Identity

…in the age of the Cloud

@mmaha

Agenda

- Identity & Access Management **Concepts**
- On-Premises to **Cloud** trend
- **Standards**
  - Typical **Flow**
- Challenges, Future
- Questions

IAM Concepts

- **Authentication**
  - Passwords (aka Shared Secret) and Password Policy
  - Need for Multi-Factor AuthN
    - 1. What you know, 2. What you have, 3. What you are (Bio-Metric), Where?
- **Authorization** - Who can do what?
  - Roles -> Critical link to Provisioning
- Employee/Customer/Partner/Supplier/User **Life Cycle**
  - Provisioning, De-provisioning (Joins, Moves, Leaves)

Services beyond the Firewall

- **Proliferation** of Apps, Services — **More identities**
  - Rising use of Google Apps, Salesforce, Office 365, Workday, Concur etc.
  - BYOD - Phones, Phablets and Tablets
- Any Application with Any Device from Any Place
  - “Identity as a Firewall”
- VPNs have limited utility

Challenges

- Proliferation of identities — Need to login multiple times
  - Multiple MFA options, if & when available
  - Deactivating or De-provisioning
- How to connect your customers to services you use on the cloud?
  - As an example, Help Desk software (Zendesk) in the cloud
- Reports
  - Who has access to what? Access reports? When?
- B2B - Connect your cloud service provider to another

On-Premises to Cloud

- On-Premises model - “Web Agents” / Proxy
- Cloud model - Federation server in the cloud; Benefits of a multi-tenant model
- On-Premises Provisioning —> Cloud based Provisioning
- On-Premises Identity Repository (LDAP) —> Cloud based Directory

Evolution of Federation

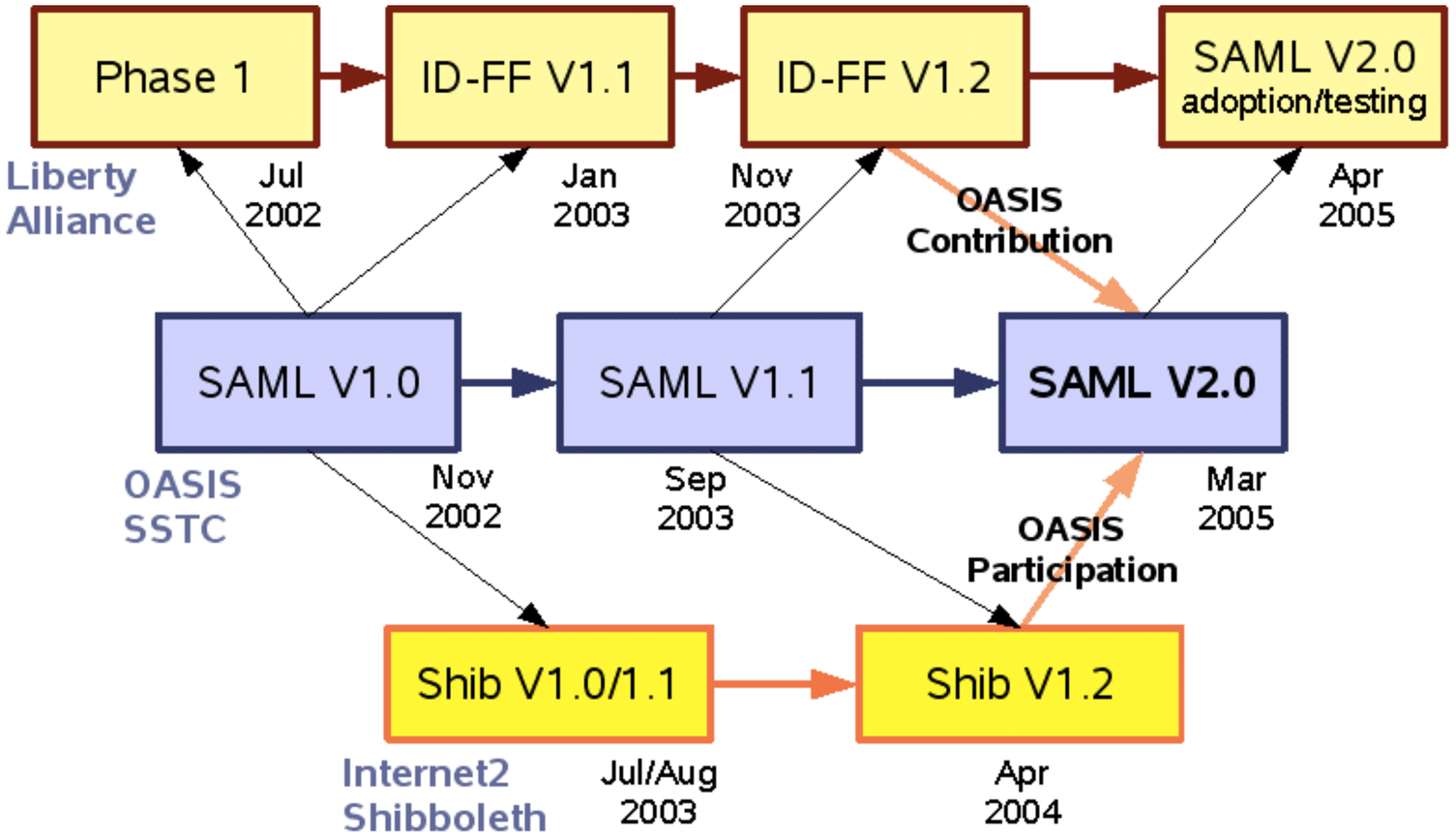
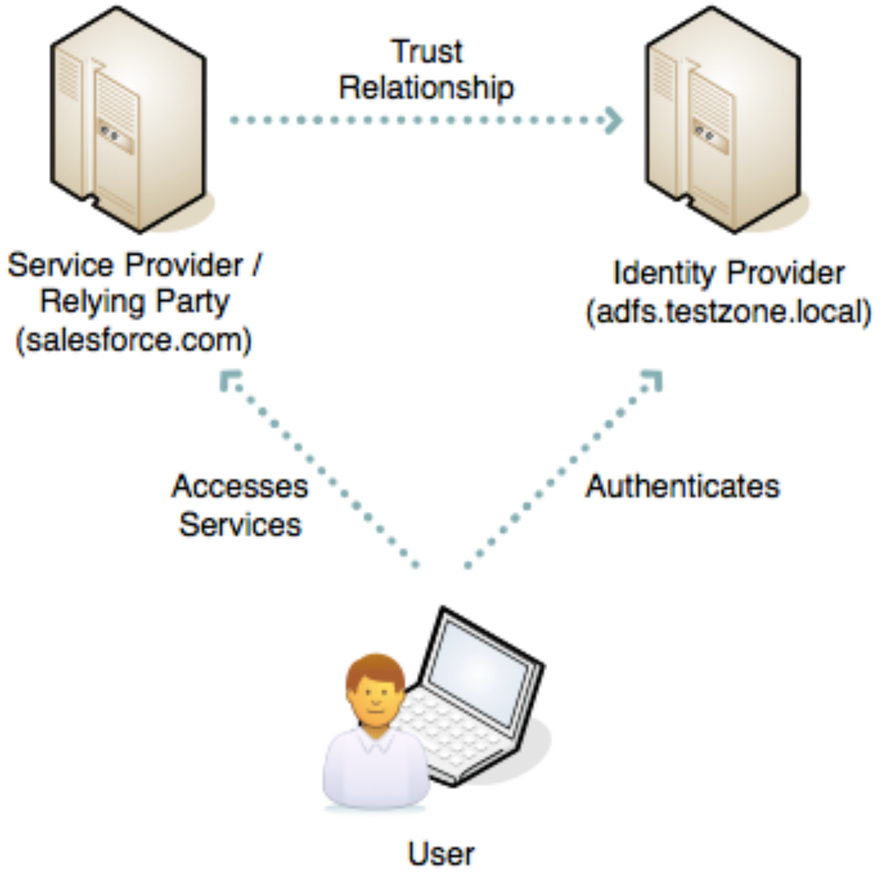


Image: http://www.xmlgrrl.com/publications/177-maler-fed-id.html

AuthN Standards

- Security Assertion Markup Language (SAML)
- OAuth 2.0
- WS-Federation (Microsoft)
- OpenID Connect - Upcoming!
- HTTP/S POST (Browser based plugin; Not a standard!)

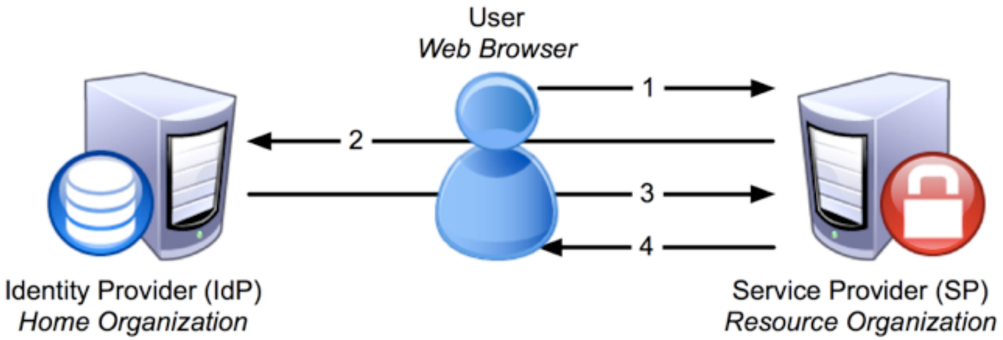
Federation Triangle



Bridges Multiple
Security Domains

Image: https://developer.salesforce.com/page/Single_Sign-On_with_Force.com_and_Microsoft_Active_Directory_Federation_Services

Typical AuthN Flow



1. The SP detects the user **attempting to access** restricted content within the resource.

2. The SP generates an **authentication request**, then sends the request, and the user, to the user's IdP.

3. The **IdP authenticates the user**, then sends the authentication response, and the user, back to the SP.

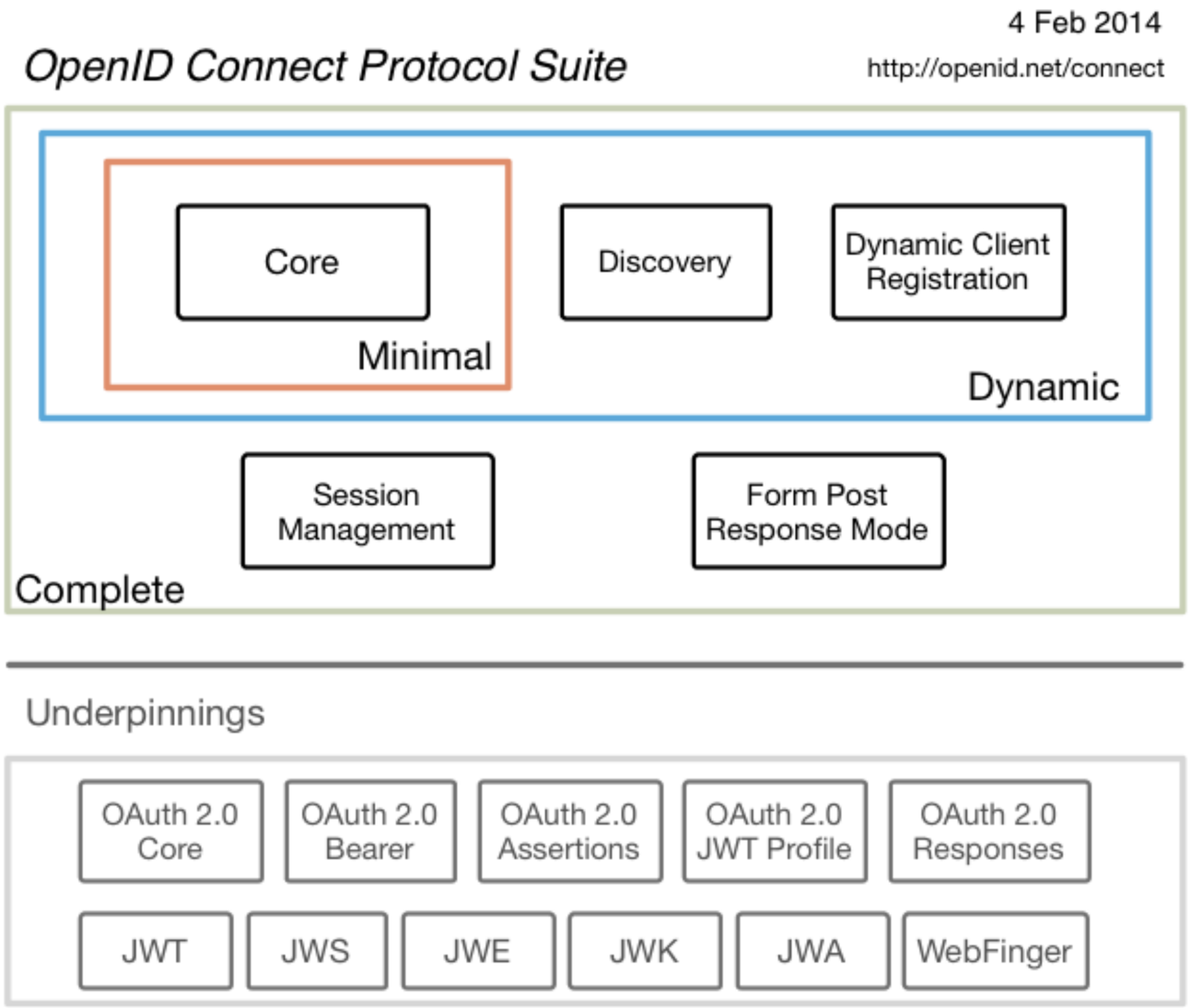
4. The **SP verifies the IdP's response** and sends the request through to the resource which **returns the originally requested content**.

Image: https://wiki.shibboleth.net/confluence/display/SHIB2/NewUnderstandingShibboleth

OAuth 2.0

- **REST** based AuthZ framework primarily for API
- No Authentication - Primarily delegation of capabilities
  - No passwords! Based on **tokens**
  - Restrict scope; Tokens are revokable
- OAuth is comparable to a **valet** key!

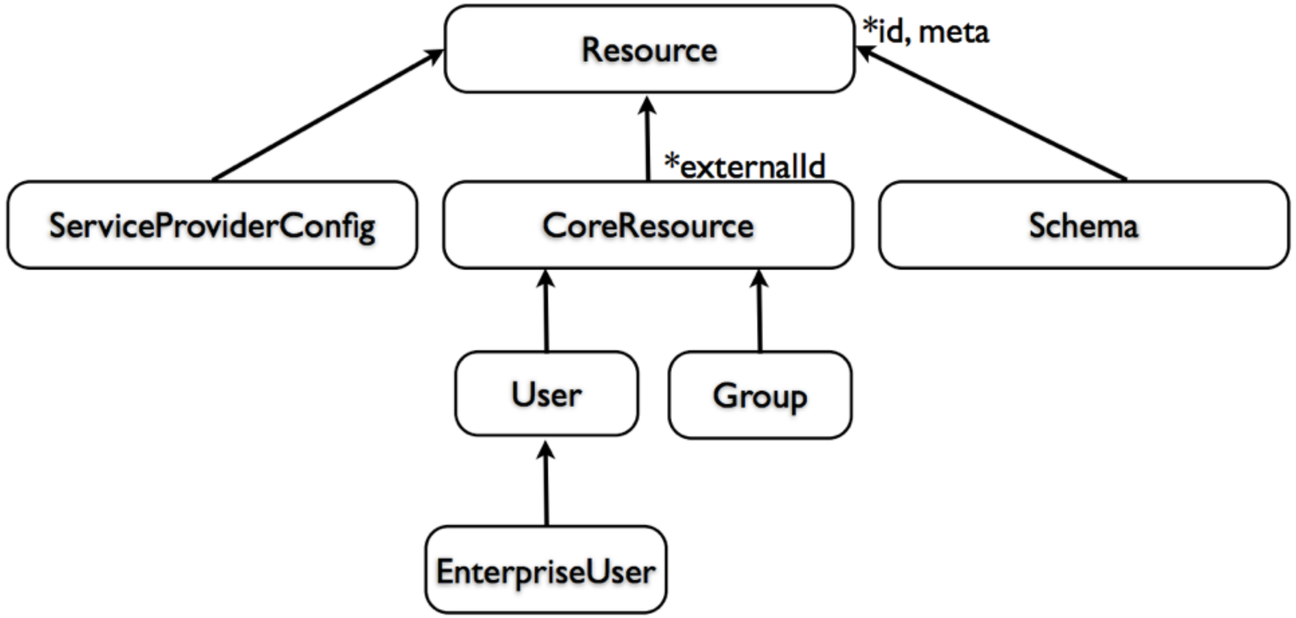
OpenID Connect



- OpenID Connect is a simple identity layer on top of OAuth
  - **Core** The core spec achieves authentication and authorization
  - **Discovery** Enables the client to find out the relevant endpoint for the user.
  - **Dynamic Registration** Enables the client to register to the server dynamically.

Provisioning Standards

- Proprietary -> SPML -> SCIM (Simple Cloud Identity Management)
  - Inbound identities (and attributes) - From HR System, AD, CSV
  - Outbound identities (and attributes) - To any system with an API or SCIM support



SCIM

Challenges

- Many…
- When **People** cannot remember the password… Social Engineering.
- When the **Process** for identity proofing is weak; Trusted source info is unreliable
- **Technology**: Backwards compatibility, Desktop/Browsers, Network…

In the near future…

- Intersection between "Consumer" identity and "Enterprise" identity — Social Auth
- Native Mobile SSO Standard - Building on OpenID Connect

Summary & Questions?

- Identities are **exploding** in the cloud
- Enterprises need to manage this - **Identity Layer**
- Cloud based **Identity Provider**(s) come in handy here…
- Mature and upcoming standards enable this: **SAML**, WS-Fed, OAuth, **OpenID Connect** and **SCIM**

LinkedIn www.linkedin.com/in/madhumahadevan

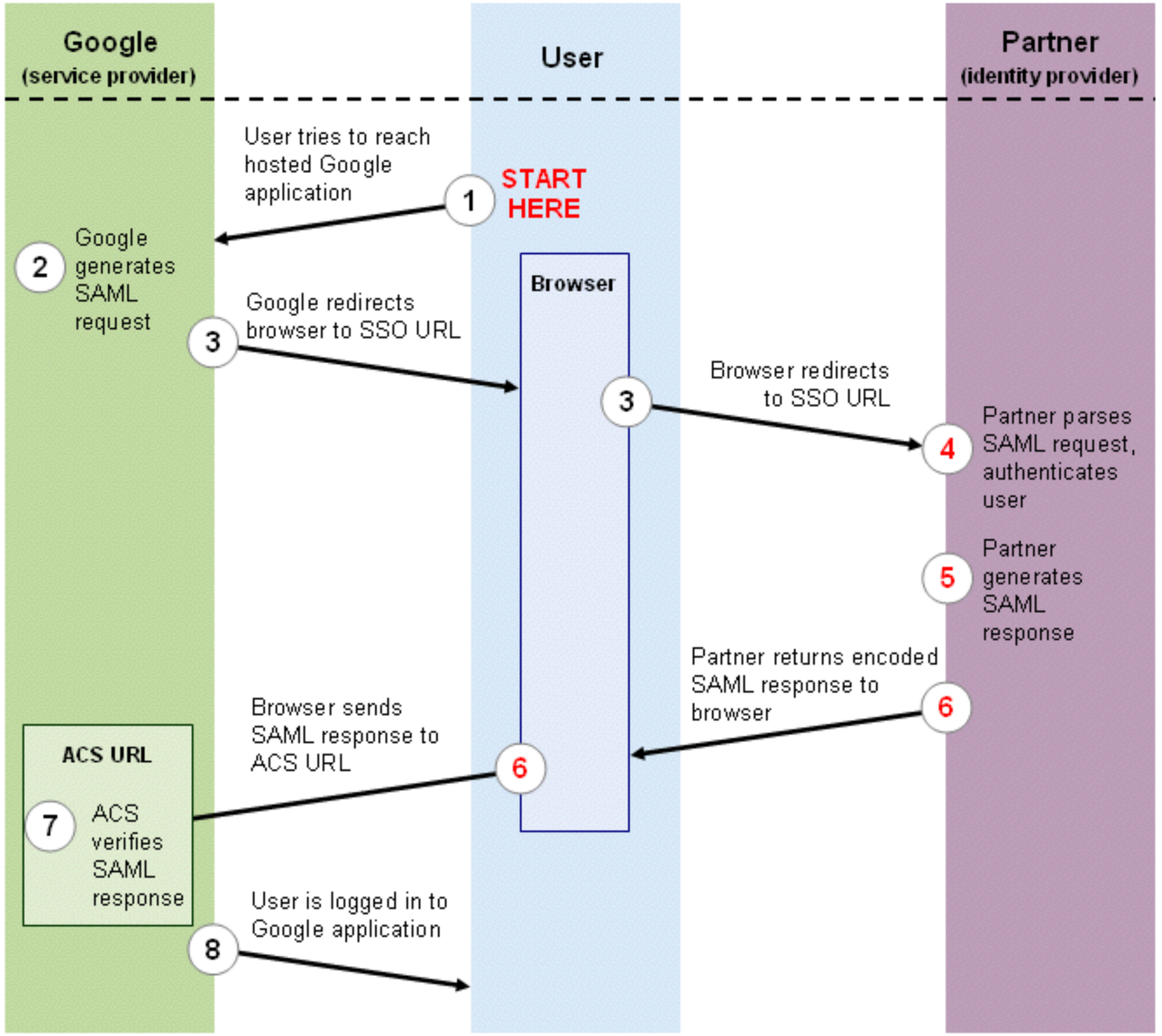
@mmaha

References

- https://www.oasis-open.org/committees/download.php/20520/SAMLV2.0-basics-Oct2006.pdf

- http://nat.sakimura.org/2011/05/15/dummys-guide-for-the-difference-between-oauth-authentication-and-openid/


APPS
DIRECTORY
ACCESS
COLLABORATION
CUSTOMER SERVICE
MARKETING
AUTHENTICATION
POLICIES
SALES
PERMISSIONS
ID
BI
DEVICES
LOCATION
GROUPS
PRODUCTIVITY
HR


Google
(service provider)
User
Partner
(identity provider)
User tries to reach hosted Google application
1
START HERE
2
Google generates SAML request
Google redirects browser to SSO URL
3
Browser
3
Browser redirects to SSO URL
4
Partner parses SAML request, authenticates user
5
Partner generates SAML response
Partner returns encoded SAML response to browser
6
Browser sends SAML response to ACS URL
6
ACS URL
7
ACS verifies SAML response
User is logged in to Google application
8