Subject Identifiers for Security Event Tokens

Annabelle Backman

IETF 104 – March 2019

Subject Identifier

- JSON object
- Type name in **`subject_type`** property
- Claims according to type definition

Subject Identifier Type

- "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`

```
{
  "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

- 03 draft published 2019-03-11

- Applications:
  - OIDF RISC

- Implementations:
  - Google: In progress
  - Amazon: In progress

02 ➔ 03: `account` URI

- "…a user's account hosted at a service provider…" [RFC7565]

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

02 ➔ 03: ~~id-token-claims~~ aliases

```
{
  "subject_type": "aliases",
  "aliases": [
    {
      "subject_type": "iss-sub",
      "iss": "https://idp.example.com/",
      "sub": "7375626A656374",
    },
    {
      "subject_type": "email",
      "email": "user@example.com",
    },
  ],
}
```

02 ➔ 03: Email Canonicalization

user.name@example.com ≟ username@example.com
≟ User.Name@example.com
≟ Username+foo@example.com

"...the recipient SHOULD use their implementation's canonicalization algorithm to resolve the email address to the same subject identifier string used in their system."

02 ➔ 03: Semantics

`account`	…a user account at a service provider, **identified with** an "acct" URI as defined in [RFC7565].
`email`	…a principal **identified with** an email address
`phone`	…a principal **identified with** a telephone number
`iss-sub`	…a principal **identified with** a pair of "iss" and "sub" claims, as defined by [JWT].
`aliases`	…a subject that is **identified with** a list of different Subject Identifiers.

Open Item: JWT claim?

- Standard claim for representing JWT subject via Subject Identifier
- Because `sub` is a single string
- …applicable to SET?