CERN’s Experience with Federated Single Sign-On

Federated identity management workshop

June 9-10, 2011

IT-OIS

Definitions

IAA: Identity, Authentication, Authorization

	Answer the questions	Attributes
Identity	“Who are you?”	Public assertion
Authentication	“Ok, how can you prove it?”	Secret response
Authorization	“What can I do?”	Token or ticket Access control

- **Identity:**
  - **Human Identity: HR record**
  - **Computer Identity: Account**
- **Authentication:**
  - **Single Sign-On, Kerberos, LDAP, SOAP, Active Directory**
- **Authorization:**
  - **E-Groups to maintain access control lists**

CERN SSO System

- **Based on Federation Standards**
- **Identity Provider: where user authenticate**
  - Using Microsoft ADFS implementation
  - Easy Active Directory integration
  - Easy Certificate and Kerberos authentication
- **Service Provider: the Application requiring authentication**
  - Any Federation compatible system
  - Shibboleth, ADFS, Oracle, etc.

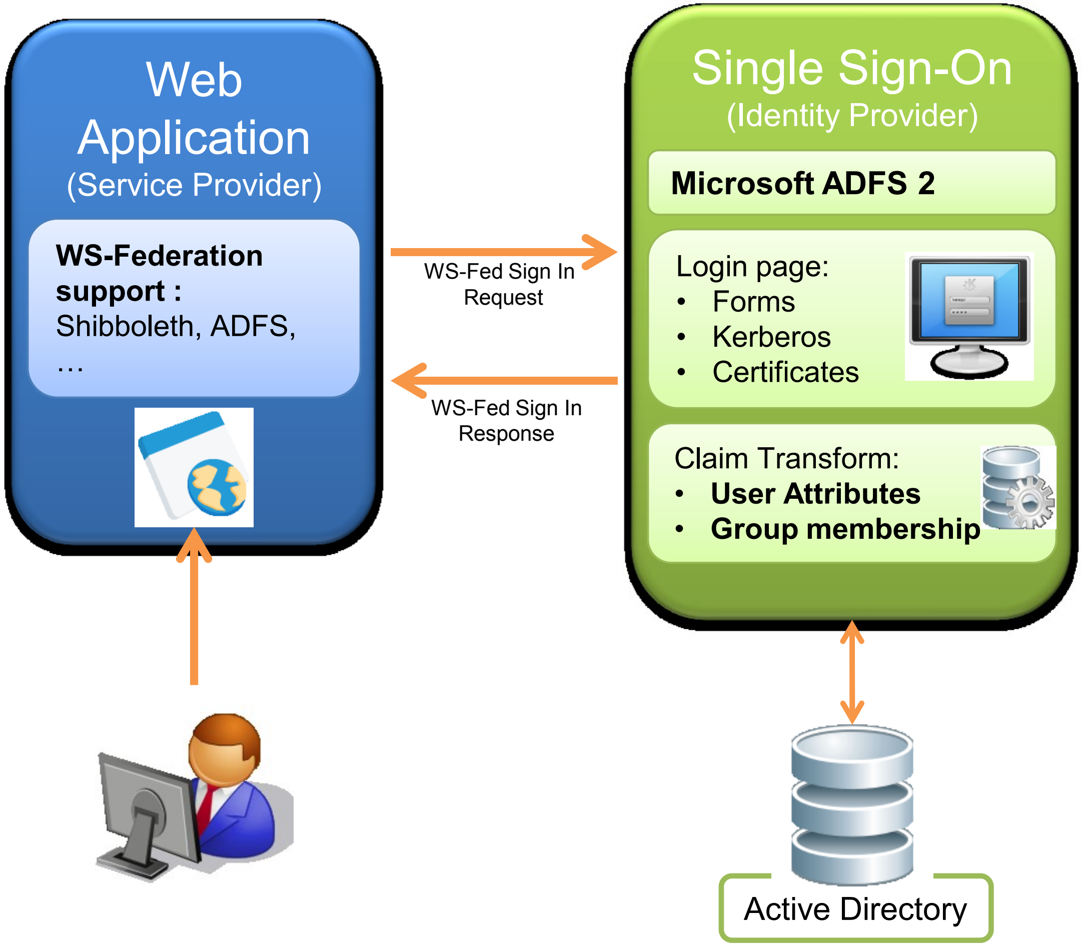
SSO Authentication methods

Authentication and Authorization

- **Different authentication methods**
  - Classic Forms (login and password)
  - Certificates (Grid Certificates, smartcards)
  - Windows Integrated and Kerberos
- **Standalone Authentication**
  - Not linked to the calling Web Application
  - A Linux/Apache application can use Windows Integrated authentication
  - All user information is available to the Application: name, email, building, etc…
- **Groups and roles: Authorization**
  - Groups membership information is sent to the calling Web Application
  - Roles system based on the central group management (E-Groups)

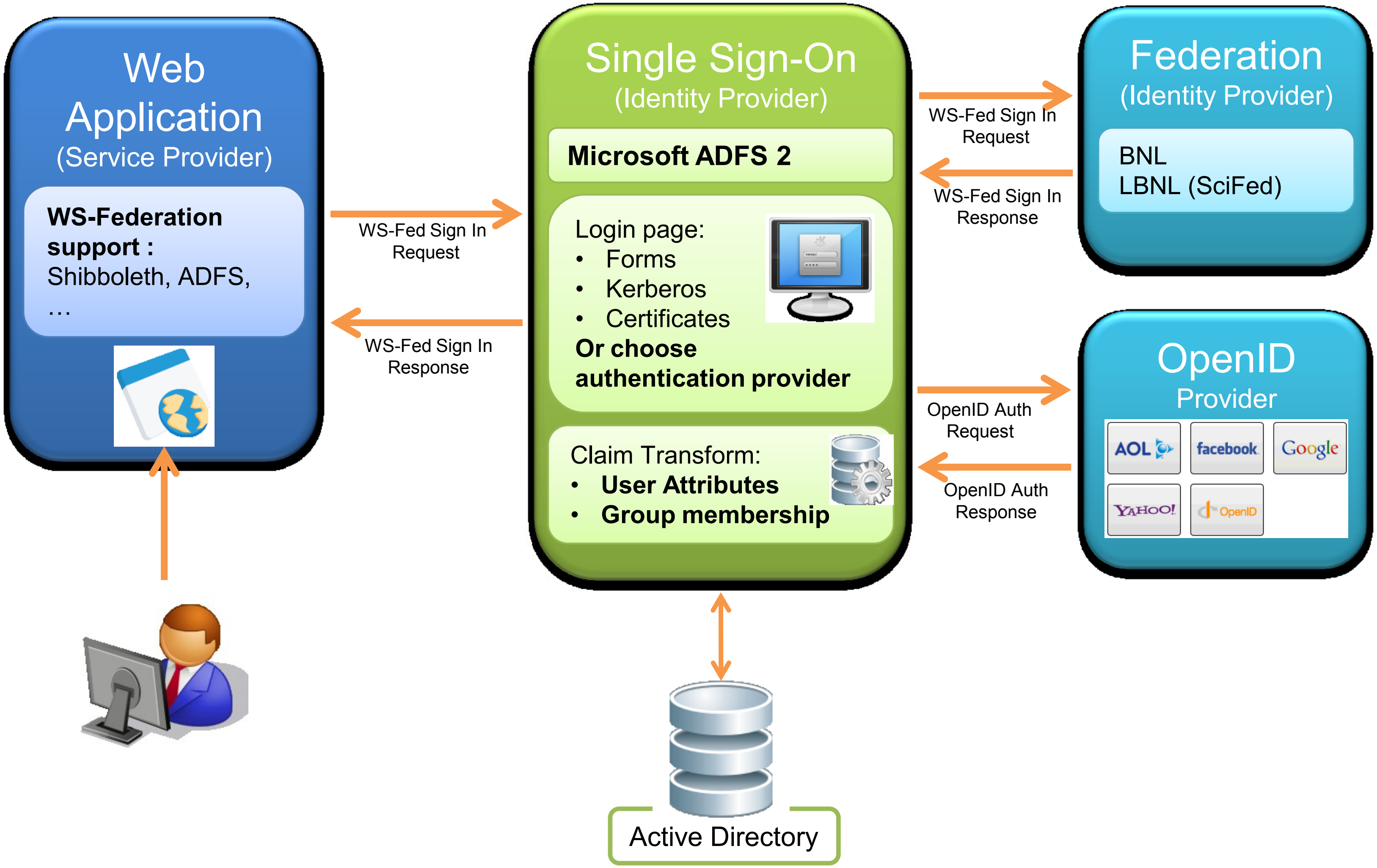
CERN SSO System

Basic Setup



CERN SSO System

Extending Possibilities



Web Application (Service Provider)

WS-Federation support : Shibboleth, ADFS, …

WS-Fed Sign In Request

WS-Fed Sign In Response

Single Sign-On (Identity Provider)

Microsoft ADFS 2

Login page:

- Forms
- Kerberos
- Certificates

Or choose authentication provider

Claim Transform:

- **User Attributes**
- **Group membership**

WS-Fed Sign In Request

WS-Fed Sign In Response

Federation (Identity Provider)

BNL
LBNL (SciFed)

OpenID Auth Request

OpenID Auth Response

OpenID Provider

AOL, facebook, Google, YAHOO!, OpenID

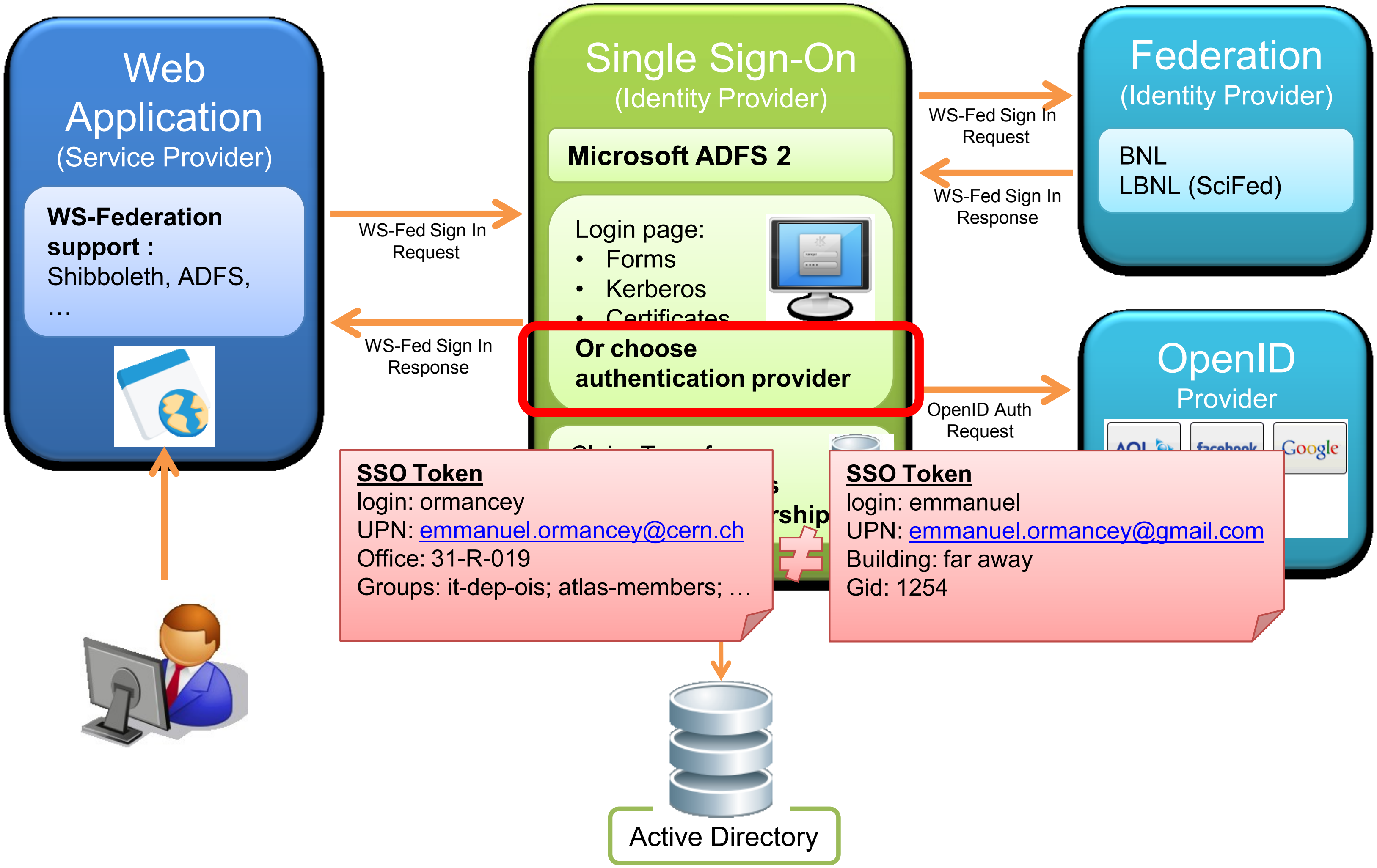
Active Directory

Ongoing Work

- **Federation testing with:**
  - BNL: allow BNL users to access ATLAS Twiki with their BNL credentials
  - LBNL (SciFed)
- **OpenID: allow OpenID authentication for ‘Lightweight accounts’**
  - Password policy to be defined
- **YubiKey: introduce 2FA alternatives**
- **Any other**

Claims/Attributes problem

Their source is unmanaged/untrusted



Web Application (Service Provider)

WS-Federation support : Shibboleth, ADFS, …

WS-Fed Sign In Request

WS-Fed Sign In Response

Single Sign-On (Identity Provider)

Microsoft ADFS 2

Login page:
- Forms
- Kerberos
- Certificates

Or choose authentication provider

WS-Fed Sign In Request

WS-Fed Sign In Response

Federation (Identity Provider)

BNL
LBNL (SciFed)

OpenID Auth Request

OpenID Provider

SSO Token
login: ormancey
UPN: emmanuel.ormancey@cern.ch
Office: 31-R-019
Groups: it-dep-ois; atlas-members; …

SSO Token
login: emmanuel
UPN: emmanuel.ormancey@gmail.com
Building: far away
Gid: 1254

Active Directory

Claims/attributes problem

Manage Authorizations: several ways

- **Use claims/attributes provided by the Authentication provider**
  - Need to define claim/attributes rules
  - Will lead to a wide range of different claims/attributes to manage
  - Each Application (service provider) will have to deal with different claims/attributes to manage authorizations
- **Map alternate external credentials to local account**
  - Map to local group memberships and attributes
  - local registration required
- **Use a common identity & groups database**
  - Shared and maintained by the community

A Unique HEP database

Proposal

- **Contains all user entries participating to the community**
  - Mappings to:
    - Grid Certificates: handle the VO certificate mappings
    - OpenID and other alternative auth systems
    - Federation identities
- **Contains Group memberships**
  - A central E-Group system for all organizations
- **Can be used to replace VOMS Registration**
  - Export to populate local VOMS mapping files
- **Use standards**
  - LDAP seems the easiest to interface

Conclusion

Authentication is fine, Authorization is a problem

- **Authentication**
  - Federation, OpenID, etc.: any can be used.
  - Trust establishment can follow GridPMA/IGTF initiative.
- **Authorization: Several schemes are available**
  - Use claims/attributes of each provider
    - Very difficult to manage. Require special mappings for each providers, each claimset being different.
    - Agree on a common claimset ?
  - Map incoming identity to a local identity
    - And reuse local attributes
    - Means duplicate all HEP accounts into all HEP systems
  - Use a common identity and authorization database
    - HEP wide group and authorization system
    - HEP wide VOMS registration system
    - Needs live access or local replication

Questions?

Contact: emmanuel.ormancey@cern.ch