
    "urn:example:secevent:events:type_3",
  ],
  "events_requested": [
    "urn:example:secevent:events:type_2",
    "urn:example:secevent:events:type_3",
    "urn:example:secevent:events:type_4",
  ],
  "events_delivered": [
    "urn:example:secevent:events:type_2",
    "urn:example:secevent:events:type_3",
  ],
}
```

Figure 14: Example: Update Stream Configuration Response

Errors are signaled with HTTP staus codes as follows:

Code	Description
400	if the request body cannot be parsed or if the request is otherwise invalid
401	if authorization failed or it is missing
403	if the Event Receiver is not allowed to update the stream configuration

Table 3: Update Stream Configuration Errors

4.1.3. Subjects

An Event Receiver can indicate to an Event Transmitter whether or not the receiver wants to receive events about a particular subject by "adding" or "removing" that subject to the Event Stream, respectively.

4.1.3.1. Adding a Subject to a Stream

To add a subject to an Event Stream, the Event Receiver makes an HTTP POST request to the Add Subject Endpoint, containing in the body a JSON object the following claims:

subject
: A Subject Identifier identifying the subject to be added. REQUIRED.

On a successful response, the Event Transmitter responds with an empty "200 OK" response. The Event Transmitter MAY choose to silently ignore the request, for example if the subject has previously indicated to the transmitter that they do not want events to be transmitted to the Event Receiver. In this case, the transmitter MAY return an empty "200 OK" response or an appropriate error code. See Security Considerations (Section 4.3).

Errors are signaled with HTTP status codes as follows:

Code	Description
400	if the request body cannot be parsed or if the request is otherwise invalid
401	if authorization failed or it is missing
403	if the Event Receiver is not allowed to add this particular subject
404	if the subject is not recognized by the Event Transmitter, the Event Transmitter may chose to stay silent in this case and respond with "200"
429	if the Event Receiver is sending too many requests in a gvien amount of time

Table 4: Add Subject Errors

The following is a non-normative example request to add a subject to a stream, where the subject is identified by an Email Subject Identifier.

```
POST /set/subjects:add HTTP/1.1
Host: transmitter.example.com
Authorization: Bearer eyJ0b2tlbiI6ImV4YW1wbGUifQo=

{
  "subject": {
    "subject_type": "email",
    "email": "example.user@example.com"
  }
}
```

Figure 15: Example: Add Subject Request

The following is a non-normative example response to a successful request:

```
HTTP/1.1 200 OK
Server: transmitter.example.com
Cache-Control: no-store
Pragma: no-cache
```

Figure 16: Example: Add Subject Response

4.1.3.2. Removing a Subject

To remove a subject from an Event Stream, the Event Receiver makes an HTTP POST request to the Remove Subject Endpoint, containing in the body a JSON object with the following claims:

subject
: A Subject Identifier identifying the subject to be removed. REQUIRED.

On a successful response, the Event Transmitter responds with a "204 No Content" response.

Errors are signaled with HTTP staus codes as follows:

Code	Description
400	if the request body cannot be parsed or if the request is otherwise invalid
401	if authorization failed or it is missing
403	if the Event Receiver is not allowed to remove this particular subject
404	if the subject is not recognized by the Event Transmitter, the Event Transmitter may chose to stay silent in this case and respond with "204"
429	if the Event Receiver is sending too many requests in a gvien amount of time

Table 5: Remove Subject Errors

The following is a non-normative example request where the subject is identified by a Phone Number Subject Identifier:

```
POST /set/subjects:remove HTTP/1.1
Host: transmitter.example.com
Authorization: Bearer eyJ0b2tlbiI6ImV4YW1wbGUifQo=

{
  "subject": {
    "subject_type": "phone",
    "phone_number": "+1 206 555 0123"
  }
}
```

Figure 17: Example: Remove Subject Request

The following is a non-normative example response to a successful request:

```
HTTP/1.1 204 No Content
Server: transmitter.example.com
Cache-Control: no-store
Pragma: no-cache
```

Figure 18: Example: Remove Subject Response

4.1.4. Verification

In some cases, the frequency of event transmission on an Event Stream will be very low, making it difficult for an Event Receiver to tell the difference between expected behavior and event transmission failure due to a misconfigured stream. Event Receivers can request that a verification event be transmitted over the Event Stream, allowing the receiver to confirm that the stream is configured correctly upon successful receipt of the event. The acknowledgment of a Verification Event also confirms to the Event Transmitter that end-to-end delivery is working, including signature verification and encryption.

An Event Transmitter MAY send a Verification Event at any time, even if one was not requested by the Event Receiver.

4.1.4.1. Verification Event

The Verification Event is a standard SET with the following attributes:

event type
: The Event Type URI is: "http://schemas.openid.net/secevent/risc/event-type/verification".

state
: OPTIONAL An opaque value provided by the Event Receiver when the event is triggered. This is a nested attribute in the event payload.

Upon receiving a Verification Event, the Event Receiver SHALL parse the SET and validate its claims. In particular, the Event Receiver SHALL confirm that the value for "state" is as expected. If the value of "state" does not match, an error response of "setData" SHOULD be returned (see Section 2.4 of [DELIVERY]).

In many cases, Event Transmitters MAY disable or suspend an Event Stream that fails to successfully verify based on the acknowledgement or lack of acknowledgement by the Event Receiver.

4.1.4.2. Triggering a Verification Event.

To request that a verification event be sent over an Event Stream, the Event Receiver makes an HTTP POST request to the Verification Endpoint, with a JSON [RFC7159] object containing the parameters of the verification request, if any. On a successful request, the event transmitter responds with an empty "204 No Content" response.

Verification requests have the following properties:

state
: OPTIONAL. An arbitrary string that the Event Transmitter MUST echo back to the Event Receiver in the verification event's payload. Event Receivers MAY use the value of this parameter to correlate a verification event with a verification request. If the verification event is initiated by the transmitter then this parameter MUST not be set.

A successful response from a POST to the Verification Endpoint does not indicate that the verification event was transmitted successfully, only that the Event Transmitter has transmitted the event or will do so at some point in the future. Event Transmitters MAY transmit the event via an asynchronous process, and SHOULD publish an SLA for verification event transmission times. Event Receivers MUST NOT depend on the verification event being transmitted synchronously or in any particular order relative to the current queue of events.

Errors are signaled with HTTP staus codes as follows:

Code	Description
400	if the request body cannot be parsed or if the request is otherwise invalid
401	if authorization failed or it is missing
429	if the Event Receiver is sending too many requests in a gvien amount of time; see related "min_verification_interval" in Section 4.1.2

Table 6: Verification Errors

The following is a non-normative example request to trigger a verification event:

```
POST /set/verify HTTP/1.1
Host: transmitter.example.com
Authorization: Bearer eyJ0b2tlbiI6ImV4YW1wbGUifQo=
Content-Type: application/json; charset=UTF-8

{
  "state": "VGhpcyBpcyBhbiBleGFtcGxlIHN0YXRlIHZhbHVlLgo="
}
```

Figure 19: Example: Trigger Verification Request

The following is a non-normative example response to a successful request:

```
HTTP/1.1 204 No Content
Server: transmitter.example.com
Cache-Control: no-store
Pragma: no-cache
```

Figure 20: Example: Trigger Verification Response

And the following is a non-normative example of a verification event sent to the Event Receiver as a result of the above request:

```
{
  "jti": "123456",
  "iss": "https://transmitter.example.com",
  "aud": "receiver.example.com",
  "iat": "1493856000",
  "events": [
    "http://schemas.openid.net/secevent/risc/event-type/verification":{
      "state": "VGhpcyBpcyBhbiBleGFtcGxlIHN0YXRlIHZhbHVlLgo=",
    },
  ],
}
```

Figure 21: Example: Verification SET

4.2. Authorization

HTTP API calls from a receiver to a transmitter SHOULD be authorized using OAuth 2 Access Tokens. The client id associated with the Access Token uniquely identifies the Receiver and the Stream.

Receivers SHOULD use the Client Credential Grant [CLIENTCRED] to obtain access tokens on its own behalf.

4.3. Security Considerations

4.3.1. Subject Probing

It may be possible for an Event Transmitter to leak information about subjects through their responses to add subject requests. A "404" response may indicate to the Event Receiver that the subject does not exist, which may inadvertantly reveal information about the subject (e.g. that a particular individual does or does not use the Event Transmitter’s service).

Event Transmitters SHOULD carefully evaluate the conditions under which they will return error responses to add subject requests. Event Transmitters MAY return a "204" response even if they will not actually send any events related to the subject, and Event Receivers MUST NOT assume that a 204 response means that they will receive events related to the subject.

4.3.2. Information Harvesting

SETs may contain personally identifiable information (PII) or other non-public information about the event transmitter, the subject (of an event in the SET), or the relationship between the two. It is important for Event Transmitters to understand what information they are revealing to Event Receivers when transmitting events to them, lest the event stream become a vector for unauthorized access to private information.

Event Transmitters SHOULD interpret add subject requests as statements of interest in a subject by an Event Receiver, and ARE NOT obligated to transmit events related to every subject an Event Receiver adds to the stream. Event Transmitters MAY choose to transmit some, all, or no events related to any given subject and SHOULD validate that they are permitted to share the information contained within an event with the Event Receiver before transmitting the event. The mechanisms by which such validation is performed are outside the scope of this specification.

4.3.3. Malicious Subject Removal

A malicious party may find it advantageous to remove a particular subject from a stream, in order to reduce the Event Receiver’s ability to detect malicious activity related to the subject, inconvenience the subject, or for other reasons. Consequently it may be in the best interests of the subject for the Event Transmitter to continue to send events related to the subject for some time after the subject has been removed from a stream.

Event Transmitters MAY continue sending events related to a subject for some amount of time after that subject has been removed from the stream. Event Receivers MUST tolerate receiving events for subjects that have been removed from the stream, and MUST NOT report these events as errors to the Event Transmitter.

5. Profiles

This section profiles several IETF secevent specifications.

The RISC Profile makes several assumptions:

- Transmitters are Oauth 2 Authorization Servers
- Receivers are OAuth 2 Clients and as such have client ids issued by Transmitters

The RISC use cases that set the requirements are described in Security Events RISC Use Cases [USECASES].

5.1. Security Event Token Profle

This section provides RISC profiling specifications for the "Security Event Token (SET)" [SET] spec.

5.1.1. Signature Key Resolution

The signature key can be obtained through "jwks_uri", see Section 3.

5.1.2. RISC Event Subject

The subject of a RISC event is identified by the "subject" claim within the event payload, whose value is a Subject Identifier. The "subject" claim is REQUIRED for all RISC events. The JWT "sub" claim MUST NOT be present in any SET containing a RISC event.

5.1.3. Explicit Typing of SETs

RISC events MUST use explicit typing as defined in Section 2.3 of [SET].

```
{
  "typ":"secevent+jwt",
  "alg":"HS256"
}
```

Figure 22: Explicitly Typed JOSE Header

The purpose is defense against confusion with other JWTs, as described in Sections 4.5, 4.6 and 4.7 of [SET]. While current Id Token [IDTOKEN] validators may not be using the "typ" header parameter, by requiring it for RISC SETs a distinct value is guaranteed for future validators.

5.1.4. The "exp" Claim

The "exp" claim MUST NOT be used in RISC SETs.

The purpose is defense in depth against confusion with other JWTs, as described in Sections 4.5 and 4.6 of [SET].

5.1.5. aud Claim

The ’aud’ claim MUST be a single value which is the client id of the Receiver.

5.1.6. Security Considerations

5.1.6.1. Distingushing SETs from other Kinds of JWTs

Of particular concern is the possibility that SETs are confused for other kinds of JWTs. The Security Considerations sesction of [SET] has several sub-sections on this subject. The RISC Profile is asking for further restrioctons:

- The "sub" claim MUST NOT be present, as described in Section 5.1.2.
- RISC SETs MUST use explicit typing, as described in Section 5.1.3.
- The "exp" claim MUST NOT be present, as described in Section 5.1.4.

5.2. SET Token Delivery Using HTTP Profile

This section provides RISC profiling specifications for the "SET Token Delivery Using HTTP" [DELIVERY] spec.

5.2.1. Stream Configuration Metadata

Each delivery method is identified by a URI, specified below by the "method" metadata.

5.2.1.1. Push Delivery using HTTP

method "http://schemas.openid.net/secevent/risc/delivery-method/push"

endpoint_url The URL where events are pushed through HTTP POST. This is set by the Receiver.

authorization_header The HTTP Authorization header that the Transmitter MUST set with each event delivery, if the configuration is present. The value is optional and it is set by the Receiver.

5.2.1.2. Polling Delivery using HTTP

method "http://schemas.openid.net/secevent/risc/delivery-method/poll"

endpoint_url The URL where events can be retrieved from. This is specified by the Transmitter.

6. IANA Considerations

6.1. Security Event Subject Identifier Types Registry

This document defines Subject Identifier Types, for which IANA is asked to create and maintain a new registry titled "Security Event Subject Identifier Types". Initial values for the Security Event Subject Identifier Types registry are given in Section 6.1.2. Future assignments are to be made through the Expert Review registration policy [BCP26] and shall follow the template presented in Section 6.1.1.

6.1.1. Registration Template

Type Name:
The name of the Subject Identifier Type, as described in Section 2.1. The name MUST be an ASCII string consisting only of lower-case characters ("a" - "z"), digits ("0" - "9"), and hyphens ("-"), and SHOULD NOT exceed 20 characters in length.

Type Description:
A brief description of the Subject Identifier Type.

Change Controller:
For types defined in documents published by the OpenID Foundation or its working groups, list "OIDF RISC Working Group". For all other types, list the name of the party responsible for the

registration. Contact information such as mailing address, email address, or phone number may also be provided.

Defining Document(s):
A reference to the document or documents that define the Subject Identifier Type. The definition MUST specify the name, format, and meaning of each claim that may occur within a Subject Identifier of the defined type, as well as whether each claim is optional or required, or the circumstances under which the claim is optional or required. URIs that can be used to retrieve copies of each document SHOULD be included.

6.1.2. Initial Registry Contents

- Type Name: "email"
- Type Description: Subject identifier based on email address.
- Change Controller: OIDF RISC Working Group
- Defining Document(s): Section 2.1.1 of this document.

- Type Name: "id-token-claims"
- Type Description: Subject identifier based on OpenID Connect ID Token claims.
- Change Controller: OIDF RISC Working Group
- Defining Document(s): Section 2.1.4 of this document.

- Type Name: "iss-sub"
- Type Description: Subject identifier based on issuer and subject.
- Change Controller: OIDF RISC Working Group
- Defining Document(s): Section 2.1.3 of this document.

- Type Name: "phone"
- Type Description: Subject identifier based on phone number.
- Change Controller: OIDF RISC Working Group
- Defining Document(s): Section 2.1.2 of this document.

6.2. Guidance for Expert Reviewers

The Expert Reviewer is expected to review the documentation referenced in a registration request to verify its completeness. The Expert Reviewer must base their decision to accept or reject the request on a fair and impartial assessment of the request. If the Expert Reviewer has a conflict of interest, such as being an author of a defining document referenced by the request, they must recuse themselves from the approval process for that request. In the case where a request is rejected, the Expert Reviewer should provide the requesting party with a written statement expressing the reason for rejection, and be prepared to cite any sources of information that went into that decision.

Subject Identifier Types need not be generally applicable and may be highly specific to a particular domain; it is expected that types may be registered for niche or industry-specific use cases. The Expert Reviewer should focus on whether the type is thoroughly documented, and whether its registration will promote or harm interoperability. In most cases, the Expert Reviewer should not approve a request if the registration would contribute to confusion, or amount to a synonym for an existing type.

7. Privacy Considerations

7.1. Subject Information Leakage

Event issuers and recipients SHOULD take precautions to ensure that they do not leak information about subjects via Subject Identifiers, and choose appropriate Subject Identifier Types accordingly. Parties SHOULD NOT identify a subject using a given Subject Identifier Type if doing so will allow the recipient to correlate different claims about the subject that they are not known to already have knowledge of. Issuers and recipients SHOULD always use the same Subject Identifier Type and the same claim values to identify a given subject when communicating with a given party in order to reduce the possibility of information leakage.

8. Normative References

[BCP26] Cotton, M., Leiba, B., and T. Narten, "Guidelines for Writing an IANA Considerations Section in RFCs", BCP 26, RFC 8126, DOI 10.17487/RFC8126, June 2017, <https://tools.ietf.org/html/rfc8126>.

[CLIENTCRED] Hardt, D., "The OAuth 2.0 Authorization Framework - Client Credentials Grant", RFC 6749, <https://tools.ietf.org/html/rfc6749#section-4.4>.

[DELIVERY] IETF, "SET Token Delivery Using HTTP", <https://tools.ietf.org/html/draft-ietf-secevent-delivery>.

[E164] International Telecommunication Union, "The international public telecommunication numbering plan", 2010, <http://www.itu.int/rec/T-REC-E.164-201011-I/en>.

[IDTOKEN] OpenID Foundation, "OpenID Connect Core 1.0 - ID Token", <http://openid.net/specs/openid-connect-core-1_0.html#IDToken>.

[MGMTAPI] IETF, "Management API for SET Event Streams", <https://tools.ietf.org/html/draft-scurtescu-secevent-simple-control-plane>.

[OIDC-DISCOVERY] Sakimura, N., Bradley, J., Jones, M., and E. Jay, "OpenID Connect Discovery 1.0", November 2014, <https://openid.net/specs/openid-connect-discovery-1_0.html>.

[RFC2119] Bradner, S., "Key words for use in RFCs to Indicate Requirement Levels", BCP 14, RFC 2119, DOI 10.17487/RFC2119, March 1997, <https://www.rfc-editor.org/info/rfc2119>.

[RFC5785] Nottingham, M. and E. Hammer-Lahav, "Defining Well-Known Uniform Resource Identifiers (URIs)", RFC 5785, DOI 10.17487/RFC5785, April 2010, <https://www.rfc-editor.org/info/rfc5785>.

[RFC7159] Bray, T., Ed., "The JavaScript Object Notation (JSON) Data Interchange Format", RFC 7159, DOI 10.17487/RFC7159, March 2014, <https://www.rfc-editor.org/info/rfc7159>.

[RFC7517] Jones, M., "JSON Web Key (JWK)", RFC 7517, DOI 10.17487/RFC7517, May 2015, <https://www.rfc-editor.org/info/rfc7517>.

[RFC7519] Jones, M., Bradley, J., and N. Sakimura, "JSON Web Token (JWT)", RFC 7519, DOI 10.17487/RFC7519, May 2015, <https://www.rfc-editor.org/info/rfc7519>.

[SECEVENT] IETF, "Security Events IETF Working Group", <https://datatracker.ietf.org/wg/secevent/about/>.

[SET] IETF, "Security Event Token (SET)", <https://tools.ietf.org/html/draft-ietf-secevent-token>.

[USECASES] IETF, "Security Events RISC Use Cases", <https://tools.ietf.org/html/draft-scurtescu-secevent-risc-use-cases-00>.

Appendix A. Acknowledgements

Transmitter Configuration Discovery (Section 3) is based on OpenID Connect Discovery 1.0 [OIDC-DISCOVERY].

Authors' Addresses

Marius Scurtescu
Google

Email: mscurtescu@google.com

Annabelle Backman
Amazon

Email: richanna@amazon.com

Phil Hunt
Oracle Corporation

Email: phil.hunt@yahoo.com

John Bradley
Yubico

Email: secevemt@ve7jtb.com