Workgroup: SCIM
Internet-Draft: draft-hunt-scim-events
Obsoletes: draft-hunt-idevent-scim-00
(if approved)
Published: 3 March 2022
Intended Status: Standards Track
Expires: 4 September 2022
Authors: P. Hunt, Ed.
IndependentId Inc

SCIM Profile for Security Event Tokens

Abstract

This specification profiles the Security Event Token specification, to define a set of events for SCIM Protocol servers that can be used for asynchronous transaction confirmations, replication, cross-domain provisioning co-ordination, and security signals.

Status of This Memo

This Internet-Draft is submitted in full conformance with the provisions of BCP 78 and BCP 79.

Internet-Drafts are working documents of the Internet Engineering Task Force (IETF). Note that other groups may also distribute working documents as Internet-Drafts. The list of current Internet-Drafts is at https://datatracker.ietf.org/drafts/current/.

Internet-Drafts are draft documents valid for a maximum of six months and may be updated, replaced, or obsoleted by other documents at any time. It is inappropriate to use Internet-Drafts as reference material or to cite them other than as "work in progress."

This Internet-Draft will expire on 4 September 2022.

Table of Contents

1. Introduction and Overview

This specification profiles Security Event Tokens (SET) [RFC8417] to define Security Events and mechanisms for delivery with SCIM

Protocol [RFC7644] systems that can be used for asynchronous transaction confirmations, replication, cross-domain provisioning co-ordination, and security signals.

1.1. Requirements Language

The key words "MUST", "MUST NOT", "REQUIRED", "SHALL", "SHALL NOT", "SHOULD", "SHOULD NOT", "RECOMMENDED", "NOT RECOMMENDED", "MAY", and "OPTIONAL" in this document are to be interpreted as described in BCP 14 [RFC2119] [RFC8174] when, and only when, they appear in all capitals, as shown here.

1.2. Notational Conventions

For purposes of readability examples are not URL encoded. Implementers MUST percent encode URLs as described in Section 2.1 of [RFC3986].

Throughout this documents all figures MAY contain spaces and extra line-wrapping for readability and space limitations. Similarly, some URI's contained within examples, have been shortened for space and readability reasons.

1.3. Definitions

This specification uses definitions from the following specifications:

- Security Event Tokens [RFC8417], and
- System for Cross-Domain Identity Management Protocol [RFC7644].

Additionally, the following terms are defined:

Attributes and Claims
: The JWT specification [RFC7519] upon which SET is based uses the term "claims" to refer to attributes in a JSON token. SCIM in contrast uses the term "attributes" to refer to JSON attributes.

For the purposes of this draft, the terms "attributes" and "claims" are equivalent.

CP

Abbreviation for "Co-ordinated Provisioning" as defined in Section 2.2.

DBR

Abbreviation for "Domain Based Replication" as defined in Section 2.1.

Event Feed

This describes the notion that a feed MAY be individualized per client. A service provider MAY offer to allow Event Receiver's to "subscribe" to specific event types or events about specific resources. If no option is offered, it is assumed the client will receive all events about all resources.

Event Receiver

A system that receives events for the purpose of subsequent action (e.g. such as replication), co-ordination of workflow, or signalling.

Event Publisher

A system that issues SETs based on a change that has occurred at a SCIM Service Provider. For example, events MAY originate from a SCIM Create, Modify, or Delete per [RFC7644] request. A SCIM Service Provider MAY be an Event Publisher or an independent service that aggregates events into Event Receiver feeds.

Message Bus

Any communications protocol or system that enables a message (e.g. a SET) to be sent to one or more receivers at the same time. Typically participants connect to a "bus" rather than in point-to-point transfer such as SET HTTP Push [RFC8935]. The "bus" takes care of fault-tolerance, routing, and delivery to recipients.

RS

Abbreviation for "Risk Signals" as defined in Section 2.3.

SCIM Service Provider

An HTTP server that implements SCIM Protocol [RFC7644] and SCIM Schema [RFC7643].

SET

Abbreviation for "Security Event Token" as defined in [RFC8417]

2. Processing Modes for Events

This specification defines 4 processing modes for SCIM Security Events that have different objectives, data requirements, and considerations for using Security Event Tokens.

2.1. Domain Based Replication

The objective of DBR is to synchronize resource changes between SCIM replicas in a common administrative domain. In this mode, information about changes for resources are shared between replicas for immediate processing. The intention is that every replica node contains the same information content in a timely fashion.

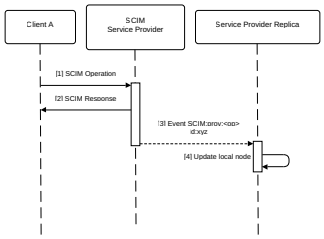

Figure 1: Domain Based Replication Sequence

In this mode, replication is a server-to-server process and it is assumed that access rights between servers is identical. Access to these messages MUST be limited to communication between replicating nodes with appropriate authorization. From a Privacy Perspective, it is assumed that all replicas of the server are in the same administrative domain and that the sharing of information is primarily for performance and availability reasons and the sharing information between replicas does not by itself enable access to new parties (e.g. where a user may not have consented).

2.2. Co-ordinated Provisioning

In "Co-ordinated Provisioning" (CP), SCIM resource change events are shared between domains with the restriction that the actual attribute value data is omitted. In any Event Publisher and Receiver relationship, the set of SCIM resources that are co-ordinated is managed within the context of a "Feed" and MAY be a subset of the total set of resources on either side. To support this, "feed" events are defined that indicate the addition and removal of SCIM resources from a feed. For example, when a user consents to the sharing of information between domains, events about the User MAY be added to the feed between the Event Publisher and Receiver.

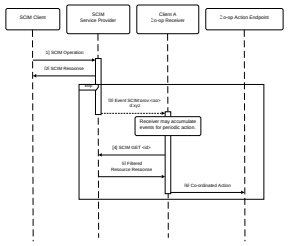

Figure 2: Co-Ordinated Provisioning Sequence

In CP mode, the receiver of an event must call back to the originating SCIM Service Provider (e.g. using a SCIM GET request) to reconcile the newly changed resource in order to obtain the changes.

Co-ordinated provisioning has the following benefits:

- Differences in schema (e.g. attributes) between domains. For example, a receiving domain may only be interested or only be allowed access to a few attributes (e.g. role based access data) to enable access to an application.

- Different Event Receivers MAY have differing needs access to information and thus be assigned varying access rights. Minimal information events combined with call-backs for data allows data filtering to be applied.

- Receivers can take independent action. For example deciding which attributes or resource lifecycle changes to accept. For example, in the case of a conflict, a receiver can prioritize one domain source over another.

- A receiver MAY throttle or buffer changes rather than act immediately on a notification. For example, for a frequently changing resource, the receiver MAY choose to make scheduled SCIM GET for resources that have been marked "dirty" by events received in the last scheduled cycle.

A disadvantage of the CP approach is that it may be considered costly in the sense that each event received might trigger a call back to the event issuer. This cost should be weighed against the cost producing filtered information in each event for each receiver. Further a receiver is not required to make a call-back on every provisioning event.

It is assumed that an underlying relationship between domains exists that permits the exchange of personal information and credentials. For example the decision to perform SCIM provisioning operations at the SCIM Service Provider issuing change events, was previously

authorized and appropriate confidentiality and privacy agreements have been met in cross-domain scenarios. Examples of this might be services for hire by an employer or a specific consent from an end-user as part of a online authorization where individual consent was obtained.

2.3. Risk Signals

The sharing of risk signals (RS) is intended for the purpose of co-ordinating change events between a SCIM Service Provider and another related security service. For example, when a password or other authentication factor has changed, a receiving security system can choose to terminate current User sessions to force a re-authentication against the modified User resource.

These signals MAY also include those described in the OpenID Shared Signals Working Group Specifications [SSWG].

These events are intended for receivers where there is a prior relationship on behalf of the users described in the SCIM Service Provider. The intent of sharing information about security events is for the purpose of securing a user account and ensuring privacy.

2.4. Async Requests

A SCIM provisioning client MAY wish to request "asynchronous" processing using the "Prefer Header for HTTP", Section 4.1 [RFC7240]. In this mode, a normal SCIM protocol POST, PUT, PATCH, or DELETE request is made, and the HTTP Header Prefer is included with the value respond-async. When a SCIM Client signals respond-async, the SCIM server response changes to HTTP Status 202 Accepted as defined in [RFC7231]. The Location header returned is the final resource location and no payload is present. Following acceptance of an asynchronous request, a notification of completion can be issued using the Async Event Notification per Section 3.5.1. The location returned SHALL correspond to the sub claim in the future Async Event SET message.

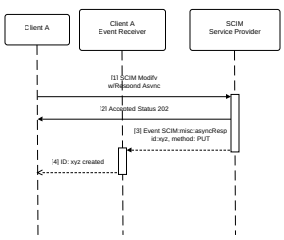

Figure 3: Asychronous Request Sequence

3. SCIM Events

A SCIM event is a message, in the form of a Security Event Token [RFC8417], that conveys information about changes that have occurred at a SCIM Service Provider that may be of interest to a receiving system. Examples of events include:

- Resource lifecycle events including creation, activation, deactivation, and removal of a resource.
- Risk signal events (e.g. password reset, authentication factor change) which may be used by a receiver to take a security response such as resetting or revoking current user sessions and tokens.
- A Password update event is used to securely distribute a hashed value in an administrative domain.
- A Async Event is used to acknowledge completion status of an Asynchronous SCIM Request.

3.1. Common Event Attributes

The following attributes are available for all events defined. The values are contained within the event payload per Section 2 [RFC8417].

id
: A SCIM id attribute identifying the SCIM Service Provider's resource that was modified. This value is required.

externalId
: If known, the externalId value of the SCIM Resource that MAY be used by a receiver to identify the corresponding resource in the Event Receiver's domain.

txn
: For the purposes of SCIM, this SET claim should be used to identify unique transactions originating at a SCIM Service Provider. The purpose is to detect duplicate transactions that may have been received. If not provided, the SET jti claim MAY be used. The difference is that txn identifies uniqueness within a SCIM Service Provider whereas JTI only identifies a unique JWT token.

data
: Defined in SCIM Bulk Operations, Section 3.7 [RFC7644], contains the information necessary to propagate the transaction to the receiving node. For example, after processing a SCIM Create operation, the data contained includes the final representation

of the created entity by the SCIM Service Provider including the assigned id value.

attributes
An array of attributes that were added, revised, or removed. For example:
"attributes": ["username","emails"]

Depending on the Processing Mode or Event definition, usually only one of data or attributes is provided.

The sub claim SHALL hold the SCIM Service Provider's Resource URI value of the affected object. Note: that the SCIM Bulk path attribute is SHALL NOT be used as this duplicates the sub claim.

This specifications defines a new schema URI prefix urn:ietf:params:event:SCIM which is used as the prefix for the following defined SCIM Events.

3.2. SCIM Feed Events

This section defines events related to notices about which resources are being added or removed from an event feed. These events are used in Co-operative Provisioning scenarios where only a sub-set of entities are shared across an Event Feed. The URI prefix for these events is: urn:ietf:params:event:SCIM:feed

3.2.1. urn:ietf:params:event:SCIM:feed:add

The specified resource was added to the Event Feed. A feed:add does not indicate a resource is new or has been recently created. For example, an existing user has had a new role (e.g. CRM_User) added to their profile which has caused their resource to join a feed.

```
{
  "jti": "6164f3bbf6ff41a88dc94f18cb0620e8",
  "sub": "/Users/2b2f880af6674ac284bae9381673d462",
  "txn": "b7b953f11cc6489bbfb87834747cc4c1",
  "events":{
    "urn:ietf:params:event:SCIM:feed:add": {
        "id":"2b2f880af6674ac284bae9381673d462"
    }
  },
  "iat": 1458505044,
  "iss":"https://scim.example.com",
  "aud":[
   "https://scim.example.com/Feeds/98d52461fa5bbc879593b7754"
  ]
}
```

Figure 4: Example SCIM Feed Add Event

3.2.2. urn:ietf:params:event:SCIM:feed:remove

The specified resource has been removed from the feed. Removal does not indicate that the resource was deleted or otherwise deactivated. This event has minimal disclosure.

```
{
  "jti": "6164f3bbf6ff41a88dc94f18cb0620e8",
  "sub": "/Users/2b2f880af6674ac284bae9381673d462",
  "events":{
    "urn:ietf:params:event:SCIM:feed:remove": {
        "id": "2b2f880af6674ac284bae9381673d462"
    }
  },
  "iat": 1458505044,
  "iss":"https://scim.example.com",
  "aud":[
   "https://scim.example.com/Feeds/98d52461fa5bbc879593b7754"
  ]
}
```

Figure 5: Example SCIM Feed Remove Event

3.3. SCIM Provisioning Events

This section defines provisioning events that have occurred within a SCIM Service Provider. These events are used in both Domain Based Replication (DBR) and Co-operative Provisioning (CP) mode. The URI prefix for these events is: urn:ietf:params:event:SCIM:prov

3.3.1. urn:ietf:params:event:SCIM:prov:create

Indicates a new SCIM resource has been created by the SCIM Service Provider and has been added to the Event Feed. Note that when a create event is sent, a corresponding urn:ietf:params:event:SCIM:feed:add event SHOULD NOT be issued in the same feed. In DBR mode mode, all claims of the new resource are included. In CP mode, the attributes returned discloses what attributes were created at the publisher. In DBR mode, the set of values reflecting the final state of the resource at the service provider are provided using the "data" attribute. Note that because this is a replication request, the id attribute that was assigned by the SCIM Service Provider is shared so that all replicas in the domain use the same resource identifier.

```
{
  "jti": "4d3559ec67504aaba65d40b0363faad8",

  "iat": 1458496404,
  "iss":"https://scim.example.com",
  "aud":[
    "https://scim.example.com/Feeds/98d52461fa5bbc879593b7754",
    "https://scim.example.com/Feeds/5d7604516b1d08641d7676ee7"
  ],
  "sub": "/Users/44f6142df96bd6ab61e7521d9",
  "events":{
    "urn:ietf:params:event:SCIM:prov:create":{
      "id":"44f6142df96bd6ab61e7521d9",
      "externalId":"jdoe",
      "data":{
        "schemas":[ "urn:ietf:params:scim:schemas:core:2.0:User"],
        "emails":[
          {"type":"work","value":"jdoe@example.com"}
        ],
        "userName":"jdoe",
        "name":{
          "givenName":"John",
          "familyName":"Doe"
        }
      }
    }
  }
}
```


Figure 6: Example SCIM Create (Domain Replication Mode)

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

Figure 7: Example SCIM Create Event (CP Mode)

The event above notifies the Event Receiver which attributes have changed but does not convey the actual information. The Event Receiver MAY retrieve that information by performing a SCIM GET to the sub value specified.

3.3.2. urn:ietf:params:event:SCIM:prov:patch

The specified resource has been updated using SCIM PATCH. When in DBR mode, the data attribute contains the PATCH Request body. In CP mode, only the modified attribute name is included.

```
{
  "jti": "6164f3bbf6ff41a88dc94f18cb0620e8",
  "sub": "/Groups/acbf3ae7-8463-...-9b4da3f908ce",
  "events":{
    "urn:ietf:params:event:SCIM:prov:patch": {
      "id": "acbf3ae7-8463-...-9b4da3f908ce",
      "externalId":"crmUsers",
      "version": "a330bc54f0671c9",
      "data": {
        "schemas":
      ["urn:ietf:params:scim:api:messages:2.0:PatchOp"],
        "Operations":[{
          "op":"add",
          "path":"members",
          "value":[{
             "display": "Babs Jensen",
             "$ref": "/Users/2819c223...413861904646",
             "value": "2819c223-7f76-453a-919d-413861904646"
          }]
        }]
      }
    }
  },
  "iat": 1458505044,
  "iss":"https://scim.example.com",
  "aud":[
   "https://scim.example.com/Feeds/98d52461fa5bbc879593b7754"
  ]
}
```


Figure 8: Example SCIM Patch Event (DBR Mode)


```
{
  "jti": "6164f3bbf6ff41a88dc94f18cb0620e8",
  "sub": "/Groups/acbf3ae7-8463-...-9b4da3f908ce",
  "events":{
    "urn:ietf:params:event:SCIM:prov:patch": {
      "id": "acbf3ae7-8463-...-9b4da3f908ce",
      "externalId":"crmUsers",
      "attributes": ["members"],
      "version": "a330bc54f0671c9"
    }
  },
  "iat": 1458505044,
  "iss":"https://scim.example.com",
  "aud":[
   "https://scim.example.com/Feeds/98d52461fa5bbc879593b7754"
  ]
}
```

Figure 9: Example SCIM Patch Event (CP Mode)

3.3.3. urn:ietf:params:event:SCIM:prov:put

The specified resource has been updated (e.g. one or more attributes has changed). In DBR mode, the SCIM PUT request body is included in the data attribute; or, In CP mode the modified attributes are listed using attributes.


```
{
  "jti": "6164f3bbf6ff41a88dc94f18cb0620e8",
  "sub": "/Users/2819c223-7f76-453a-919d-413861904646",
  "events":{
    "urn:ietf:params:event:SCIM:prov:patch": {
      "id": "2819c223-7f76-453a-919d-413861904646",
      "version": "a330bc54f0671c9",
      "data": {
        "schemas":["urn:ietf:params:scim:schemas:core:2.0:User"],
        "id":"2819c223-7f76-453a-919d-413861904646",
        "userName":"jdoe",
        "externalId":"jdoe",
        "name":{
           "formatted":"Mr. Jon Jack Doe III",
           "familyName":"Doe",
           "givenName":"Jon",
           "middleName":"Jack"
        },
        "roles":[],
        "emails":[
          {"value":"jdoe@example.com"},
          {"value":"anon@jdoe.org"}
        ]
      }
    }
  },
  "iat": 1458505044,
  "iss":"https://scim.example.com",
  "aud":[
   "https://scim.example.com/Feeds/98d52461fa5bbc879593b7754"
  ]
}
```


Figure 10: Example SCIM Put Event (DBR Mode)

```
{
  "jti": "6164f3bbf6ff41a88dc94f18cb0620e8",
  "sub": "/Users/2819c223-7f76-453a-919d-413861904646",
  "events":{
    "urn:ietf:params:event:SCIM:prov:patch": {
      "id": "2819c223-7f76-453a-919d-413861904646",
      "version": "a330bc54f0671c9",
      "attributes": ["userName","externalId","name","roles","emails"]
    }
  },
  "iat": 1458505044,
  "iss":"https://scim.example.com",
  "aud":[
   "https://scim.example.com/Feeds/98d52461fa5bbc879593b7754"
  ]
}
```

Figure 11: Example SCIM Put Event (CP Mode)

3.3.4. urn:ietf:params:event:SCIM:prov:delete

The specified resource has been deleted from the SCIM publisher. The resource is also removed from the feed. When a DELETE is sent, a corresponding feedRemove is not issued. A delete event has minimal disclosure profile only.

```
{
  "jti": "6164f3bbf6ff41a88dc94f18cb0620e8",
  "sub": "/Users/2b2f880af6674ac284bae9381673d462",
  "events":{
    "urn:ietf:params:event:SCIM:prov:delete": {
        "id": "2b2f880af6674ac284bae9381673d462",
        "externalId": "jDoe"
    }
  },
  "iat": 1458505044,
  "iss":"https://scim.example.com",
  "aud":[
   "https://scim.example.com/Feeds/98d52461fa5bbc879593b7754"
  ]
}
```

Figure 12: Example SCIM Delete Event

3.3.5. urn:ietf:params:event:SCIM:prov:activate

The specified resource (e.g. User) has been activated. This event indicates a high-level change in state as agreed between the Event Publisher and Event Receiver. For example, an activated resource is

one that can now have an active session (may log in) from a security perspective.

```
{
  "jti": "6164f3bbf6ff41a88dc94f18cb0620e8",
  "sub": "/Users/2b2f880af6674ac284bae9381673d462",
  "events":{
    "urn:ietf:params:event:SCIM:prov:activate": {
      "id": "2b2f880af6674ac284bae9381673d462"
    }
  },
  "iat": 1458505044,
  "iss":"https://scim.example.com",
  "aud":[
   "https://scim.example.com/Feeds/98d52461fa5bbc879593b7754"
  ]
}
```

Figure 13: Example SCIM Activate Event

3.3.6. urn:ietf:params:event:SCIM:prov:deactivate

The specified resource (e.g. User) has been deactivated and disabled. The exact meaning must be agreed to by the Event Publisher and its corresponding Event Receiver. Typically this means the sub may no longer have an active security session. As with the activate event, this event has minimal disclosure requirements.

3.4. SCIM Signals Events

This section defines security signal events that have occured within a SCIM Service Provider.The URI prefix for these events is: urn:ietf:params:event:SCIM:signal

3.4.1. urn:ietf:params:event:SCIM:sig:authMethod

A new authentication method has been added to the User profile. As attackers often use new authentication methods to lock-out Users from their account, this signal can be used by the receiver that the chance of account them may be temporarily elevated. The receiver MAY also wish to take action such as resetting current authorizations or sessions.

```
{
  "jti": "3d0c3cf797584bd193bd0fb1bd4e7d30",
  "sub": "/Users/44f6142df96bd6ab61e7521d9",
  "events":{
    "urn:ietf:params:event:SCIM:sig:authMethod": {
        "id": "44f6142df96bd6ab61e7521d9"
    }
  },
  "iat": 1458496025,
  "iss": "https://scim.example.com"
}
```

Figure 14: Example SCIM Authentication Factor Change Event

3.4.2. urn:ietf:params:event:SCIM:sig:pwdReset

The specified resource (e.g. User) has changed its password or the password has been reset. When the password has changed, the attributes attribute is supplied with the value "password".

```
{
  "jti": "3d0c3cf797584bd193bd0fb1bd4e7d30",
  "sub": "/Users/44f6142df96bd6ab61e7521d9",
  "events": {
    "urn:ietf:params:event:SCIM:sig:pwdReset": {
      "id": "44f6142df96bd6ab61e7521d9"
    }
  },
  "iat": 1458496025,
  "iss": "https://scim.example.com",
  "aud":[
    "https://jhub.example.com/Feeds/98d52461fa5bbc879593b7754",
    "https://jhub.example.com/Feeds/5d7604516b1d08641d7676ee7"
  ]
}
```

Figure 15: Example SCIM Password Change Event

3.5. Miscellaneous Events

This section defines events related miscellaneous events such as Asynchronous Request complettion that have occured within a SCIM Service Provider. The URI prefix for these events is: urn:ietf:params:event:SCIM:misc

3.5.1. urn:ietf:params:event:SCIM:misc:asyncResp

This event signals the completion of a SCIM request. The payload contains the attributes defined in SCIM Bulk Section 3.7 [RFC7644]

and is the same a single SCIM Bulk Response Operation as per Section 3.7.3.


```
{
  "jti": "6164f3bbf6ff41a88dc94f18cb0620e8",
  "sub": "/Users/b7c14771-226c-4d05-8860-134711653041",
  "txn": "7880fc68a2f0428ebbb5a906e5aeae53",
  "events":{
    "urn:ietf:params:event:SCIM:misc:asyncResp": {
        "id":"b7c14771-226c-4d05-8860-134711653041",
        "method": "PUT",
        "version": "W\/\"huJj29dMNgu3WXPD\"",
        "status": "200"
    }
  },
  "iat": 1458505044,
  "iss":"https://scim.example.com",
  "aud":[
   "https://scim.example.com/Feeds/98d52461fa5bbc879593b7754"
  ]
}
```


Figure 16: Example SCIM Async Response Event

4. Event Delivery

As Security Event Tokens are based on JWT tokens, it is possible to exchange events by a number of transfer mechanisms such as: XMPP [RFC6120], HTTP [RFC7540], and Message Buses (e.g. [RFC3259], Apache Kafka [Kafka]). This draft discusses 2 general delivery methods: Message Bus and Point-to-Point.

4.1. Security Event Token Signing and Encryption

This specification uses Security Event Tokens as the message format for SCIM Events. As SETs are based on JWT tokens [RFC7519], they can be transmitted unsecurity, signed, or encrypted. For more information see the JWT Cookbook specification [RFC7520] for examples. The decision on whether to use JWS and JWE depends on operational considerations. For each SCIM Feed relationship, it is up to deployers to decide on signing, encryption and algorithm requirements. Deployers SHOULD be aware that too much emphasis on turning on every possible encryption feature may cause operational performance to suffer. Deployers MUST weigh the security trade-offs of up-to-date SCIM services, vs. the potential information loss of an event.

Unsecured

Per Section 6 [RFC7519], tokens MAY be generated with {"alg":"none"}. This mode speeds up processing and is best used in DBR scenarios. Unencrypted tokens MUST be transferred over authenticated TLS layer encryption and SHOULD only be used in a restricted network environment.

Signed

JWS ([RFC7515]) signed SETs are useful when it is important to be able to verify the issuer of a SET as valid. In addition, some systems MAY wish to validate the authenticity of the event in a review process which may occur at a later date. While the content can be validated as originating from the correct issuer and is unmodified, the message contents remain unsecure. Signed SETs MUST be transferred over encrypted transport.

Encrypted

JWE ([RFC7516]) are encrypted SETs and are useful when the transport mechanism is not fully securable (e.g. messages carried by a third party). The use of JWEs ensures only the designated receiver can read the event and provides mutual authentication within the SET mesage itself.

4.2. Point-to-Point Delivery Over HTTP

Security Event Tokens MAY be delivered using push-based HTTP delivery [RFC8935], or pull-based HTTP Polling [RFC8936]. Both of these protocols define a method of transfer and acknowledgement to prevent loss-of-information and to provide re-transmission and recover. The method of transfer is best decided by considering the following advantages and disadvantages in a production scenario:

Push-based delivery has the following advantages:

* Message transfer is instant (when compared to using a common Event Publisher acting as a relay), and in high event frequency scenarios, HTTP connections can be kept open.

* Scales well when an SCIM Event Publisher has thousands of event receivers and TCP resources may be limited.

* Does not require events to be routed to a single publisher node. SCIM Events may be issued by SCIM Service Provider nodes where the transaction occurred.

* SCIM Events only need to be retained until they have been delivered to designated receivers.

Push-delivery has the following disadvantages:

* A SCIM Event Publisher system needs authorization credentials enabling it to access the HTTP SCIM Event delivery endpoint.

* When synchronizing business data that is behind protected firewalls, a virtual network or other firewall policy may be required to allow external network based SCIM providers to deliver SCIM Events to internally hosted systems.

Delivery by HTTP Polling has the following advantages:

* It is possible for a SCIM Event Receiver to use the same SCIM credentials it uses when access the normal SCIM Service Provider service defined by [RFC7644].

* Systems behind protected network boundaries can reach externally hosted systems without requiring special firewall or network configuration.

* Instantaneous transfer can be used using HTTP Long-polling as described Section 2.1 of [RFC8936].

Polling-based delivery has the following disadvantages:

* Long-polling requires the use of persistent connections for which TCP resources may be limited. HTTP Long-polling is best used in scenarios when there are relatively few Event Receivers.

* The SCIM Event Publisher MUST retain events for the Event Receiver until delivered.

4.3. Using Message Bus Delivery

Security Event Tokens MAY be delivered using a message bus. While this draft will not talk about any particular message bus, it will discuss the pros and cons for message buses in general and any anticipated issues and requirements.

Message buses have the following advantages:

* Connection management and credentials may be greatly simplified as participants only need to authenticate to the "bus" to issue and receive events.

* Message buses can have "broadcast" features that are able to deliver the same event to many recipients such as in a global deployment of replicated SCIM servers. Issuers save resources by only having to publish once to a bus rather than to each receiver directly.

*Depending on the implementation, a Message Bus can be used as a buffer and in some cases for data recovery. For example, some buses may have infinite retention of events.

*Message-buses can support bi-directional and other more complex flow relationships (e.g. sharding).

Message buses may have following disadvantages:

*A message bus may have some delivery delays (seconds to minutes) when compared to point-to-point systems.

*Message buses may require significant infrastructure commitments in order to meet delivery reliability. However it may also be true that a point-to-point system may also impose significant resource requirements requiring a SCIM service provider to assume the same work.

*Multi-issuer scenarios may require more conflict resolution processing. E.g. such as prioritizing specific nodes as "masters" for specific SCIM attributes.

5. Event Handling

5.1. Conflict Resolution

In scenarios where there may be multiple issuers of SCIM Events, it becomes possible that conflicts can arise when the same version of a resource is modified by multiple parties.

Editors note: TO BE COMPLETED

5.2. Optimizing Events

In cases where resources change frequently, SCIM Service Providers MAY choose to release events on an interval basis in order to reduce traffic. For example, a large Group with millions of members may have hundreds of changes per minute. For optimization, a SCIM Service Provider MAY choose to issue a cumulative event once per minute instead of for each change event.

Editors note: TO BE COMPLETED

6. Security Considerations

[[TO BE COMPLETED]]

7. Privacy Considerations

[[TO BE COMPLETED]]

8. IANA Considerations

This section registers the schema extensions found in Section 3 in the "Event" registry as per Section 4.2 [RFC8417].

Schema URI: SeeSection 3.

Schema Name: See corresponding names underSection 3.

Intented ResourceType: N/A. Events are not intended to be persisted in SCIM.

Purpose: See each description inSection 3.

Single-valued Attributes: None.

Multi-valued Attributes: All schemas in this specification share the same attributes. SeeSection 3.1.

Summary of schema URI registrations:

Schema URI	Name	Reference
urn:ietf:params:event:SCIM:feed:add	Resource added to Feed Event	Section 3.2.1
urn:ietf:params:event:SCIM:feed:remove	Remove resouce From Feed Event	Section 3.2.2
urn:ietf:params:event:SCIM:prov:create	New Resource Event	Section 3.3.1
urn:ietf:params:event:SCIM:prov:patch	Resource Patch Event	Section 3.3.2
urn:ietf:params:event:SCIM:prov:put	Resource Put Event	Section 3.3.3
urn:ietf:params:event:SCIM:prov:delete	Resource Deleted Event	Section 3.3.4
urn:ietf:params:event:SCIM:prov:activate	Resource Activated Event	Section 3.3.5
urn:ietf:params:event:SCIM:prov:deactivate	Resource Deactivated Event	Section 3.3.6
urn:ietf:params:event:SCIM:sig:authMethod	New authentication method added	Section 3.4.1
urn:ietf:params:event:SCIM:sig:pwdReset	Password Reset Event	Section 3.4.2

Table 1

9. References

9.1. Normative References

[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>.

[RFC3986] Berners-Lee, T., Fielding, R., and L. Masinter, "Uniform Resource Identifier (URI): Generic Syntax", STD 66, RFC 3986, DOI 10.17487/RFC3986, January 2005, <https://www.rfc-editor.org/info/rfc3986>.

[RFC7231] Fielding, R., Ed. and J. Reschke, Ed., "Hypertext Transfer Protocol (HTTP/1.1): Semantics and Content", RFC 7231, DOI 10.17487/RFC7231, June 2014, <https://www.rfc-editor.org/info/rfc7231>.

[RFC7240] Snell, J., "Prefer Header for HTTP", RFC 7240, DOI 10.17487/RFC7240, June 2014, <https://www.rfc-editor.org/info/rfc7240>.

[RFC7515] Jones, M., Bradley, J., and N. Sakimura, "JSON Web Signature (JWS)", RFC 7515, DOI 10.17487/RFC7515, May 2015, <https://www.rfc-editor.org/info/rfc7515>.

[RFC7516] Jones, M. and J. Hildebrand, "JSON Web Encryption (JWE)", RFC 7516, DOI 10.17487/RFC7516, May 2015, <https://www.rfc-editor.org/info/rfc7516>.

[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>.

[RFC7520] Miller, M., "Examples of Protecting Content Using JSON Object Signing and Encryption (JOSE)", RFC 7520, DOI 10.17487/RFC7520, May 2015, <https://www.rfc-editor.org/info/rfc7520>.

[RFC7643] Hunt, P., Ed., Grizzle, K., Wahlstroem, E., and C. Mortimore, "System for Cross-domain Identity Management: Core Schema", RFC 7643, DOI 10.17487/RFC7643, September 2015, <https://www.rfc-editor.org/info/rfc7643>.

[RFC7644] Hunt, P., Ed., Grizzle, K., Ansari, M., Wahlstroem, E., and C. Mortimore, "System for Cross-domain Identity Management: Protocol", RFC 7644, DOI 10.17487/RFC7644, September 2015, <https://www.rfc-editor.org/info/rfc7644>.

[RFC8174] Leiba, B., "Ambiguity of Uppercase vs Lowercase in RFC 2119 Key Words", BCP 14, RFC 8174, DOI 10.17487/RFC8174, May 2017, <https://www.rfc-editor.org/info/rfc8174>.

[RFC8417] Hunt, P., Ed., Jones, M., Denniss, W., and M. Ansari, "Security Event Token (SET)", RFC 8417, DOI 10.17487/RFC8417, July 2018, <https://www.rfc-editor.org/info/rfc8417>.

[SSWG] Tulshibagwale, A., Cappalli, T., Scurtescu, M., Backman, A., and J. Bradley, "OpenID Shared Signals and Events Framework Specification 1.0 - draft 01", 8 June 2021. Cappalli, T. and A. Tulshibagwale, "OpenID Continuous Access Evaluation Profile 1.0 - draft 02", 8 June 2021.

9.2. Informative References

[Kafka] Apache Software Foundation, "Apache Kafka", 2017.

[RFC3259] Ott, J., Perkins, C., and D. Kutscher, "A Message Bus for Local Coordination", RFC 3259, DOI 10.17487/RFC3259, April 2002, <https://www.rfc-editor.org/info/rfc3259>.

[RFC6120] Saint-Andre, P., "Extensible Messaging and Presence Protocol (XMPP): Core", RFC 6120, DOI 10.17487/RFC6120, March 2011, <https://www.rfc-editor.org/info/rfc6120>.

[RFC7540] Belshe, M., Peon, R., and M. Thomson, Ed., "Hypertext Transfer Protocol Version 2 (HTTP/2)", RFC 7540, DOI 10.17487/RFC7540, May 2015, <https://www.rfc-editor.org/info/rfc7540>.

[RFC8935] Backman, A., Ed., Jones, M., Ed., Scurtescu, M., Ansari, M., and A. Nadalin, "Push-Based Security Event Token (SET) Delivery Using HTTP", RFC 8935, DOI 10.17487/RFC8935, November 2020, <https://www.rfc-editor.org/info/rfc8935>.

[RFC8936] Backman, A., Ed., Jones, M., Ed., Scurtescu, M., Ansari, M., and A. Nadalin, "Poll-Based Security Event Token (SET) Delivery Using HTTP", RFC 8936, DOI 10.17487/RFC8936, November 2020, <https://www.rfc-editor.org/info/rfc8936>.

Appendix A. Acknowledgments

Thanks to Morteza Ansari who contributed significantly to draft-hunt-idevent-scim-00, upon which this draft is based.

The editor would like to thank the participants in the the SCIM working group and the id-event list for their support of this specification.

Appendix B. Change Log

Draft 00 - PH - First Draft

Author's Address

Phil Hunt (editor)
Independent Identity Inc

Email: phil.hunt@independentid.com