Security Events Working Group
Internet-Draft
Intended status: Standards Track
Expires: January 25, 2020

A. Backman, Ed.
Amazon
M. Scurtescu
Coinbase

July 24, 2019

Subject Identifiers for Security Event Tokens
draft-ietf-secevent-subject-identifiers-05

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.

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 January 25, 2020.

Copyright Notice

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 7.1. A Subject Identifier Type MAY describe more claims than are strictly necessary to 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 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 7.1.

3.1. Account Subject Identifier Type

The Account Subject Identifier Type describes a user account at a service provider, identified with an "acct" URI as defined in [RFC7565]. Subject Identifiers of this type MUST contain a "uri" claim whose value is the "acct" URI for the subject. The "uri" claim is REQUIRED and MUST NOT be null or empty. The Account Subject Identifier Type is identified by the name "account".

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

```
{
  "subject_type": "account",
  "uri": "acct:example.user@service.example.com",
}
```

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

3.2. Email Subject Identifier Type

The Email Subject Identifier Type describes a principal identified with an email address. Subject Identifiers of this type MUST contain an "email" claim whose value is a string containing the email address of the subject, formatted as an "addr-spec" as defined in Section 3.4.1 of [RFC5322]. The "email" claim is REQUIRED and MUST NOT be null or empty. The value of the "email" claim SHOULD identify a mailbox to which email may be delivered, in accordance with [RFC5321]. 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 2: Example: Subject Identifier for the Email Subject Identifier Type.

3.2.1. Email Canonicalization

Many email providers will treat multiple email addresses as equivalent. For example, some providers treat email addresses as case-insensitive, and consider "user@example.com", "User@example.com", and "USER@example.com" as the same email address. This has led users to view these strings as equivalent, driving service providers to implement proprietary email canonicalization algorithms to ensure that email addresses entered by users resolve to the same canonical string. When receiving an Email Subject Identifier, the recipient SHOULD use their implementation's canonicalization algorithm to resolve the email address to the same subject identifier string used in their system.

3.3. Phone Number Subject Identifier Type

The Phone Number Subject Identifier Type describes a principal identified with a telephone number. Subject Identifiers of this type MUST contain a "phone_number" 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_number" claim is REQUIRED and MUST NOT be null or empty. The Phone Number Subject Identifier Type is identified by the name "phone-number".

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

```
{
  "subject_type": "phone-number",
  "phone_number": "+12065550100",
}
```

Figure 3: Example: Subject Identifier for the Phone Number Subject Identifier Type.

3.4. Issuer and Subject Subject Identifier Type

The Issuer and Subject Subject Identifier Type describes a principal identified with a pair of "iss" and "sub" claims, as defined by [JWT]. 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 are REQUIRED and 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 4: Example: Subject Identifier for the Issuer and Subject Subject Identifier Type.

3.5. Aliases Subject Identifier Type

The Aliases Subject Identifier Type describes a subject that is identified with a list of different Subject Identifiers. It is intended for use when a variety of identifiers have been shared with the party that will be interpreting the Subject Identifier, and it is unknown which of those identifiers they will recognize or support. Subject Identifiers of this type MUST contain an "identifiers" claim whose value is a JSON array containing one or more Subject Identifiers. Each Subject Identifier in the array MUST identify the same entity. The "identifiers" claim is REQUIRED and MUST NOT be null or empty. It MAY contain multiple instances of the same Subject Identifier Type (e.g., multiple Email Subject Identifiers), but SHOULD NOT contain exact duplicates. This type is identified by the name "aliases".

"alias" Subject Identifiers MUST NOT be nested; i.e., the "identifiers" claim of an "alias" Subject Identifier MUST NOT contain a Subject Identifier of type "aliases".

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

```
{
  "subject_type": "aliases",
  "identifiers": [
    {
      "subject_type": "email",
      "email": "user@example.com",
    },
    {
      "subject_type": "phone-number",
      "phone_number": "+12065550100",
    },
    {
      "subject_type": "email",
      "email": "user+qualifier@example.com",
    }
  ],
}
```

Figure 5: Example: Subject Identifier for the Aliases Subject Identifier Type.

4. Subject Identifiers in JWTs

4.1. "sub_id" Claim

This document defines the "sub_id" JWT Claim, in accordance with Section 4.2 of [RFC7519]. When present, the value of this claim MUST be a Subject Identifier that identifies the principal that is the subject of the JWT. The "sub_id" claim MAY be included in a JWT, whether or not the "sub" claim is present. When both the "sub" and "sub_id" claims are present in a JWT, they MUST identify the same principal.

Below is are non-normative examples of JWTs containing the "sub_id" claim:

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

Figure 6: Example: JWT containing a `sub_id` claim and no `sub` claim.

```
{
  "iss": "issuer.example.com",
  "sub": "user@example.com",
  "sub_id": {
    "subject_type": "email",
    "email": "user@example.com",
  },
}
```

Figure 7: Example: JWT where both the `sub` and `sub_id` claims identify the subject using the same identifier.

```
{
  "iss": "issuer.example.com",
  "sub": "user@example.com",
  "sub_id": {
    "subject_type": "email",
    "email": "elizabeth@example.com",
  },
}
```

Figure 8: Example: JWT where both the `sub` and `sub_id` claims identify the subject using different values of the same identifier type.

```
{
  "iss": "issuer.example.com",
  "sub": "user@example.com",
  "sub_id": {
    "subject_type": "account",
    "uri": "acct:example.user@service.example.com",
  },
}
```

Figure 9: Example: JWT where the `sub` and `sub_id` claims identify the subject via different types of identifiers.

4.2. "sub_id" and "iss-sub" Subject Identifiers

The "sub_id" claim MAY contain an "iss-sub" Subject Identifier. In this case, the JWT's "iss" claim and the Subject Identifier's "iss" claim MAY be different. For example, an OpenID Connect [OIDC] client may construct such a JWT when issuing a JWT back to its OpenID Connect Identity Provider, in order to communicate information about the services' shared subject principal using an identifier the Identity Provider is known to understand. Similarly, the JWT's "sub" claim and the Subject Identifier's "sub" claim MAY be different. For example, this may be used by an OpenID Connect client to communicate the subject principal's local identifier at the client back to its Identity Provider.

Below are non-normative examples of a JWT where the "iss" claims are the same, and a JWT where they are different.

```
{
  "iss": "issuer.example.com",
  "sub_id": {
    "subject_type": "iss-sub",
    "iss": "issuer.example.com",
    "sub": "example_user",
  },
}
```

Figure 10: Example: JWT with a `iss-sub` Subject Identifier where JWT issuer and subject issuer are the same.

```
{
  "iss": "client.example.com",
  "sub_id": {
    "subject_type": "iss-sub",
    "iss": "issuer.example.com",
    "sub": "example_user",
  },
}
```

Figure 11: Example: JWT with an `iss-sub` Subject Identifier where the JWT issuer and subject issuer are different.

```
{
  "iss": "client.example.com",
  "sub": "client_user",
  "sub_id": {
    "subject_type": "iss-sub",
    "iss": "issuer.example.com",
    "sub": "example_user",
  },
}
```

Figure 12: Example: JWT with an `iss-sub` Subject Identifier where the JWT `iss` and `sub` claims differ from the Subject Identifier's `iss` and `sub` claims.

5. Privacy Considerations

5.1. Identifier Correlation

The act of presenting two or more identifiers for a single principal together (e.g., within an "aliases" Subject Identifier, or via the "sub" and "sub_id" JWT claims) may communicate more information about the principal than was intended. For example, the entity to which the identifiers are presented, now knows that both identifiers relate to the same principal, and may be able to correlate additional data

based on that. When transmitting Subject Identifiers, the transmitter SHOULD take care that they are only transmitting multiple identifiers together when it is known that the recipient already knows that the identifiers are related (e.g., because they were previously sent to the recipient as claims in an OpenID Connect ID Token).

6. Security Considerations

There are no security considerations.

7. IANA Considerations

7.1. 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 7.1.1.

7.1.1. 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.

7.1.2. Initial Registry Contents

7.1.2.1. Account Subject Identifier Type

- Type Name: "account"
- Type Description: Subject identifier based on "acct" URI.
- Change Controller: IETF secevent Working Group
- Defining Document(s): Section 3 of this document.

7.1.2.2. Email Subject Identifier Type

- Type Name: "email"
- Type Description: Subject identifier based on email address.
- Change Controller: IETF secevent Working Group
- Defining Document(s): Section 3 of this document.

7.1.2.3. Issuer and Subject Subject Identifier Type

- Type Name: "iss-sub"
- Type Description: Subject identifier based on an issuer and subject.
- Change Controller: IETF secevent Working Group
- Defining Document(s): Section 3 of this document.

7.1.2.4. Phone Number Subject Identifier Type

- Type Name: "phone-number"
- Type Description: Subject identifier based on an phone number.
- Change Controller: IETF secevent Working Group
- Defining Document(s): Section 3 of this document.

7.1.2.5. Aliases Subject Identifier Type

- Type Name: "aliases"
- Type Description: Subject identifier that groups together multiple different subject identifiers for the same subject.
- Change Controller: IETF secevent Working Group
- Defining Document(s): Section 3 of this document.

7.1.3. 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.

7.2. JSON Web Token Claims Registration

This document defines the "sub_id" JWT Claim, which IANA is asked to register in the "JSON Web Token Claims" registry IANA JSON Web Token Claims Registry [IANA.JWT.Claims] established by [SET].

7.2.1. Registry Contents

- Claim Name: "sub_id"
- Claim Description: Subject Identifier
- Change Controller: IESG

- Specification Document(s): Section 4.1 of this document.

8. References

8.1. 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>.

[IANA.JWT.Claims] IANA, "JSON Web Token Claims", n.d., <http://www.iana.org/assignments/jwt>.

[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>.

[RFC5321] Klensin, J., "Simple Mail Transfer Protocol", RFC 5321, DOI 10.17487/RFC5321, October 2008, <https://www.rfc-editor.org/info/rfc5321>.

[RFC5322] Resnick, P., Ed., "Internet Message Format", RFC 5322, DOI 10.17487/RFC5322, October 2008, <https://www.rfc-editor.org/info/rfc5322>.

[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>.

[RFC7565] Saint-Andre, P., "The 'acct' URI Scheme", RFC 7565, DOI 10.17487/RFC7565, May 2015, <https://www.rfc-editor.org/info/rfc7565>.

[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>.

8.2. Informative References

[OIDC] Sakimura, N., Bradley, J., Jones, M., de Medeiros, B., and C. Mortimore, "OpenID Connect Core 1.0", November 2014, <http://openid.net/specs/openid-connect-core-1_0.html>.

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

Draft 01 - AB:

- Added reference to RFC 5322 for format of "email" claim.
- Renamed "iss_sub" type to "iss-sub".
- Renamed "id_token_claims" type to "id-token-claims".
- Added text specifying the nature of the subjects described by each type.

Draft 02 - AB:

- Corrected format of phone numbers in examples.
- Updated author info.

Draft 03 - AB:

- Added "account" type for "acct" URIs.
- Replaced "id-token-claims" type with "aliases" type.
- Added email canonicalization guidance.

- Updated semantics for "email", "phone", and "iss-sub" types.

Draft 04 - AB:

- Added "sub_id" JWT Claim definition, guidance, examples.
- Added text prohibiting "aliases" nesting.
- Added privacy considerations for identifier correlation.

Draft 05 - AB:

- Renamed the "phone" type to "phone-number" and its "phone" claim to "phone_number".

Authors' Addresses

Annabelle Backman (editor)
Amazon

Email: richanna@amazon.com

Marius Scurtescu
Coinbase

Email: marius.scurtescu@coinbase.com