Subject Identifiers for Security Event Tokens
draft-ietf-secevent-subject-identifiers-00

Abstract

   Security events communicated within Security Event Tokens may support
   a variety of identifiers to identify the subject and/or other
   principals related to the event. This specification formalizes the
   notion of subject identifiers as named sets of well-defined claims
   describing the subject, a mechanism for representing subject
   identifiers within a [JSON] object such as a JSON Web Token [JWT] or
   Security Event Token [SET], and a registry for defining and
   allocating names for these claim sets.

Table of Contents

1. Introduction

As described in section 1.2 of [SET], the subject of a security event
may take a variety of forms, including but not limited to a JWT
principal, an IP address, a URL, etc. Furthermore, even in the case
where the subject of an event is more narrowly scoped, there may be
multiple ways by which a given subject may be identified. For
example, an account may be identified by an opaque identifier, an
email address, a phone number, a JWT "iss" claim and "sub" claim,
etc., depending on the nature and needs of the transmitter and
receiver. Even within the context of a given transmitter and
receiver relationship, it may be appropriate to identify different
accounts in different ways, for example if some accounts only have
email addresses associated with them while others only have phone
numbers. Therefore it can be necessary to indicate within a SET the
mechanism by which the subject of the security event is being
identified.

2. 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].

3. Subject Identifiers

A Subject Identifier Type is a light-weight schema that describes a set of claims that 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 4.1. A Subject Identifier Type MAY describe more claims than are strictly necessary to uniquely identify a subject, and MAY describe conditions under which those claims are required, optional, or prohibited.

A Subject Identifier is a [JSON] object containing a "subject_type" claim whose value is the unique name of a Subject Identifier Type, and a set of additional "payload claims" which are to be interpreted according to the rules defined by that Subject Identifier Type. Payload claim values MUST match the format specified for the claim by the Subject Identifier Type. A Subject Identifier MUST NOT contain any payload claims prohibited or not described by its Subject Identifier Type, and MUST contain all payload claims required by its Subject Identifier Type.

The following Subject Identifier Types are registered in the IANA "Security Event Subject Identifier Types" registry established by Section 4.1.

3.1. 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".

Below is a non-normative example Subject Identifier for the Email Subject Identifier Type:

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

Figure 1: Example: Subject Identifier for the Email Subject Identifier Type.

3.2. 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".

Below is a non-normative example Subject Identifier for the Email
Subject Identifier Type:

```
{
  "subject_type": "phone",
  "phone": "+1 (206) 555-0100",
}
```

Figure 2: Example: Subject Identifier for the Phone Number Subject
Identifier Type.

3.3. 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 [JWT], 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".

Below is a non-normative example Subject Identifier for the Issuer
and Subject Subject Identifier Type:

```
{
  "subject_type": "iss_sub",
  "iss": "http://issuer.example.com/",
  "sub": "145234573",
}
```

Figure 3: Example: Subject Identifier for the Issuer and Subject
Subject Identifier Type.

3.4. 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
   A "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".

Below is a non-normative example Subject Identifier for the ID Token
Claims Subject Identifier Type:

```
{
  "subject_type": "id_token_claims",
  "iss": "http://issuer.example.com/",
  "sub": "145234573",
  "email": "user@example.com",
}
```

Figure 4: Example: Subject Identifier for the ID Token Claims Subject
Identifier Type.

4. IANA Considerations

4.1. 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 3. Future
assignments are to be made through the Expert Review registration
policy [BCP26] and shall follow the template presented in
Section 4.1.1.

4.1.1. Registration Template

Type Name
    The name of the Subject Identifier Type, as described in
    Section 3. 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 "OpenID Foundation 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.

4.1.2. Initial Registry Contents

4.1.2.1. Email Subject Identifier Type

o Type Name: "email"

o Type Description: Subject identifier based on email address.

o Change Controller: IETF secevent Working Group

o Defining Document(s): Section 3 of this document.

4.1.2.2. ID Token Claims Subject Identifier Type

o Type Name: "id_token_claims"

o Type Description: Subject identifier based on OpenID Connect ID
   Token claims.

o Change Controller: IETF secevent Working Group

o Defining Document(s): Section 3 of this document.

4.1.2.3. Issuer and Subject Subject Identifier Type

o Type Name: "iss_sub"

o Type Description: Subject identifier based on an issuer and
   subject.

o Change Controller: IETF secevent Working Group

o Defining Document(s): Section 3 of this document.

4.1.2.4. Phone Number Subject Identifier Type

o Type Name: "phone"

o Type Description: Subject identifier based on an phone number.

o Change Controller: IETF secevent Working Group

o Defining Document(s): Section 3 of this document.

4.1.3. 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.

5. Privacy Considerations

There are no privacy considerations.

6. Security Considerations

There are no security considerations.

7. 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://www.rfc-editor.org/info/rfc8126>.

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

[IDTOKEN] Sakamura, N., Bradley, J., Jones, M., de Medeiros, B., and
           C. Mortimore, "OpenID Connect Core 1.0 - ID Token", April
           2017, <http://openid.net/specs/
           openid-connect-core-1_0.html#IDToken>.

[JSON]   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>.

[JWT]   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>.

[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>.

[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>.

[SET]   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>.

Acknowledgements

   This document is based on work developed within the OpenID RISC
   Working Group. The authors would like to thank the members of this
   group for their hard work and contributions.

Change Log

   (This section to be removed by the RFC Editor before publication as
   an RFC.)

   Draft 00 - AB - First draft

Authors' Addresses

   Annabelle Backman
   Amazon

   Email: richanna@amazon.com

   Marius Scurtescu
   Google

   Email: mscurtescu@google.com