Subject Identifiers for Security Event Tokens

Annabelle Backman
IETF 102 – July 2018
Secevents ⇦ RISC ⇦ Secevents

• draft-backman-secevent-subject-identifiers-00

• draft-ietf-secevent-subject-identifiers-00
sub: Suboptimal for Some Scenarios

• Disambiguate multiple identifier types
  • Email
  • Phone #
  • OIDC subject ID
  • Token hashes

• Complex identifiers
  • OIDC issuer and subject
  • Token hash, key description, and algorithm
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",
    }
  }
}
```
Subject Identifier Type

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

• A name for the type
  • email, phone, iss_sub

• The set of supported claims for the type
  • { email }, { phone }, { iss, sub }

• IANA Registry: “Security Event Subject Identifier Types”
Subject Identifier

• JSON object

• Type name in subject_type property

• Claims according to type definition
Example: Email

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

Example: Phone Number

{
    "subject_type": "phone",
    "phone": "+1 206 555 0123"
}
Example: Issuer and Subject

{

    "subject_type": "iss-sub",
    "iss": "https://issuer.example.com/",
    "sub": "abc1234"

}
Example: ID Token Claims

{
    "subject_type": "id-token-claims",
    "iss": "https://issuer.example.com/",
    "sub": "abc1234",
    "email": "user@example.com",
    "phone_number": "+1 206 555 0123"
}
Work Remaining

• Tell me what’s wrong about my IANA Registry definition

• Additional core types?

• Not just for subjects?
OAuth Example: token_revoked

```json
{
    "subject": {
        "subject_type": "oauth_token",
        "token_type": "refresh_token",
        "token_identifier_alg": "token_string",
        "token": "7265667265736820746F6B656E207374726966E67"
    },
    "token_subject": {
        "subject_type": "iss-sub",
        "iss": "https://idp.example.com/",
        "sub": "75736572206964"
    },
    "reason": "inactive"
}
```