Identity Events

IETF95
Phil Hunt, Morteza Ansari, William Denniss
SCIM WG
April 2016

Events

- A proposal to define a common format for expressing events between publishers and subscribers
- Events describe something that has occurred
  - E.g.
    - Session Logout
    - Token Revocation
    - Account Take-over
    - Provisioning Events (SCIM)

BACKGROUND

Background

- IETF94 – Tokyo
  - Informal get together to discuss common standard for
    - OIDC Logout
    - OAuth Revocation
    - OIDF RISC Events
    - SCIM Provisioning Events
    - OIDF HEART
  - Could we use JWT/JOSE to express and transport events?

Events and State

- REST protocols transfer "state" from clients to service providers synchronously
- Events occur asynchronously and "inform" subscribers of a change in "state"
- Events ARE NOT commands
  - Statements of fact
  - Are historical

Identity and State

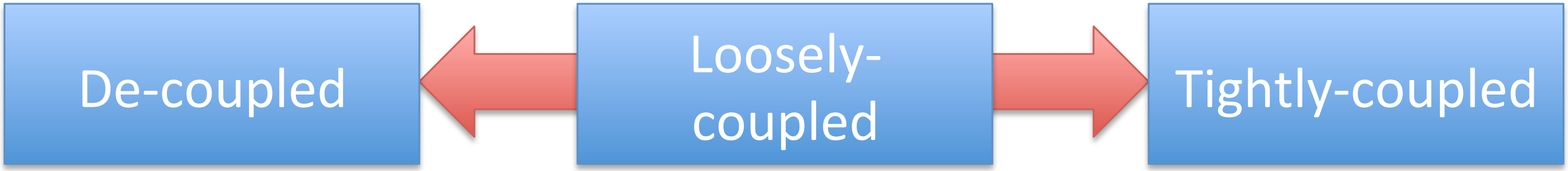
- What is unique about Identity?
- Even de-coupled systems are impacted
  - Claims
  - State of the person matters because we are talking about the same person
- Privacy requires systems to use minimum personal information
  - Each service should only have what it needs
  - Systems will always be-unequal
- Because security and privacy impacted
  - Co-ordination of events becomes necessary

State Relationship Cases

Implicitly coupled
e.g. Information about
the same person

Cross-domain linked
e.g. SCIM Provisioning

State is positively
controlled
e.g. Replication



De-coupled

Loosely-coupled

Tightly-coupled

Regardless of the protocol relationship,
personal data almost always connectable
For good and bad…

Why Not Commands?

- Often assumes tight coupling
  - Assumes the client is aware of the service state that it wants to update – not true!
  - There are still significant error conditions that may occur
- Domains reluctant to reveal too much about "state" of entities it holds (see privacy)
  - Co-ordinate yes. Tight control – almost never!
- Errors can reveal information
- **Statements of fact lead to simpler protocol**
  - Requires the subscriber to decide what is appropriate in their domain
  - let's look at an example…

State Transform Example

- Cumulus Cloud
  - Key service provider for Acme Enterprise
  - Nebulous has a relationship with Nimbus to offer CRM in the cloud
- Nimbus Cloud offers CRM as a service
  - Only knows about people authorized to use their service

State Transform Example

- Cumulus changes state of "Alice" by adding "CRM_User" to her "roles"
- Cumulus publishes change event to Nimbus
- Nimbus interprets event…
  - Is "Alice" known?
    - If not, Nimbus asks Nebulous for user "Alice" (e.g. SCIM GET)
    - Alice might already be known via a different relationship
  - Nimbus provisions user "Alice" if necessary
  - Nimbus adds user "Alice" to "CRM_Users" and provisiongs CRM service
- Nimbus has interpreted a single event and takes multiple actions to co-ordinate state
  - Nimbus has control of its own state

Event Characteristics

- Minimal data exchange
  - Privacy by design
- Subscriber independent action
  - subscriber decides action if any
  - no state error signalling
  - reverts to normal REST for secondary calls
- State remain independent and distinct
  - Security and accuracy is improved

CURRENT DRAFTS

ID Event Drafts

- draft-hunt-idevent-token
  - Identity Event Tokens based on JWT
- draft-hunt-idevent-distribution
  - Subscription Metadata
  - Delivery Method Registry
    - HTTP POST (Web Callback)
    - HTTP GET (Polling)
    - Web Push
- draft-hunt-idevent-scim
  - Id Event token profile for SCIM

The Identity Event

- A JWT token

- JWT attributes
  - jti, iat, nbf, sub, iss, aud
    - iss is publisher, aud is the subscription

- Event attributes
  - eventUris – the URIs of events contained in the message
    - Each URI may have a JSON object that has event specific information

Example SCIM Create Event

```
{
  "jti": "4d3559ec67504aaba65d40b0363faad8",
  "eventUris":[
    "urn:ietf:params:event:SCIM:create"
  ],
  "iat": 1458496404,
  "iss": "https://scim.example.com",
  "aud":[
   "https://scim.example.com/Feeds/98d52461fa5bbc879593b7754",
   "https://scim.example.com/Feeds/5d7604516b1d08641d7676ee7"
  ],
  "sub": "https://scim.example.com/Users/44f6142df96bd6ab61e
  "urn:ietf:params:event:SCIM:create":{
    "attributes":["id","name","userName","emails"],
    "values":{
      "emails":[
       {"type":"work","value":"jdoe@example.com"}
      ],
      "userName":"jdoe",
      "id":"44f6142df96bd6ab61e7521d9",
      "name":{
        "givenName":"John",
        "familyName":"Doe"
      }
}}}
```

The event type

SCIM Event Data

Example RISC Event

```
{
  "jti": "4d3559ec67504aaba65d40b0363faad8",
  "eventUris":[
    "urn:ietf:params:event:RISC:email_reassigned"
  ],
  "iat": 1458496404,
  "iss": "https://scim.example.com",
  "aud":[
      "https://risc.example.com/inbound/5d7604516b1d08641d7676ee7"
  ],
  "sub": "8385937503959",
  "urn:ietf:params:event:RISC:email_reassigned":{
    "email_hash":"39d4c90372a940205hdac835",
}}
```

The event type

RISC Event Data

Example Extended Event

```
{
  "jti": "3d0c3cf797584bd193bd0fb1bd4e7d30",
  "eventUris":[
    "urn:ietf:params:event:SCIM:password",
    "urn:ietf:params:event:extension:example.com:password"
  ],
  "iat": 1458496025,
  "iss": "https://scim.example.com",
  "aud":[
    "https://jhub.example.com/Feeds/98d52461fa5bbc879593b7754",
    "https://jhub.example.com/Feeds/5d7604516b1d08641d7676ee7"
  ],
  "sub":
    "https://scim.example.com/Users/44f6142df96bd6ab61e7521d9",
  "urn:ietf:params:event:SCIM:password":{
    "id":"44f6142df96bd6ab61e7521d9",
  },
  "urn:ietf:params:event:extension:example.com:password":{
     "resetAttempts":5
  }
}
```

SCIM Password Reset Event

An extension

Event Delivery Message

```
{
"eventTkns":[
  "eyJhbGciOiJub25lIn0
  .
  eyJwdWJsaXNoZXJVcmkiOiJodHRwczovL3NjaW0uZXhhbXBsZS5jb20iLCJmZWV
  kVXJpcyI6WyJodHRwczovL2podWIuZXhhbXBsZS5jb20vRmVlZHMvOThkNTI0Nj
  FmYTViYmM4Nzk1OTNiNzc1NCIsImh0dHBzOi8vamh1Yi5leGFtcGxlLmNvbS9GZ
  WVkcy81ZDc2MDQ1MTZiMWQwODY0MWQ3Njc2ZWU3Il0sInJlc291cmNlVXJpcyI6
  WyJodHRwczovL3NjaW0uZXhhbXBsZS5jb20vVXNlcnMvNDRmNjE0MmRmOTZiZDZ
  hYjYxZTc1MjFkOSJdLCJldmVudFR5cGVzIjpbIkNSRUFURSJdLCJhdHRyaWJ1dG
  VzIjpbImlkIiwibmFtZSIsInVzZXJOYW1lIiwicGFzc3dvcmQiLCJlbWFpbHMiX
  SwidmFsdWVzIjp7ImVtYWlscyI6W3sidHlwZSI6IndvcmsiLCJ2YWx1ZSI6Impk
  b2VAZXhhbXBsZS5jb20ifV0sInBhc3N3b3JkIjoibm90NHUybm8iLCJ1c2VyTmF
  tZSI6Impkb2UiLCJpZCI6IjQ0ZjYxNDJkZjk2YmQ2YWI2MWU3NTIxZDkiLCJuYW
  1lIjp7ImdpdmVuTmFtZSI6IkpvaG4iLCJmYW1pbHlOYW1lIjoiRG9lIn19fQ
  ."],
"eventCnt":1,
"eventPend":false
}
```

Discussion Items

- Distribution Schemes?
  - One-to-one, One-to-many, Many-to-Many*, P-2-P*
- Ability to lookup events by date or by etag
  - Issue: Impact on scale and ability to story history vs. audit
- Ability to detect missing events
  - E.g. each message gives the JTI of the last event delivered – issue: requires state
- Issued at
  - Time the event happened or JWT issued? Need to distinguish?
- Privacy Considerations
  - Even the resource identifier may be considered PII
  - Is this a privacy by design, privacy enhancing approach?