IETF 83
SCIM
Simple Cloud Identity Management
“The what”

Morteza Ansari
morteza.ansari@cisco.com
What is the problem?

• “How do I provision a user account for service X?”
• “How do I deprovision a user account from service X?”
• “How do I update an existing account for service X?”
• “How do I keep my organization’s users in sync with service X?”
• “How do I manage groups?”
What is the problem?
What is a user?

dn: cn=HomeJSimpson,o=domain-name
cn: HomerJSimpson
objectClass: top
objectClass: person
objectClass: organizationalPerson
objectClass: inetOrgPerson
mail: HJSimpson@burnsco.com
givenname: Homer
sn: Simpson
postalAddress: 742 Evergreen Terrace
l: Springfield
st: Kentsouri
postalCode: 01234
telephoneNumber: (888) 555-1111
jpegPhoto: <http://www.simpsons.com/homer.jpg>

Homer J. Simpson
Springfield Nuclear Plant
Safety Inspector
(888) 555-1111 Work
(123) 666-1111 Home
HJSimpson@burnsco.com
742 Evergreen Terrace
Springfield, Kentsouri 01234
http://www.simpsons.com
How do we do it today?

- Manual (UI)
- Bulk (CSV upload)
- API
- Connector
- SAML Just-In-Time provisioning
Solutions – Challenges

• Manual
  – Does not scale (n users * m services)
  – Security concerns with stale identities
  – Error prone

• Bulk
  – Security concerns with stale identities
  – Inconsistent support among vendors
  – Schema mapping
Solutions – Challenges

• API
  – Vendor specific
  – Schema mapping

• Connector
  – Vendor specific
  – One connector per vendor
  – Sparse backends support
Solutions – Challenges

• **SAML JIT**
  – Works great when pre-provisioning is not required
  – Works for create/update – no deprovisioning
  – Does not work for groups
  – Schema mapping
Why not ....?

• Existing federations?
  – Works in conjunction with federations
    • Pre-provisioning done via SCIM
    • Authentication done via SAML, OpenID, ...

• OAuth?
  – User being provisioned is not on the call path
    • Org to org NOT user to service
  – OAuth is used for protocol authN/Z
Why not ....?

- **LDAP?**
  - Architectural fit for services
    - LB, tooling, rate limiting, measurement, ...
    - Encoding, connections, ...
    - Additional flexibility/capability is harder to scale and secure
      - How to bolt OAuth to LDAP?
  - Flat data model
  - Bulk operations not supported
  - Security concerns – real or perceived
Why not ....?

- **SPML**
  - OASIS Standard (1.0 – 2003; 2.0 – 2006)
  - No core Schema
  - Complex – real or perceived
  - Some traction within enterprises, none for cloud services
  - Limited support - few tools/products
We need to solve

• **Simple!**
• CRUD operations for
  – Users
  – Groups
  – Possibly other identity related objects (e.g. Devices)
• Bulk operations
• Extension semantics (schema & protocol)
• AuthN/AuthZ for protocol
• Security review
• Protocol Binding/mapping for SAML, LDAP
We don’t need to solve

• Defining new authentication/authorization frameworks or mechanisms
• Authorization model for SCIM endpoints
• Managing non-identity related resources