SCIM

IETF 83
“The how”

Trey Drake
trey.drake@unboundid.com

Topics

- Basis
- Schema and protocol drafts
- Security considerations

Basis

- Industry Consortium - Stake in the ground
- Widen the audience, change, and improve
- ~9 independent implementations
  - Open source and proprietary
  - 2nd Interop on Wednesday

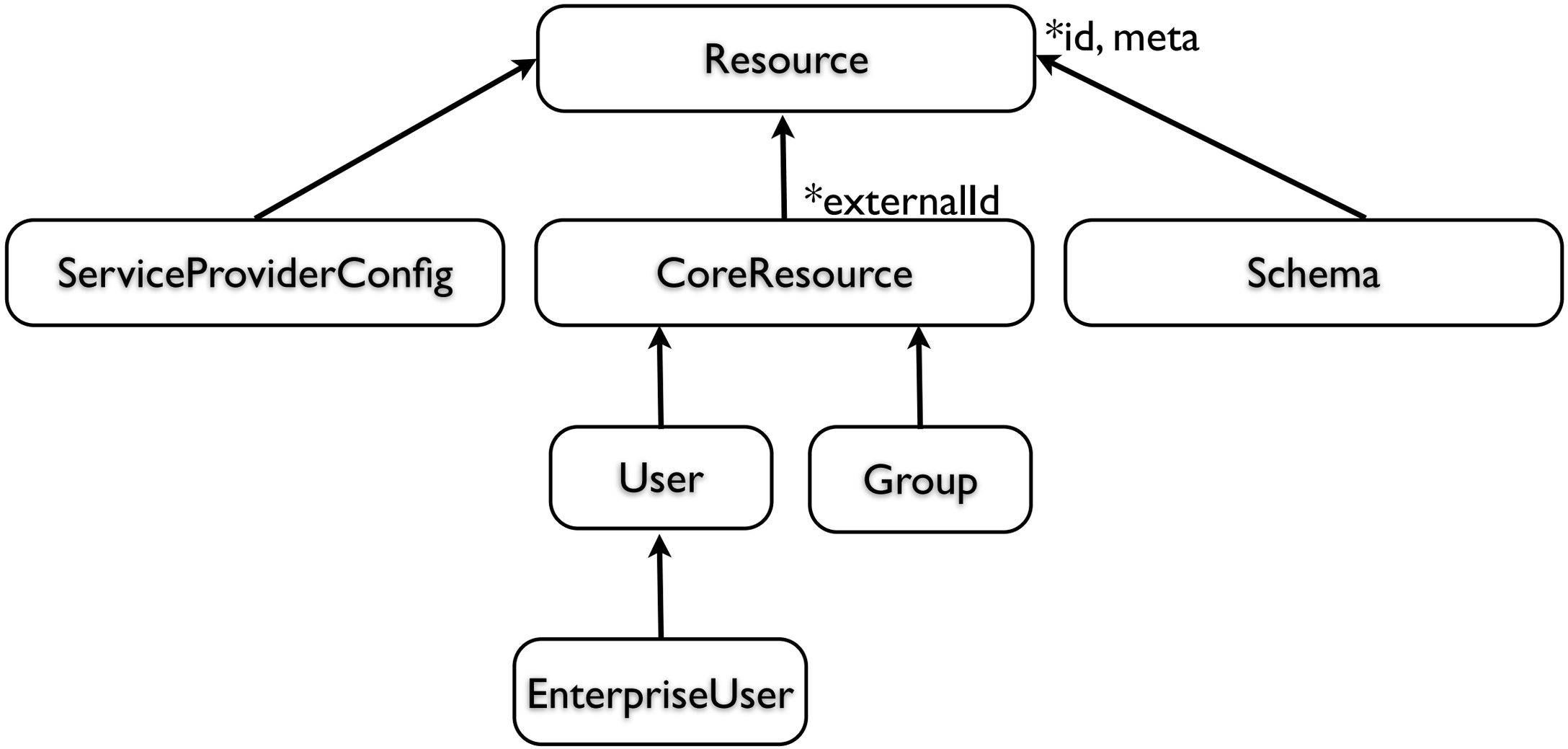
Specifications

- Core schema
- Protocol
- XML Schema
- Desire for additional mappings

Schema

- Rich Information Model
  - Xml and json data models
- Concrete artifacts (User and Group)
- Usage language (MTI and recommended)
- Extensibility: Inheritance and mix-in
- http://tools.ietf.org/html/draft-scim-core-schema-00.html

Model


Resource
*id, meta
*externalId
ServiceProviderConfig
CoreResource
Schema
User
Group
EnterpriseUser

Simple Structure

- A resource is:
  - Attribute container
  - Name spaced
- An attribute is:
  - Simple or Complex
  - Single or Multi-valued

Example: User

Required

Complex

Simple

Complex Multi-valued

```
{
  "schemas":["urn:scim:schemas:core:1.0"],
  "id":"2819c223-7f76-453a-919d-413861904646,
  "externalId":"bjensen",
  "meta":{
    "created":"2011-08-01T18:29:49.793Z",
    "lastModified":"2011-08-01T18:29:49.793Z",
    "location":"https://example.com/v1/Users/2819c223...",
    "version":"W\/\"f250dd84f0671c3\""
  },
  "name":{
    "formatted":"Ms. Barbara J Jensen III",
    "familyName":"Jensen",
    "givenName":"Barbara"
  },
  "userName":"bjensen",
  "phoneNumbers":[
    {
      "value":"555-555-8377",
      "type":"work"
    }
  ],
  "emails":[
    {
      "value":"bjensen@example.com",
      "type":"work"
    }
  ]
}
```

Example: Ext User

Declaration

Use

```
{
"schemas":["urn:scim:schemas:core:1.0",
           "urn:scim:schemas:extension:enterprise:1.0”],
"id":"2819c223-7f76-453a-919d-413861904646,
"externalId":"bjensen",
"userName":"bjensen",
"urn:scim:schemas:extension:enterprise:1.0": {
  "employeeNumber": "701984",
  "costCenter": "4130",
  "organization": "Universal Studios",
  "division": "Theme Park",
  "department": "Tour Operations",
  "manager": {
    "managerId": "26118915-6090-4610-87e4-49d8ca9f808d",
    "displayName": "John Smith"
  }
 }
}
```

Example: Group

Type (User|Group)

Optional & Read Only

```
{
  "schemas":["urn:scim:schemas:core:1.0"],
  "id":"2819c223-7f76-453a-919d-413861904646,
  "displayName": "Tour Guides",
  "members":[
    {
      "value":"2819c223-7f76-453a-919d-413861904646",
      "displayName":"Babs Jensen",
      "type":"User"
    },
    {
      "value":"2819c223-7f76-453a-919d-413861904646",
      "displayName":"Mandy Pepperidge",
      "type":"User"
    }
  ]
}
```

Protocol

- Synchronous, HTTP, ReST
- CRUD + Search* + Discovery + Bulk*
- Simple MTI, Complex optional
- Extensible*, Versioned
- “cURL” friendly
- http://tools.ietf.org/id/draft-scim-api-00.html

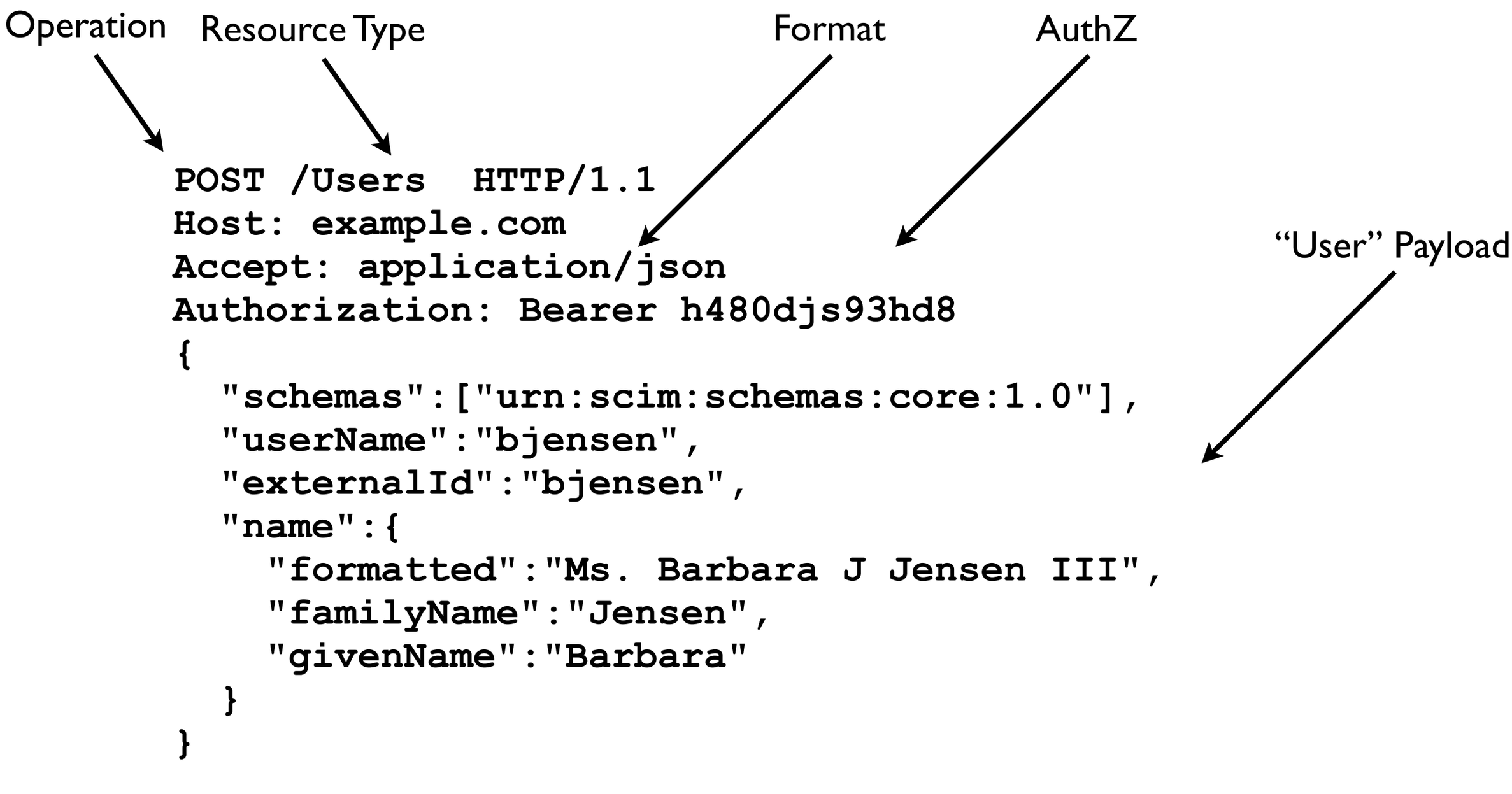
Operations

- Create = POST https://example.com/{v}/{resource}
- Read = GET https://example.com/{v}/{resource}/{id}
- Update = PUT https://example.com/{v}/{resource}/{id}
- Delete = DELETE https://example.com/{v}/{resource}/{id}
- *Update = PATCH https://example.com/{v}/{resource}/{id}
- *Search = https://example.com/{v}/{resource}?filter={attribute} {op} {value} & sortBy={attributeName} & sortOrder={ascending|descending}
- *Bulk

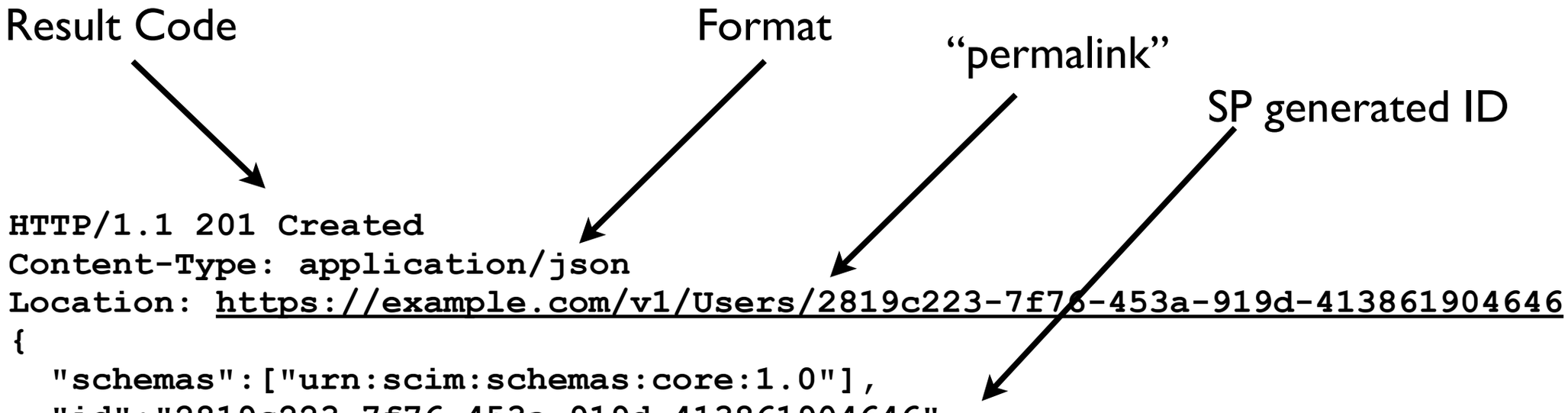
Discovery

- GET /Schemas
  - Introspect resources and attribute extensions
- GET /ServiceProviderConfig
  - Spec compliance, auth schemes, data models

Create Request

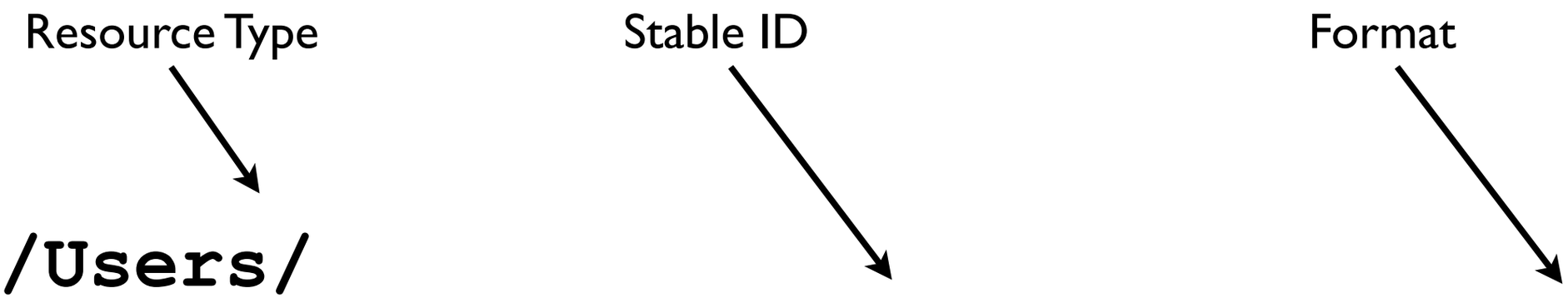


Create Response




```
HTTP/1.1 201 Created
Content-Type: application/json
Location: https://example.com/v1/Users/2819c223-7f76-453a-919d-413861904646
{
  "schemas":["urn:scim:schemas:core:1.0"],
  "id":"2819c223-7f76-453a-919d-413861904646",
  "externalId":"bjensen",
  "meta":{
    "created":"2011-08-01T21:32:44.882Z",
    "lastModified":"2011-08-01T21:32:44.882Z",
    "location":"https://example.com/v1/Users/2819c223-7f76-453a-919d-413861904646",
    "version":"W\/\"e180ee84f0671b1\""
  },
  "name":{
    "formatted":"Ms. Barbara J Jensen III",
    "familyName":"Jensen",
    "givenName":"Barbara"
  },
  "userName":"bjensen"
}
```

Get Request




```
GET /Users/
2819c223-7f76-453a-919d-413861904646.json
Host: example.com
Accept: application/json
Authorization: Bearer h480djs93hd8
```

Get Response

Result Code

Format

"permalink"

SP ID

```
HTTP/1.1 200 OK
Content-Type: application/json
Location: https://example.com/v1/Users/
2819c223-7f76-453a-919d-413861904646
{
  "schemas":["urn:scim:schemas:core:1.0"],
  "id":"2819c223-7f76-453a-919d-413861904646",
  "externalId":"bjensen",
  "meta":{
    "created":"2011-08-01T21:32:44.882Z",
    "lastModified":"2011-08-01T21:32:44.882Z",
    "location":"https://example.com/v1/Users/
2819c223-7f76-453a-919d-413861904646",
    "version":"W\/\"e180ee84f0671b1\""
  },
  "name":{ ...
```

Filter Request

https://example.com/{resource}?filter={attribute} {op} {value}

& sortBy={attributeName}

& sortOrder={ascending|descending}&attributes={attributes}

https://example.com/Users?filter=title pr and userType eq “Employee”

&sortBy=title

&sortOrder=ascending

&attributes=title,username

Filter Response

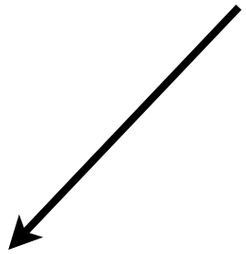
Pagination

Users

SP ID ever present

```
{
  "schemas":["urn:scim:schemas:core:1.0"],
  "totalResults":2,
  "Resources":[
    {
      "id":"c3a26dd3-27a0-4dec-a2ac-ce211e105f97",
      "title":"Assistant VP",
      "userName":"bjensen"
    },
    {
      "id":"a4a25dd3-17a0-4dac-a2ac-ce211e125f57",
      "title":"VP",
      "userName":"jsmith"
    }
  ]
}
```

Protocol Extensibility



- Version in URL
  - https://example.com/{version}/{resource}
- Follow Resty principles
  - additional URL args
  - additional URL endpoints

XML Schema

- XML XSD
  - Core
    - Resource, User, Group
    - Payload wrapper, Errors
- Enterprise extension

Security Considerations

- Protocol
- User PII, et al.

Security: Protocol

- TLS MTI
- Standard HTTP considerations apply
- Authentication is discoverable, bearer token recommended
- No a priori authorization scheme

Security: User

Password

AuthZ

```
{
  "id":"2819c223-7f76-453a-919d-413861904646,
  "externalId":"bjensen",
  "name":{
    "formatted":"Ms. Barbara J Jensen III",
    "familyName":"Jensen",
    "givenName":"Barbara"
  },
  "password":"maybe_plaintext",
  "roles":[
    {
      "value":"RA"
    }
  ],
  "groups":[
    {
      "value":"Student"
    }
  ],
  "entitlements":[
    {
      "value":"delete users",...
```

Hi/Low Fidelity Bindings

- LDAP
- SAML
- OpenIDConnect

Recap

- Looking for more eyeballs
- Suite of minimum viable specification(s)
- Facilitate implementation & integration
- Facilitate extension