RSA CONFERENCE 2007

Federated SOA: Harmonizing ID Security and Web Services

Sara Gates,
VP, Software Infrastructure Marketing,
Sun Microsystems,
02/09/07 - SOA-401

RSACONFERENCE2007

Federated SOA: Harmonizing ID Security and Web Services

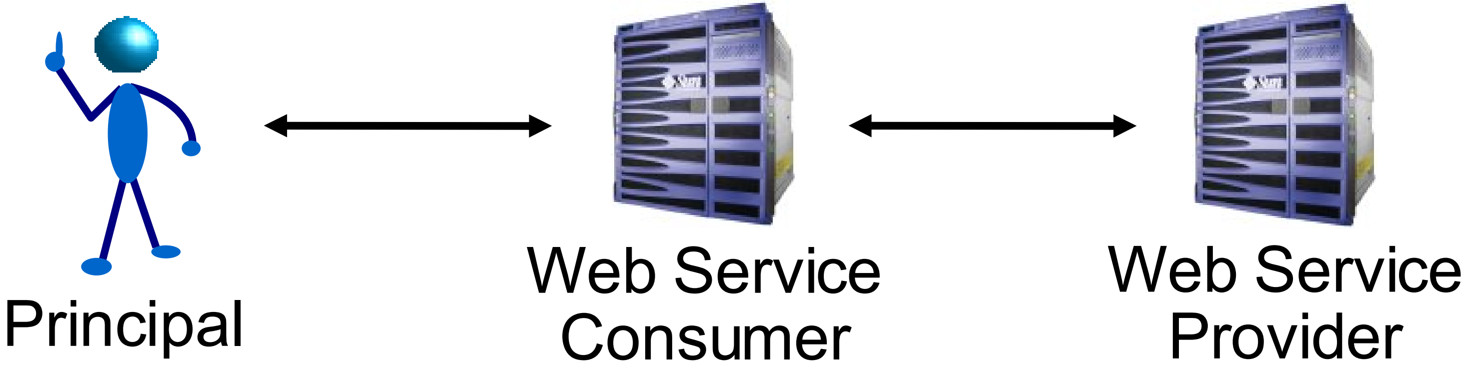
~~Sara Gates,~~
VP, ~~Software Infrastructure Marketing~~,
Sun Microsystems,
02/09/07 - SOA-401

RSA CONFERENCE 2007

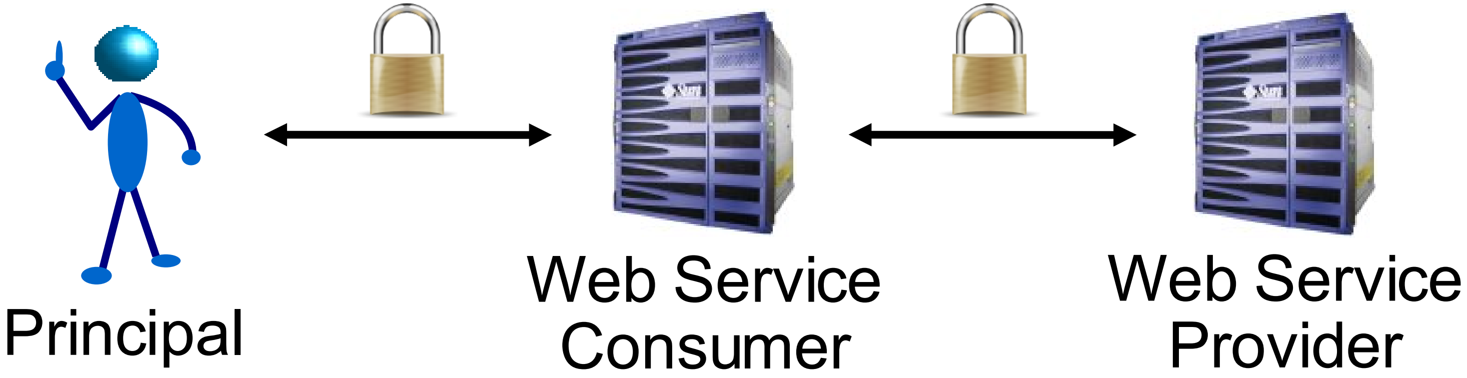
Federated SOA: Harmonizing ID Security and Web Services

Pat Patterson,
Federation Architect,
Sun Microsystems,
02/09/07 - SOA-401

Typical Web Service Model



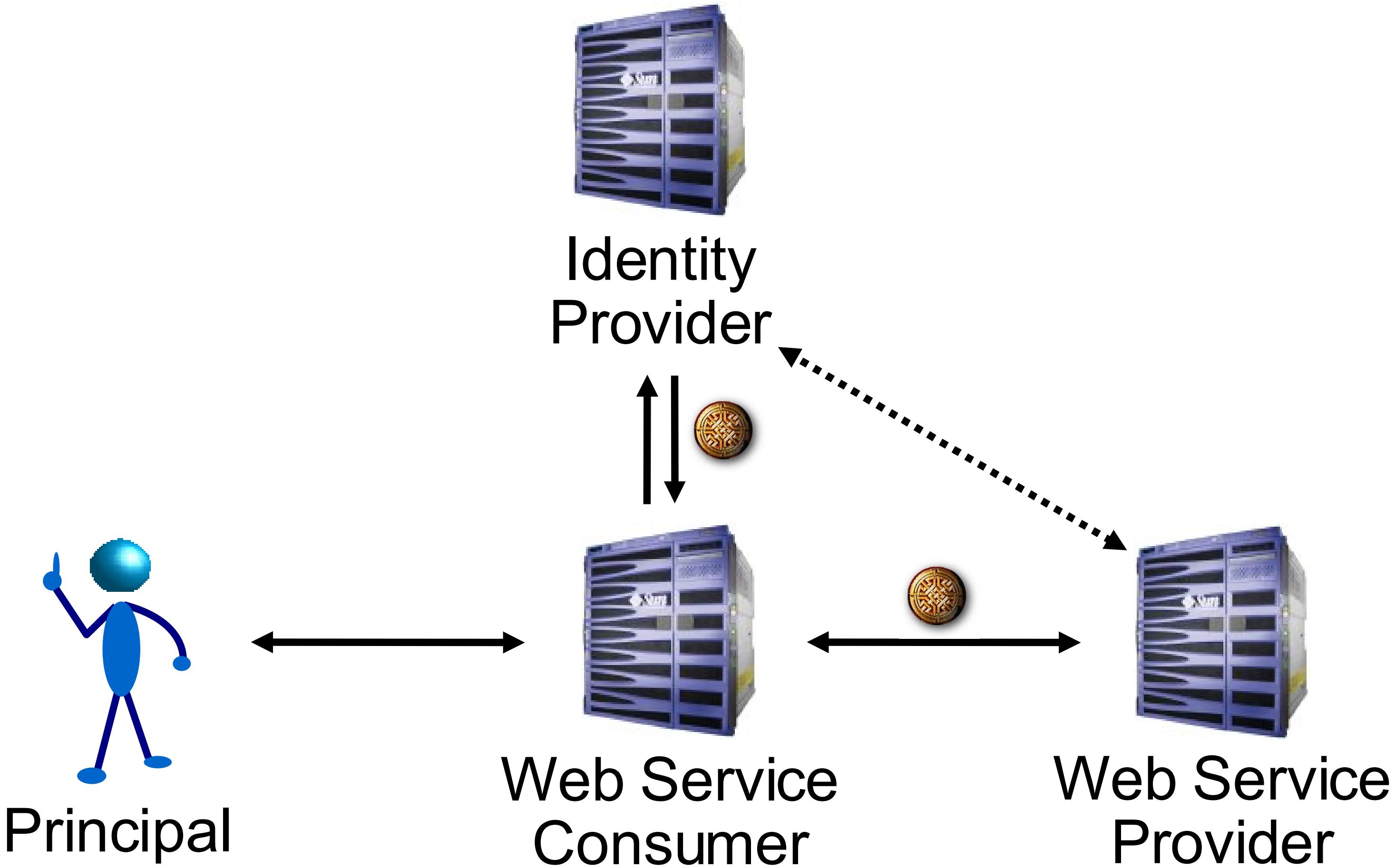
Transport-level Security



Transport-level Security != Identity

- Difficult choice between
  - No client authentication
  - Client authentication via certificates
- Scope of protection is limited to individual 'hops'
- Even with client authentication, no real non-repudiation due to difficulty of archiving and verifying message flow
- TLS/SSL is still essential for confidentiality and integrity at the transport level, but is not enough – we need a solution at the message level

Basic Web Service Security



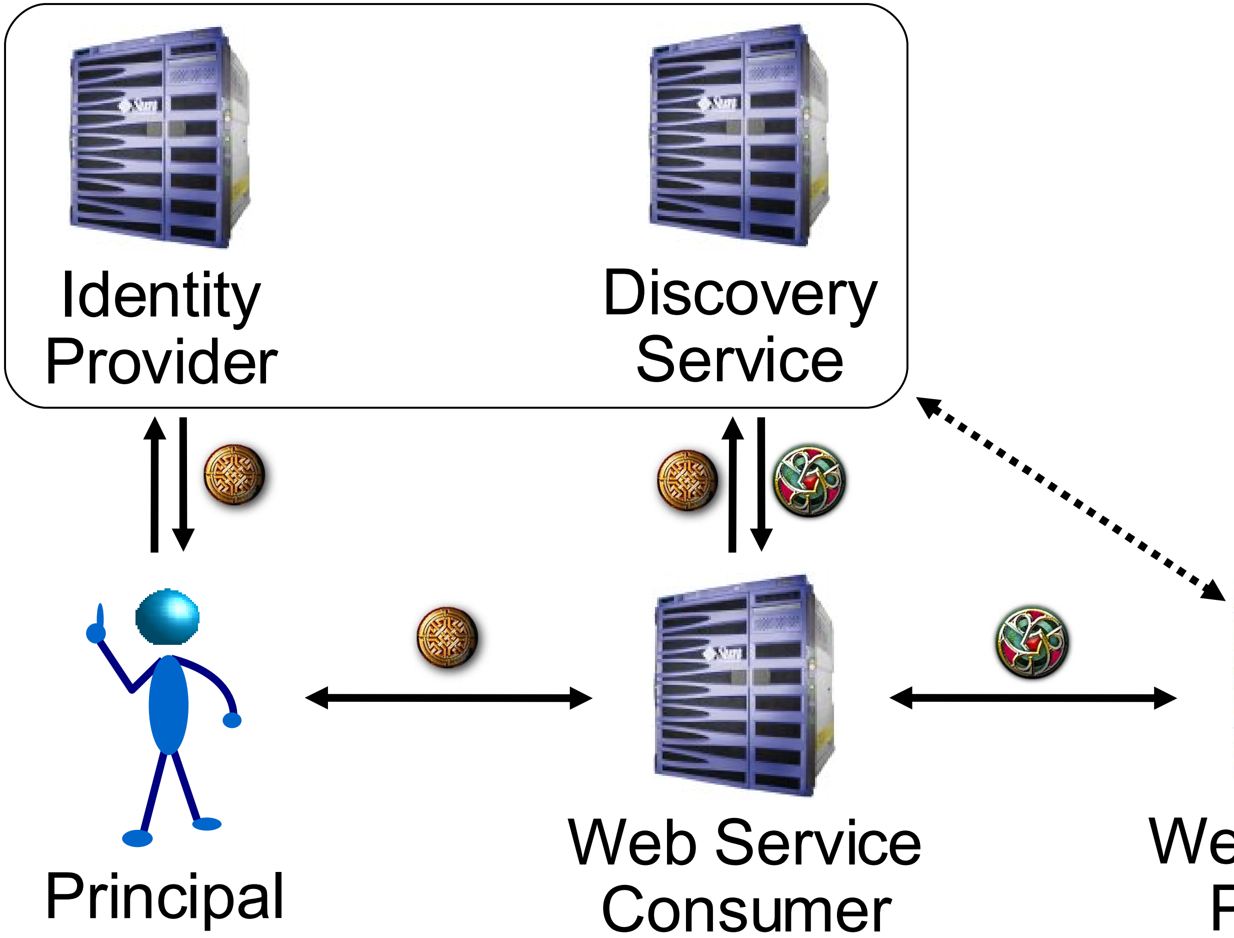
Message-level Security – Getting There

- Identity *token* carried in SOAP header
  - WS-Security, WS-I Basic Security Profile
  - Industry has converged on SAML Assertion as the token
- SAML allows for bearer tokens, holder-of-key tokens, audience restrictions etc
- Token can be archived with message
- BUT...
- Restricting the audience to the immediate recipient leaves us with similarly limited scope of protection – one hop

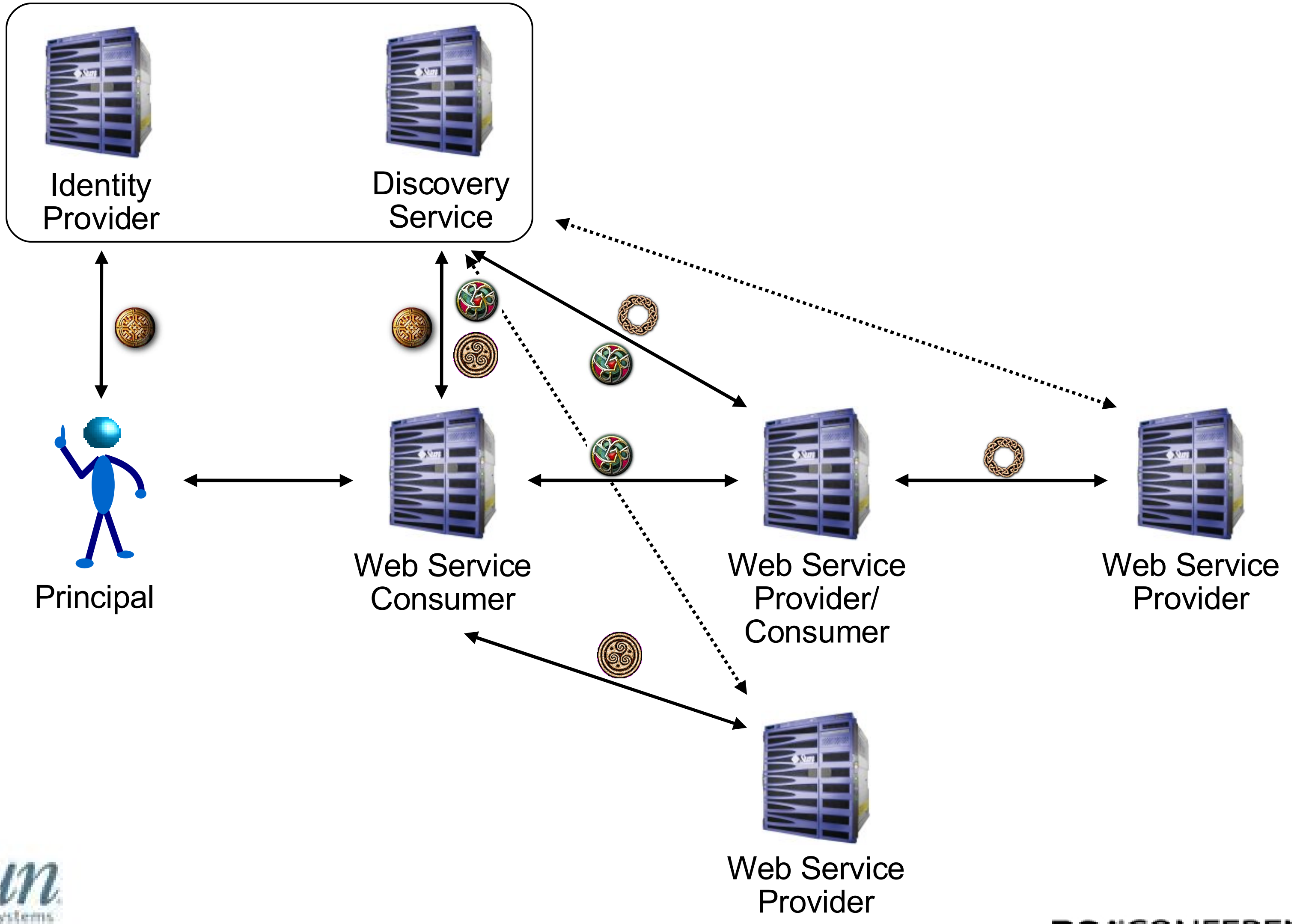
Requirements for Web Service *Identity*

- Identify the principal
- Locate the service
- Preserve identity
  - Across multiple 'hops'
  - Across domain boundaries
  - Across vendors' products
- Using existing technologies and idioms
- Maintaining privacy

Identity Web Services



Scaling Out


Identity Provider
Discovery Service
Principal
Web Service Consumer
Web Service Provider/ Consumer
Web Service Provider
Web Service Provider

Liberty Identity Web Services Framework (ID-WSF)

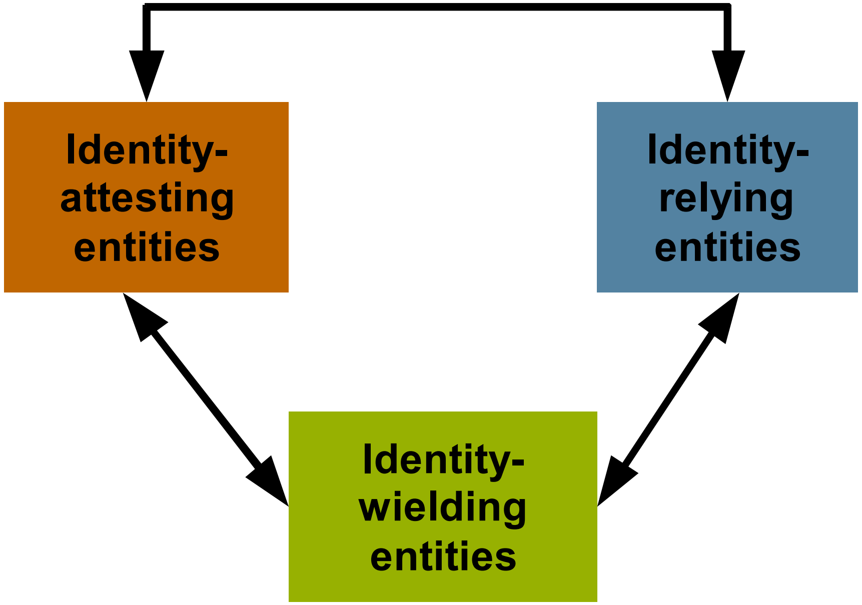
- Dynamic service discovery and addressing
- Common web services transport mechanisms to apply identity-aware message security
- Abstractions and optimizations to allow anything – including client devices – to host identity services
- Unified data access/management model for developers
- Flexibility to develop arbitrary new services
- User privacy through use of pseudonyms

Liberty-published Standards in Context

- **ID-WSF:** Identity Web Services Framework
- Focused on application-to-application interaction

ID-SIS: Service Interface Specs

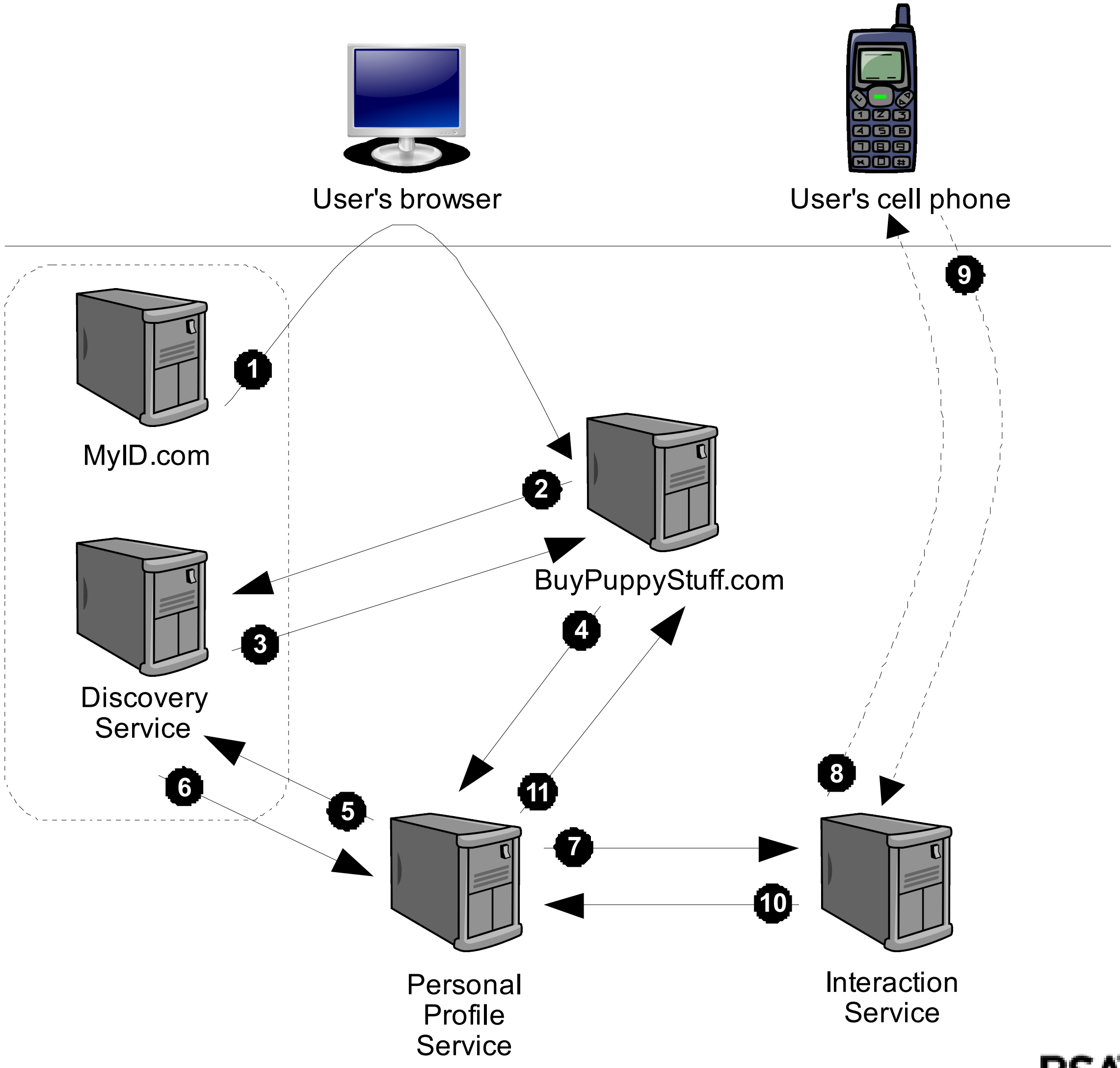
- ID-SIS plus ID-WSF equals *“Liberty Web Services”*
- Defines particular useful services
- Personal profile, geo-location...


Identity-attesting entities
Identity-relying entities
Identity-wielding entities

ID-FF: Identity Federation Framework

- *“Liberty Federation”*
- Focused on human-to-application interaction
- Now converged with SAML V2.0

An All-Singing, All-Dancing Sample Flow

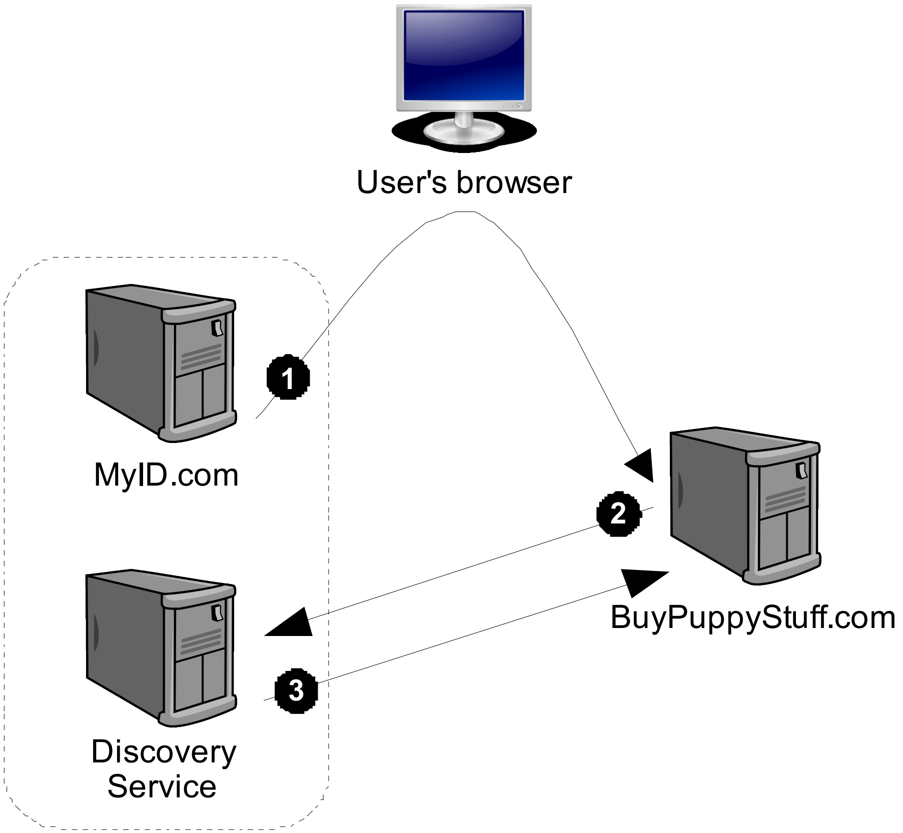


Kicking Off an App-to-App Interaction

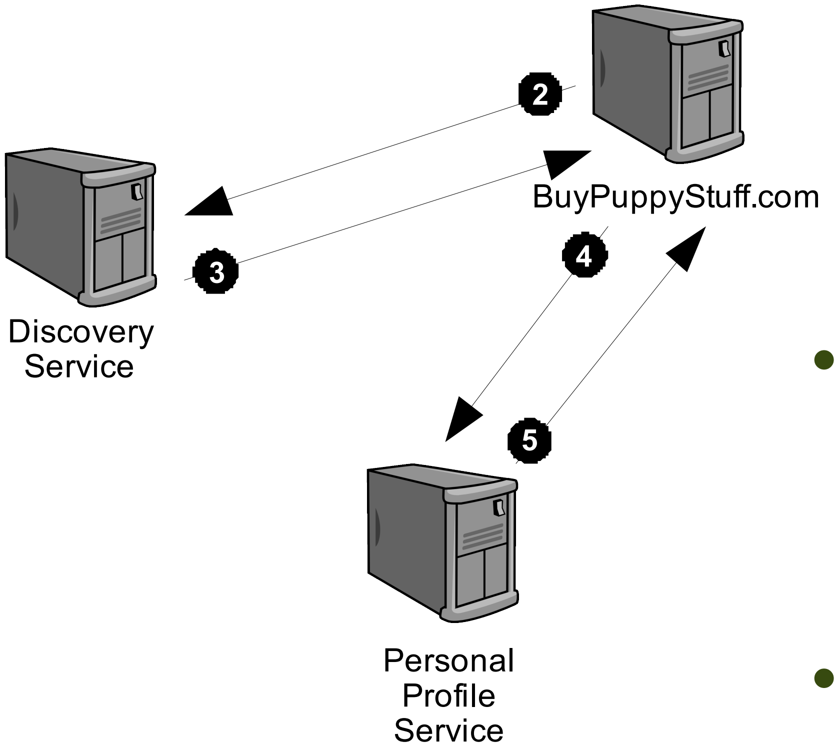
- It usually starts with a user (possibly not you!) logging in and asking for some service behavior involving your identity

- During SSO, the IdP informs the SP where to find *your* **Discovery Service (DS)**
  - A hub for locating, and possibly getting coarse-grained authorization to use, various identity services of yours

- In a typical deployment, the IdP and DS form one tightly coupled software component



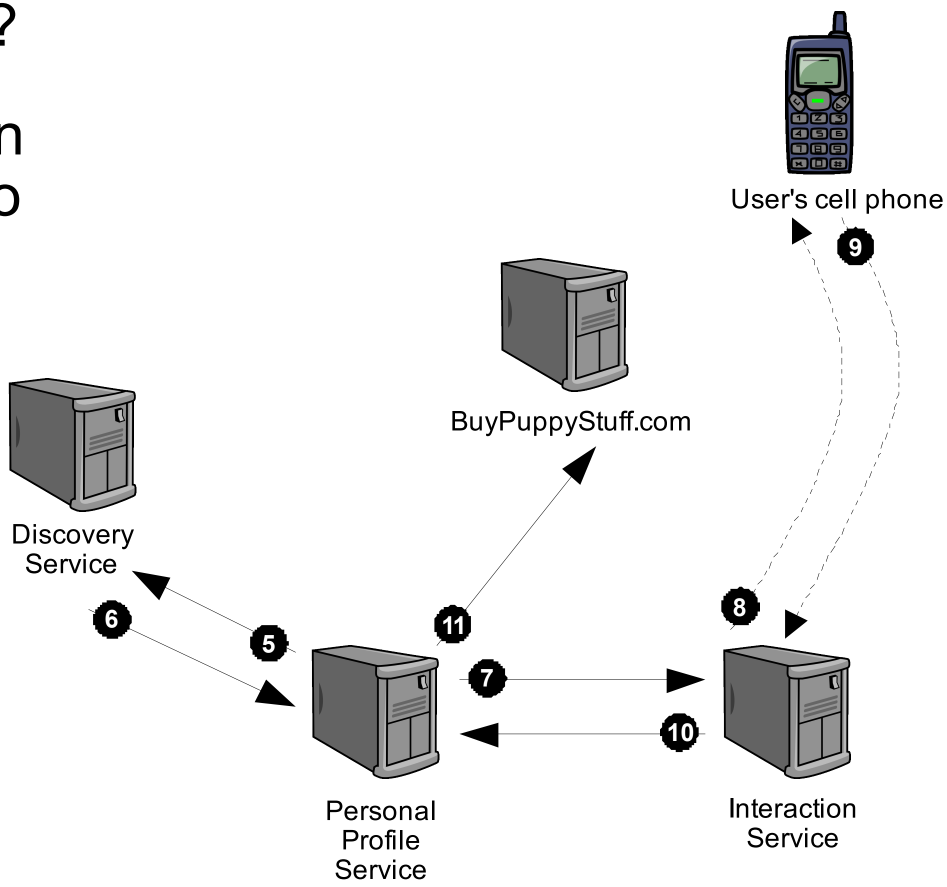
The Locate-and-Access Dance



- The SP dons the role of a **web service consumer (WSC)**
  - A WSC is the requestor endpoint, and a **web service provider (WSP)** is the responder endpoint
  - **Tip:** Mentally add “of identity data” to remember which is which
- The WSC asks the DS where a particular WSP is, and asks for access
  - WSPs will typically do fine-grained WSC authorization themselves
- One example of a WSP is the ID-SIS **Personal Profile (PP)** service for name, address, etc.

Getting Information-Sharing Approval

- What if the PP service needs to check with you before responding?
- It can ask your DS where to find an **Interaction Service (IS)** for you so it can bother you real-time
  - According to your own policy preferences for what's important enough to bother you with
- The PP is acting as a WSC
  - Doing the locate-and-access dance itself, just like BuyPuppyStuff did
- The IS uses non-Liberty means to (e.g.) SMS you for approval



Mapping to Products

- Sun Java System Access Manager
  - The 'whole stack' for identity web services - Identity Provider, Discovery Service, Service Provider etc etc etc
  - Web Access Control, Single Sign-On, Federation
  - Version 7.1 includes substantial new tooling support for both WS-I BSP and ID-WSF
    - NetBeans Enterprise Pack
- Sun Java System Federation Manager
  - Service Provider
- Open Federation, OpenSSO
  - Open source

Conclusion

- Analysis is all important – understand your requirements
  - “As simple as possible, but no simpler”
- Download NetBeans Enterprise Pack or OpenSSO to get a feel for identity web services
- PoC, Pilot to crystallize requirements
  - http://blogs.sun.com/superpat/tags/turkcell
- Phase in identity web services – initial phase should not be mission critical!
  - http://blogs.sun.com/superpat/tags/bipac
- Consider joining the Liberty Alliance
- Attend Eve Maler and Brett McDowell's session – “Federated Identity: Evolving Past Industry Strife” - 11:10am Green Room 103

Resources

- Sun Java System Access Manager
  - http://www.sun.com/software/products/access_mgr/
- OpenSSO
  - https://opensso.dev.java.net/
- Liberty Alliance
  - http://projectliberty.org
- Pat's Blog
  - http://blogs.sun.com/superpat

RSA CONFERENCE 2007

Federated SOA: Harmonizing ID Security and Web Services

Pat Patterson,
Federation Architect,
Sun Microsystems,
pat.patterson@sun.com