Securing Enterprise: Employability and HR

Federation and XACML as Security and Access Control Layer

Sampo Kellomäki (sampo@symlabs.com)

OASIS Open Standards Forum
Ditton Manor, October 1, 2008

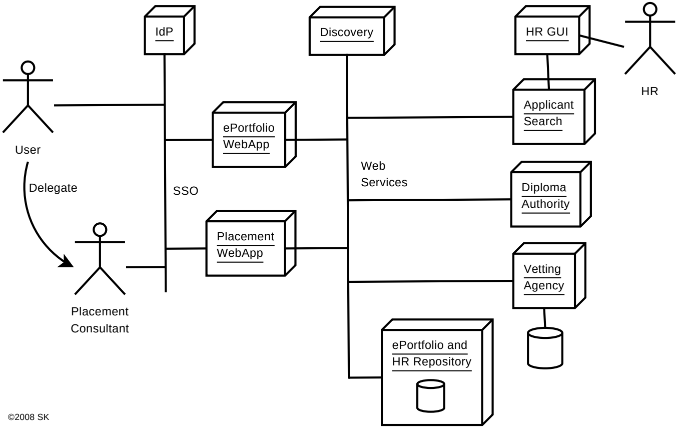
Employability and HR Vertical

- Multiple Players - Excellent case for federation
  - Consumer / Employee, getting his identity from a number of sources
  - Enterprise players
  - Service Provider Players
- Web Application front ends
- Fat clients: Web Services
- SOA: Web Services
- A lot of policy around what can be accessed by whom - XACML

Privacy Sensitive Data, Compelling Need to Share

- You do not play if you do not share
- Strong consciousness about implications of sharing
  - Filter depending on who asks
  - Policy enforcement
- Pseudonymous identity, but real data
- Authorativeness of data: Entitlements, Professional Certifications

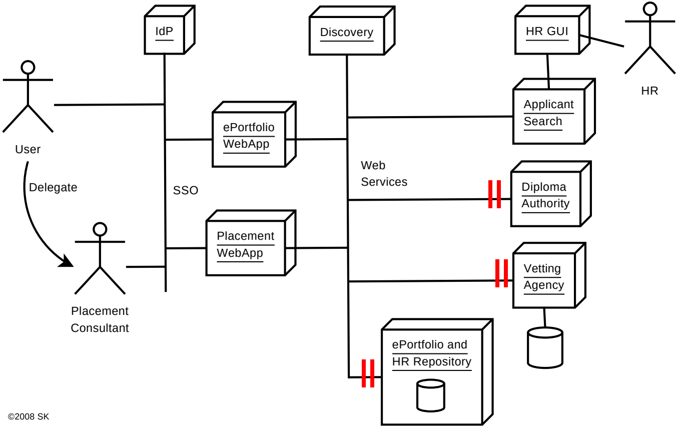
Multiple Organizations Consuming and Offering Services



Requirements

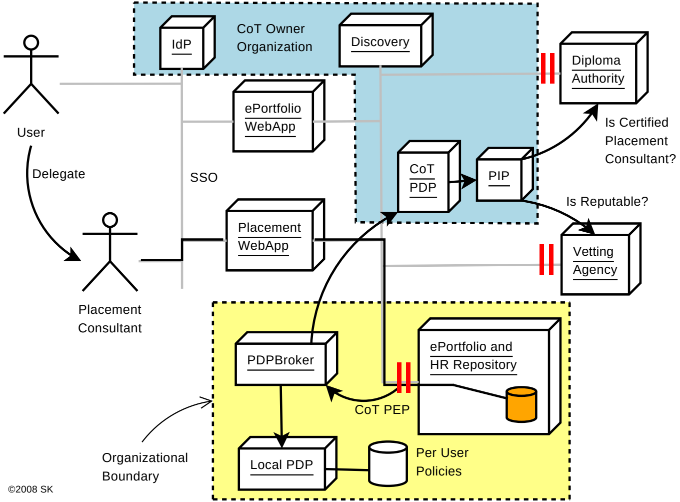
- Players
  - User
  - Placement Consultant
  - Placement Agency
  - Diploma Authority (e.g. Educational Institution granting degrees)
  - Employer HR
  - Vetting Agency
- Policies
  - System-wide
  - Per service
  - Per Data
  - Per user

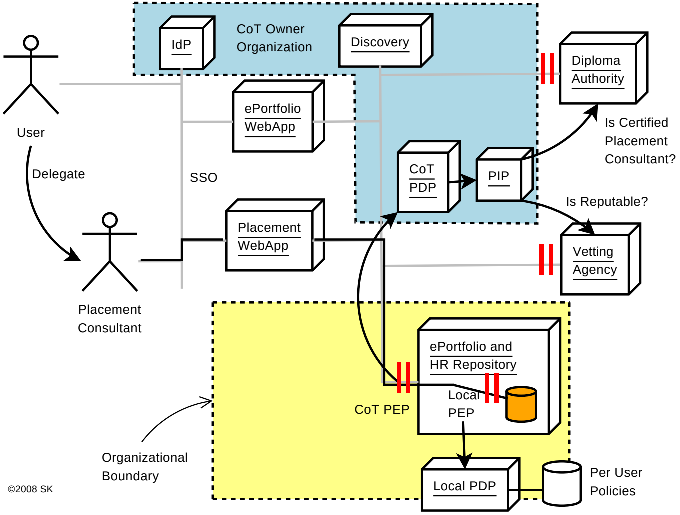
Need for Control



Which PDP Dilemma

- ePortfolio, Entitlement Authority, and Vetting Agency all have very privacy sensitive information
- All are operated by different organization: can they use one PDP?
- Entitlement based system is well suited
  - Information from SSO layer
  - Information from Diploma Authority
  - Information from Vetting Agency
  - All information describes to what category a person belongs to
  - Rules can then be applied to decide whether access is granted
- Rules will be owned by organization releasing data
- Per user rules are also possible
- Overall network may also have rules, available from global CoT PDP


IdP
CoT Owner Organization
Discovery
User
Diploma Authority
ePortfolio WebApp
Is Certified Placement Consultant?
Delegate
SSO
CoT PDP
PIP
Is Reputable?
Placement WebApp
Vetting Agency
Placement Consultant
PDPBroker
ePortfolio and HR Repository
CoT PEP
Organizational Boundary
Local PDP
Per User Policies


CoT Owner Organization
IdP
Discovery
User
Delegate
ePortfolio WebApp
SSO
Diploma Authority
Is Certified Placement Consultant?
CoT PDP
PIP
Is Reputable?
Placement Consultant
Placement WebApp
Vetting Agency
ePortfolio and HR Repository
Local PEP
CoT PEP
Organizational Boundary
Local PDP
Per User Policies
©2008 SK

PDP Solutions

- Local PDP for rules owned by local organization
  - Can also hold per user rules
- Global CoT-wide PDP for the "house rules"
- PIP uses web services to further query job certifications and reputation
- PDP Broker realization
  - ePortfolio repository only has one PEP - minimal modification to application
  - PDP Broker is flexible component that allows for future evolution of the architecture
- Two PEPs in cascade solution
  - First PEP checks global policy
  - Second PEP checks house rules and per user policy
- Other arragements, such as PDP Broker direct to Diploma Authority

Experiences

- Granularity - scalability problem
  - Every request making full XACML request is expensive
  - PDP Broker caches decisions to reduce load
- System workable for about 25 requests per second on normal PC server hardware
- XACML rule debugging pretty tough: better keep simple
- Test battery vital for ensuring the rules stay right when there are changes

Technology

- Symlabs IdP (and Discovery)
- Symlabs PDP Broker
- Apache with `mod_auth_saml` SP, PEP
- `ZXID.org` ID-HR-XML WSC and WSP
- ElfEL ePortfolio system

Thank You

Sampo Kellomäki (sampo@symlabs.com)
+351-918.731.007
www.symlabs.com
www.zxid.org
http://freshmeat.net/zxid

Acronym Expansion

PEP Policy Enforcement Point

PDP Policy Decision Point

PIP Policy Information Point

IdP Identity Provider (SAML role, asserting party, credential authority)

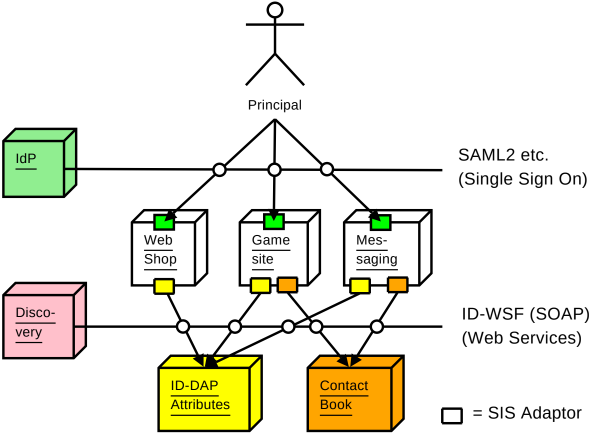
SP Service Provider (e.g. web site) (SAML role, relying party)

WSC Web Services Client

WSP Web Services Provider

DS Discovery Service

SAML 2.0 for SSO, Liberty ID-WSF for SOAP



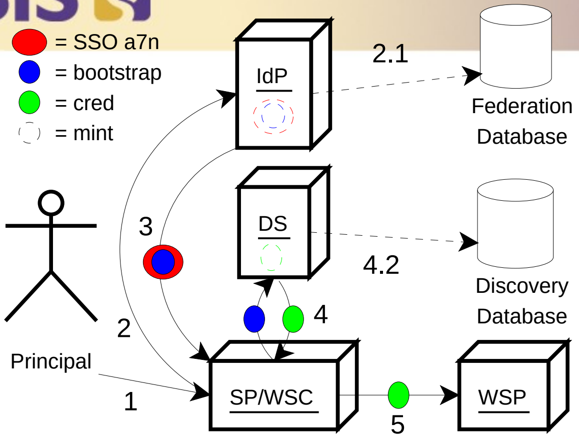


Figure 1: Single Sign-On (2,3), Discovery (4), and call to WSP (5). The blue ball represents discovery bootstrap.

Liberty ID-WSF (Web Services Framework)

- Focuses on passing identity on SOAP calls (just what SOA needs)
- Secures the SOAP call
  - WS-Security header
  - SAML token conveying authenticated user present and consented
  - Digital signature
- Helps locate SOAP services
  - Bootstrap
  - Discovery
- Calling other user's web services: People Service
- User consent querying: Interaction Service

ID-WSF Services

- Personal Profile
- ID-DAP (ID Directory Access)
- ID-HR-XML
- Contact Book
- Presence
- GeoLocation
- ID Messaging (email, MMS)
- Your own service