OAuth2 SCIM JIT Client Registration -Schema Discussion-

Phil Hunt

August 1, 2013

IETF 87 SCIM WG

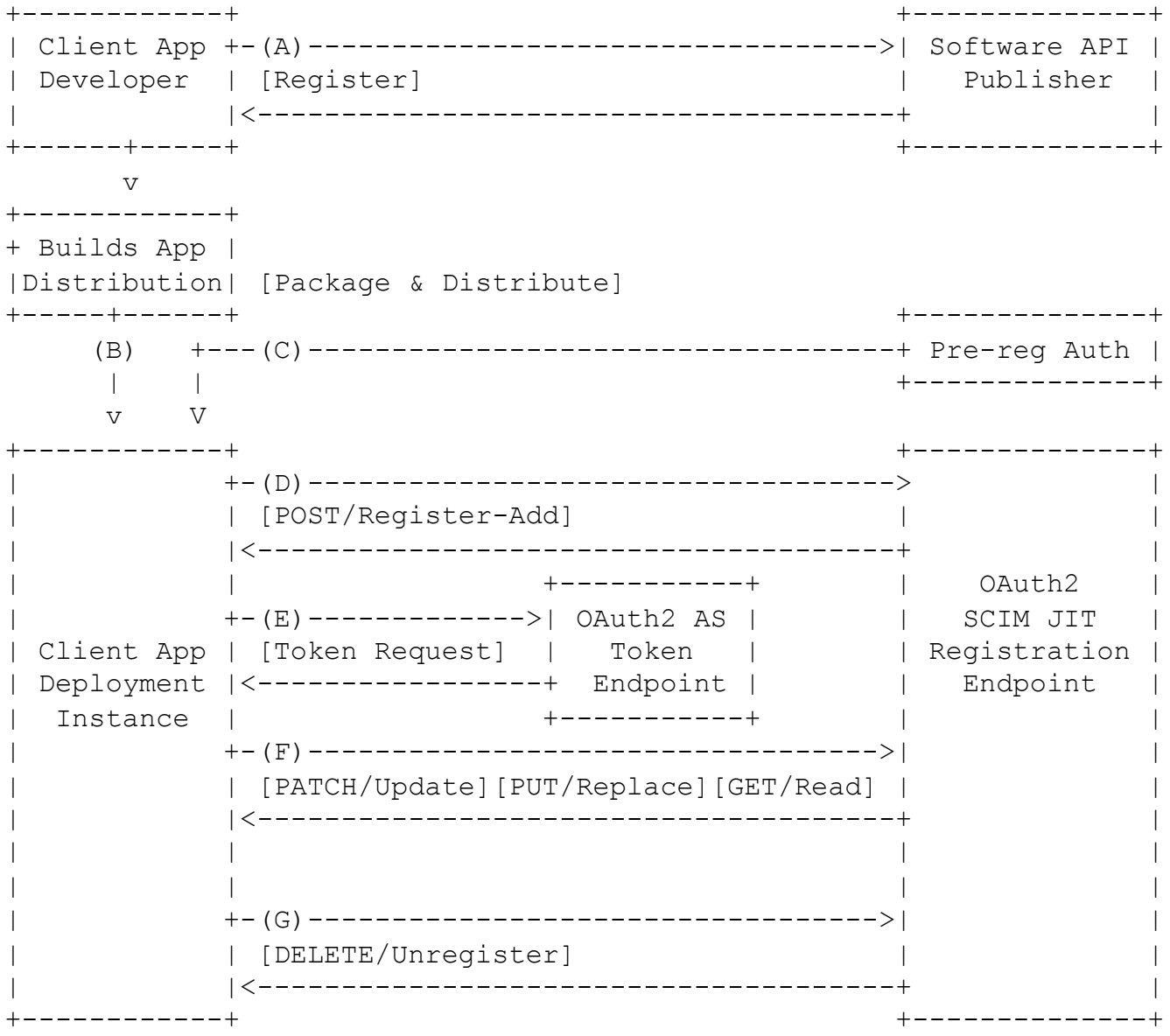
Agenda

- Quick Review of draft-hunt-oauth-scim-client-reg
  - Example of new approach to extending SCIM schema
- Discuss Localization of Data Issue

OAuth-SCIM-Client-Reg Intro

- This is a draft that permits OAuth 2 clients to register with a SCIM endpoint to obtain client credentials.
- Evolution of draft-ietf-oauth-dyn-reg
- Currently in the OAuth WG
- Defines a SCIM method for Clients to exchange client specific UI (client_name) and protocol attributes in exchange for client_id, and optional client authentication credential (client_secret aka password)

Basic Flow


Client App Developer
(A)
[Register]
Software API Publisher
Builds App Distribution
[Package & Distribute]
(B)
(C)
Pre-reg Auth
(D)
[POST/Register-Add]
(E)
[Token Request]
OAuth2 AS Token Endpoint
OAuth2 SCIM JIT Registration Endpoint
Client App Deployment Instance
(F)
[PATCH/Update][PUT/Replace][GET/Read]
(G)
[DELETE/Unregister]

Example Client


```
{
  "schemas":["urn:scim:schemas:core:1.0",
             "urn:scim:schemas:oauth:2.0:Client"],
  "id":"2060107e82-fbe3-42bd-b199-15df7081a8ae",
  "software_id":"5ed2dd14-3ef7-4655-a41d-b5bd4c5266cc",
  "software_version":"5.1.2.3.4",
  "client_name":"Example Social Client",
  "logo_uri":"https://client.example.org/logo.png",
  "jwks_uri":"https://client.example.org/my_public_keys.jwks",
  "token_endpoint_auth_method":"client_secret_post",
  "scope":"read write dolphin",
  "client_id":"2060107e82-fbe3-42bd-b199-15df7081a8ae",
  "client_secret":"Z7tk2XqLKo1CfE14374teR4V554e8JUS",
  "redirect_urls":[""https://client.example.org/callback",
    "https://client.example.org/callback2"],
  "targetEndpoint":"https://social.example.com/base"
}
```

LOCALIZATION

Localization Problem for OAuth Clients

- OAuth Clients inform registration endpoint about certain UI and protocol elements
  - client_name, client_uri, logo_uri, policy_uri, tos_uri,
  - potentially: targetEndpoint, scope, redirect_uri?
- Two types of clients:
  - Personal/Native: clients used by one user (cell)
    - Client registers using client's selected language
    - Very large numbers of clients
  - Web Clients: client shared by many users
    - localization not 1 or 2 langs but 8, 30, or more!
    - Small to medium numbers of clients

3 Ways To Represent

- Attribute name masking
- Multi-value Style
- Extended Value
- others…?

Attribute Name Masking

```
{
 ...
      "client_name": "My Client",
      "client_name#en":"My Client",
      "client_name#ja-Jpan-JP": "\u30AF\u30E9\u30A4\u30A2\u30F3\u30C8\u540D"
 ...
}
```

Multi-Value Style

```
{
  …

      "client_name":[
        {
         "value":"My Client",
         "lang":"en",
         "primary":"TRUE"
        }
        {
          "value":"\u30AF\u30E9\u30A4\u30A2\u30F3\u30C8\u540D",
          "lang":"ja-Jpan-JP"
        }
      ]
 …
}
```

Extend Value

```
{
 …
  "client_name":
  {
    "en-us" : "The Magical World of Bob",
    "fr" : "Le Monde Magique de Bob"
  }
 …
}
```

WG QUESTIONS

Questions

- Since many SCIM sites may be OAuth protected, does WG have an interest in this spec other than as a use case?
  - Would we want to add this to our charter?
- Does the WG want to address attribute localization?
  - Is there a particular format preferred?

- General Discussion?