Cloud Provisioning and Security Using OAuth2 and SCIM

Allan Foster
ForgeRock Inc

Session ID: IAM-107B
Session Classification: Intermediate

RSA CONFERENCE EUROPE 2012

Perimeter is swiss cheese

Essential services
“out there”
Where is your data?
Who has your data?

The cloud is part of our IT strategy!

- Users want services
- Build vs Buy
- Still need to protect our Data
- Work with the SaaS providers
- Standards vs one-off integrations

So? What are the challenges?

- Authentication
  - Who are our uses?
  - How do we ensure that?
- Data Access
  - Who needs what data?
  - What data do they need?
  - What will they do with it?

Authorization

Who can do what?

How do we ensure that?

Provisioning

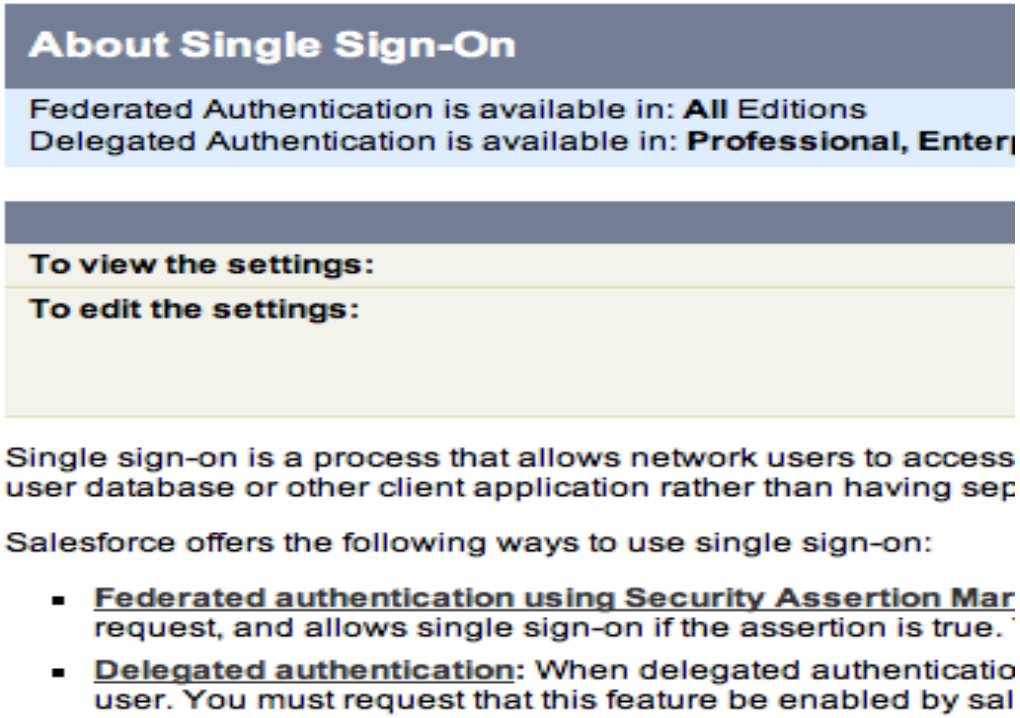
Are the users current?

Who says they are ours?

Lets look at possible solutions

Authentication

- Corporate single sign on
- Well understood
- SAML2
- OpenID-Connect



About Single Sign-On

Federated Authentication is available in: **All** Editions
Delegated Authentication is available in: **Professional, Enter**

To view the settings:

To edit the settings:

Single sign-on is a process that allows network users to access
user database or other client application rather than having sep

Salesforce offers the following ways to use single sign-on:

- **Federated authentication using Security Assertion Mar**
  request, and allows single sign-on if the assertion is true.
- **Delegated authentication**: When delegated authenticatio
  user. You must request that this feature be enabled by sal

Authorization

XACML?
Proprietary?

Role Based

Provisioning

- Enterprise owns the Identities
- Enterprise owns the Roles
- Provision cloud apps
  - users
  - roles
- Standardization is key

SCIM

- System for Cross Domain Identity Management
- Application Level
- REST protocol
  - Create
  - Update
  - Retrieve
- Identities and Roles

Why SCIM?

- Interoperable
- Adopted by multiple services
- Supported by enterprise identity solutions
- Wide support:
  - UnboundID
  - Google
  - Salesforce
  - Forgerock
  - Ping

What is SCIM?

- REST Provisioning protocol
- JSON and XML
- Authentication & Authorization
  - Out of Band
  - OAuth2 is recommended
- Standardized extensible schema

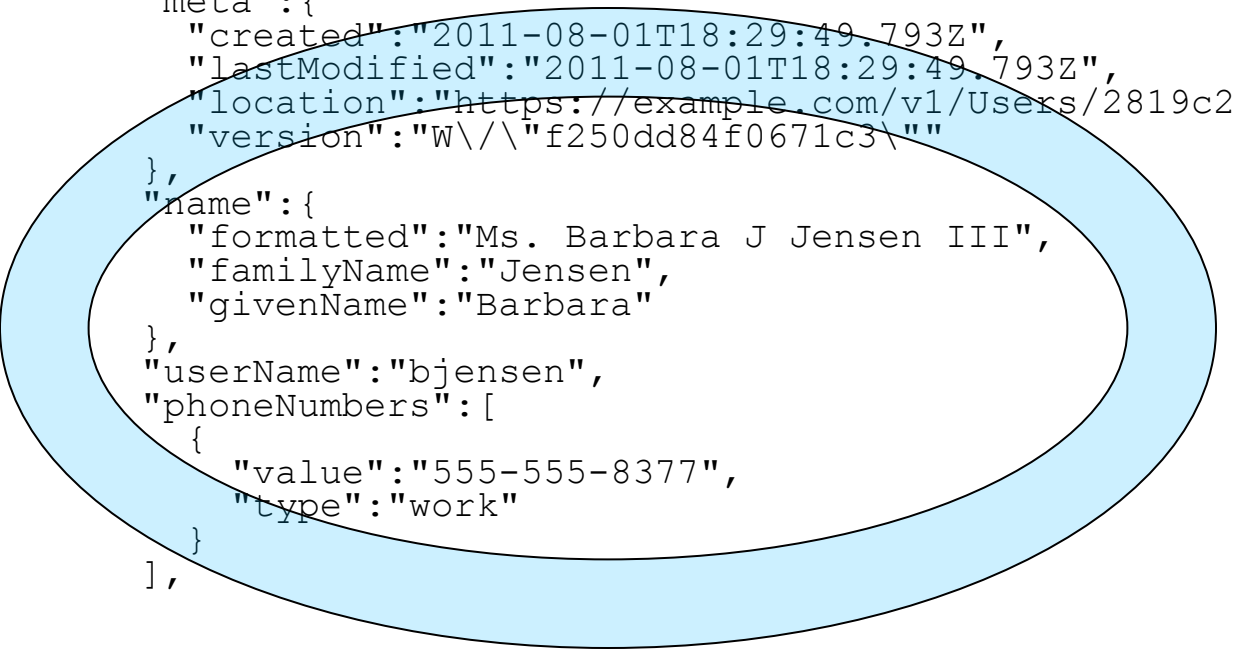
SCIM Retrieve Request

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

SCIM Retrieve Response

```
HTTP/1.1 200 OK
Content-Type: application/json
Location: https://example.com/v1/Users/2819c223-7f76-453a-919d
ETag: W/"f250dd84f0671c3"

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



Resource Access

- Users & Groups are resources
- SCIM uses OAuth2 for authorization
- OAuth2 is used to protect many resources

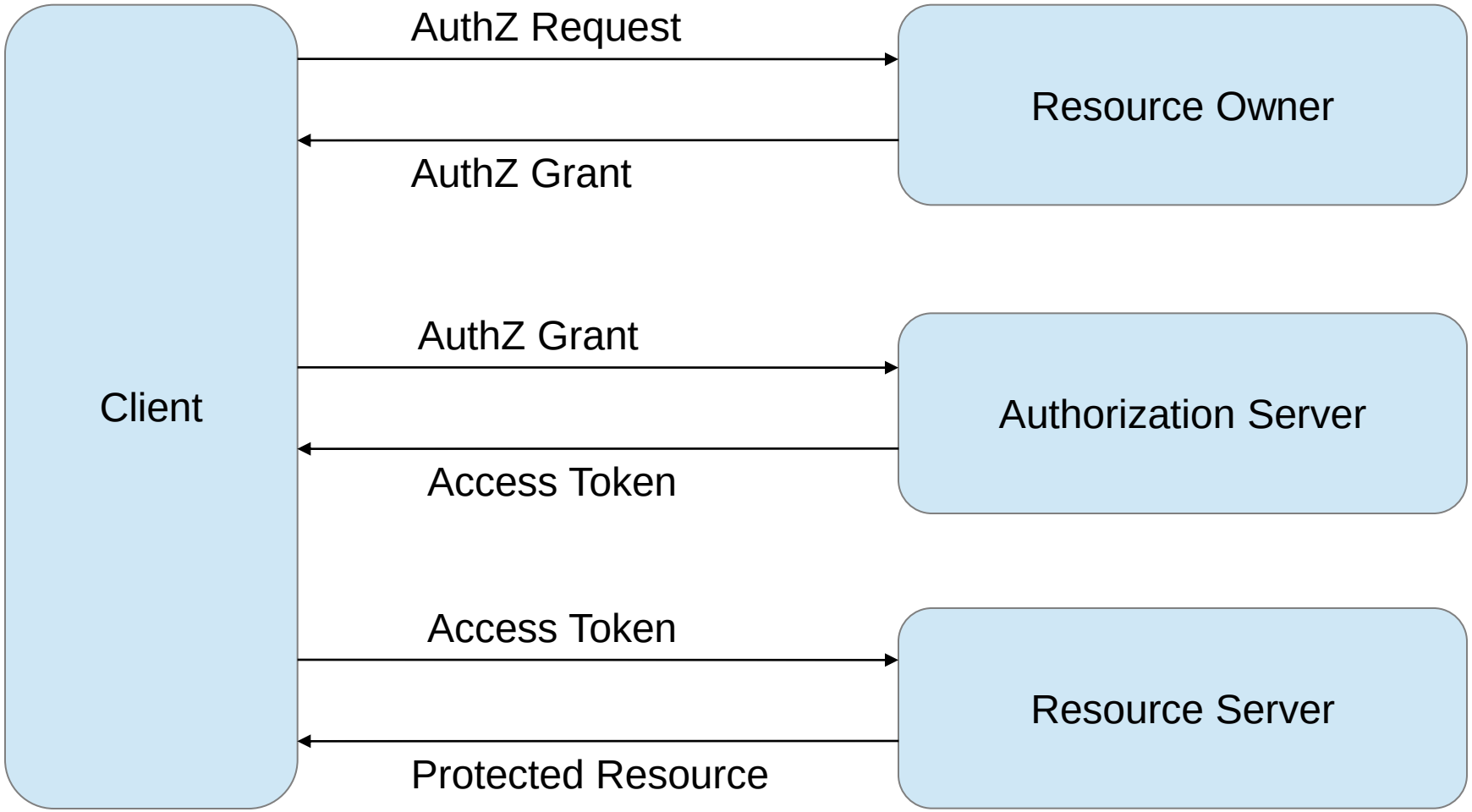
OAuth2 tokens

- Access Tokens
- Allows access to a specific resource
- Consent
  - User
  - Enterprise
- Refresh tokens

OAuth2 - The standard

- Standardized
- Simple to implement
- JWT – Java Web Token
- An access token scoped to the data you need.
- Data Owners Consent
  - User
  - Enterprise (Access Control)
- Token Lifetime from Seconds, to Years.

OAuth2 Flow


Client
AuthZ Request
AuthZ Grant
Resource Owner
AuthZ Grant
Access Token
Authorization Server
Access Token
Protected Resource
Resource Server

Using OAuth2

```
GET /resource HTTP/1.1
Host: server.example.com
Authorization: Bearer abcdef01234
```

```
{
  "access_token":"abcdef01234",
  "token_type":"Bearer",
  "expires_in":3600,
  "refresh_token":"ABCD01234"
}
```

Why OAuth2?

- Widespread adoption at providers
  - Google
  - Facebook
  - SalesForce
  - Force.com
- Allows secure access to user data in the cloud
- REST web services adopting OAuth2

OAuth2 in the Enterprise

- Becoming standard for REST protection
- Simple Interoperable security
- Enables secure external access to resources
- Widespread adoption

Integrate the cloud

- Cloud integrates into Enterprise
- Seamless Provisioning
- Corporate Approval process
- Coherent Access Management

Demo

Apply

- Realize that you can:
- Expose data,

- without exposing everything

- Enable the Cloud, and services

- without endangering the enterprise

- Allow access to what is needed

- without opening access to everything

Define the resources you need to enable.