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

```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

• 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]

```json
{
    "subject_type": "account",
    "uri": "acct:example.user@service.example.com",
}
```
02 → 03: \textbf{id} token \textbf{claims} \textbf{aliases}

```json
{
  "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."
<table>
<thead>
<tr>
<th>account</th>
<th>...a user account at a service provider, identified with an &quot;acct&quot; URI as defined in [RFC7565].</th>
</tr>
</thead>
<tbody>
<tr>
<td>email</td>
<td>...a principal identified with an email address</td>
</tr>
<tr>
<td>phone</td>
<td>...a principal identified with a telephone number</td>
</tr>
<tr>
<td>iss-sub</td>
<td>...a principal identified with a pair of &quot;iss&quot; and &quot;sub&quot; claims, as defined by [JWT].</td>
</tr>
<tr>
<td>aliases</td>
<td>...a subject that is identified with a list of different Subject Identifiers.</td>
</tr>
</tbody>
</table>
Open Item: JWT claim?

• Standard claim for representing JWT subject via Subject Identifier

• Because Sub is a single string

• ...applicable to SET?