Subject Identifiers for Security Event Tokens

Annabelle Backman
IETF 105 – July 2019
Subject Identifiers

• "light-weight schema that describes a set of claims that uniquely identifies a subject."

  • Name
    • email, phone, iss_sub

  • Description of type of entity represented (e.g. user account associated with email)

  • Supported claims
    • { email }, { phone }, { iss, sub }

• IANA Registry: “Security Event Subject Identifier Types”
RISC Example: account_disabled

```json
{
    "iss": "https://risc.example.com/",
    "events": {
        "https://schemas.openid.net/secevent/risc/event-type/account-disabled": {
            "subject": {
                "subject_type": "iss-sub",
                "iss": "https://idp.example.com/",
                "sub": "7375626A656374"
            },
            "reason": "hijacking"
        }
    }
}
```
Current Status

• 04 draft published 2019-07-08

• Applications:
  • OIDF RISC

• Implementations:
  • Google: In progress
  • Amazon: In progress
03 ➔ 04: Identifier Correlation Risk

• See text in the Privacy Considerations section.
03 → 04: Prohibit nested aliases

```json
{
    "subject_type": "aliases",
    "aliases": [
        {
            "subject_type": "aliases",
            "aliases": [
                ...
            ],
        },
    ],
}
```
03 ➔ 04: sub_id JWT Claim

- "...a Subject Identifier that identifies the principal that is the subject of the JWT."

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

• JWTs MAY include sub, sub_id, both, or neither.

• sub and sub_id MUST identify the same principal.

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

```json
{
    "iss":   "issuer.example.com",
    "sub":   "example.user@example.com",
    "sub_id": {
        "subject_type": "account",
        "email": "euser@gmail.com",
    },
}
```
sub_id and sub: Different Types

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

- JWT issuer and subject issuer MAY be different.

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

• Feedback on sub_id?

• ...Are we done here?