Event Stream Management API: RISC Profile

Annabelle Backman, Amazon
IETF 100 Singapore
November 2017
Use Cases

• Enrolling in events for a given subject (Implicit RPs)
• Un-enrolling in events for a given subject
• Selecting desired events
• Configuring delivery methods
• Monitoring stream availability
Authorization

• Bearer tokens via HTTP Authorization header
• No user interaction (e.g. OAuth 2.0 Client Credentials grant)
Subject Types

Email

```
{
    "type": "http://schemas.openid.net/secevent/risc/subject-type/email",
    "email": "user@example.com",
    "email_verified": false
}
```

Phone

```
{
    "type": "http://schemas.openid.net/secevent/risc/subject-type/phone",
    "phone": "+1 206-555-1212",
    "phone_verified": true
}
```

Issuer / Subject

```
{
    "type": "http://schemas.openid.net/secevent/risc/subject-type/iss-sub",
    "iss": "https://id.example.com/",
    "sub": "example.user.id.1234"
}
```
Subject Types: In SETs

Email

```json
{
  "typ": "application/jwt+set",
  "iss": "https://id.example.com/",
  "jti": "example.set.id.1234",
  "txn": "example.txn.1234",
  "risc_subject": {
    "type": "http://schemas.openid.net/secevent/risc/subject-type/email",
    "email": "user@example.com",
    "email_verified": false
  },
  "events": {
    "https://schemas.openid.net/events/risc/account-locked": {
      "reason": "compromise"
    }
  }
}
```
Subject Types: In SETs

Phone

```json
{
   "typ": "application/jwt+set",
   "iss": "https://id.example.com/",
   "jti": "example.set.id.1234",
   "txn": "example.txn.1234",
   "risc_subject": {
      "type": "http://schemas.openid.net/secevent/risc/subject-type/phone",
      "phone": "+1 206-555-1212",
      "phone_verified": true
   },
   "events": {
      "https://schemas.openid.net/events/risc/account-locked": {
         "reason": "compromise"
      }
   }
}
```
Subject Types: In SETs

Issuer and Subject

```json
{
  "typ": "application/jwt+set",
  "iss": "https://id.example.com/",
  "jti": "example.set.id.1234",
  "txn": "example.txn.1234",
  "risc_subject": {
    "type": "http://schemas.openid.net/secevent/risc/subject-type/iss-sub",
    "iss": "https://id.example.com/",
    "sub": "example.user.id.1234"
  },
  "events": {
    "https://schemas.openid.net/events/risc/account-locked": {
      "reason": "compromise"
    }
  }
}
```
Subject Types: Add / Remove Requests

Email

POST /stream/example.stream.1234/add_subject HTTP/1.1
Host: api.example.com
Authorization: Bearer ZXhhbXBsZSBiZWFyZXIgdG9rZW4K
Accept: application/json
Content-Type: application/json
Content-Length: 163

{
  "risc_subject": {
    "type": "http://schemas.openid.net/secevent/risc/subject-type/email",
    "email": "user@example.com",
    "email_verified": false
  }
}
Subject Types: Add / Remove Requests

Phone

POST /stream/example.stream.1234/add_subject HTTP/1.1
Host: api.example.com
Authorization: Bearer ZXhhbXBsZSBiZWFyZXIgdG9rZW4K
Accept: application/json
Content-Type: application/json
Content-Length: 161

{
    "risc_subject": {
        "type": "http://schemas.openid.net/secevent/risc/subject-type/phone",
        "phone": "+1 206-555-1212",
        "phone_verified": true
    }
}
Subject Types: Add / Remove Requests

Issuer and Subject

POST /stream/example.stream.1234/add_subject HTTP/1.1
Host: api.example.com
Authorization: Bearer ZXhhbXBsZSBiZWFyZXIgdG9rZW4K
Accept: application/json
Content-Type: application/json
Content-Length: 176

{
    "risc_subject": {
        "type": "http://schemas.openid.net/secevent/risc/subject-type/iss-sub",
        "iss": "https://id.example.com/",
        "sub": "example.user.id.1234"
    }
}
Discovery

- Event Stream capabilities: event types, delivery method(s), etc.
- Configuration management API endpoint discovery
Discovery

- Event Stream capabilities: event types, delivery method(s), etc.
- Configuration management API endpoint discovery
- Who is authoritative for an identifier?
Subject Type-specific Discovery?

- OIDC defines discovery off issuer/subject, email address
- Mobile Connect provides discovery for mobile phone numbers
Questions?

• http://openid.net/wg/risc/