WELCOME TO JAVAPOLIS

JAVAPOLIS '07

10 - 14 DECEMBER ▪ ANTWERP ▪ BELGIUM

JAVAPOLIS '07
10 - 14 DECEMBER ▪ ANTWERP ▪ BELGIUM

SAML 2.0

Pat Patterson
Federation Architect
Sun Microsystems

Sun microsystems

Overall Presentation Goal

Learn about SAML,
how it's used to implement web single sign-on and secure web services and how to use it

Speaker’s Qualifications

- Pat Patterson is...
  - A Federation Architect at Sun Microsystems
  - The 'community guy' for OpenSSO
  - One of Sun's reps at the Liberty Alliance
  - A speaker for Sun on identity and federation
  - A blogger, covering identity, federation and single malt scotch whisky

SAML is pretty straightfoward,
if you look at it piece by piece.

The Problems

- “I have too many passwords – my monitor is covered in Post-its!”
- “We're implementing Sarbanes-Oxley – we need to control access to applications!”
- “We need to access outsourced functions!”
- “Our partners need to access our applications!”

Conflicting Pressures?

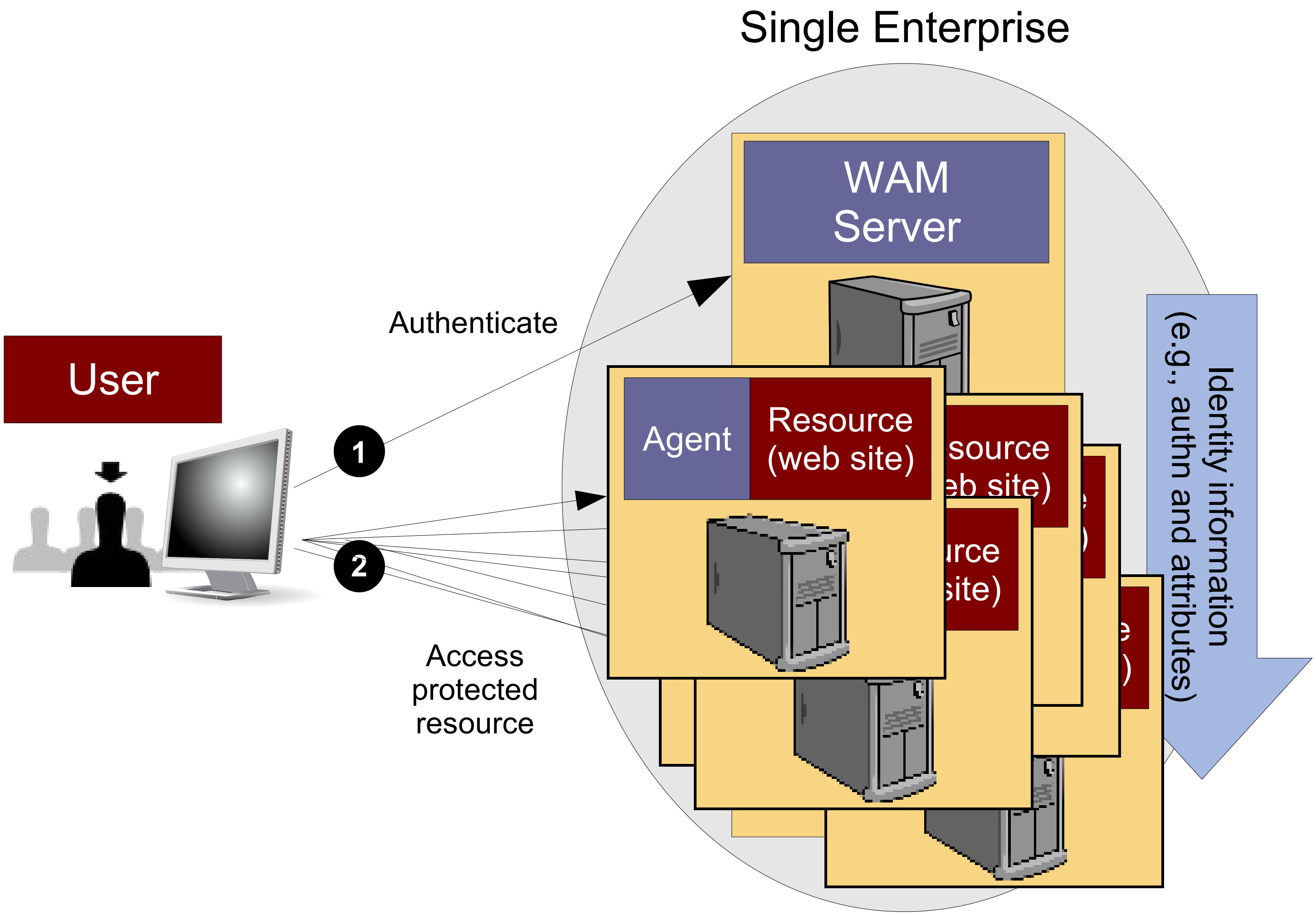
Interoperability

Security

User Convenience

Compliance

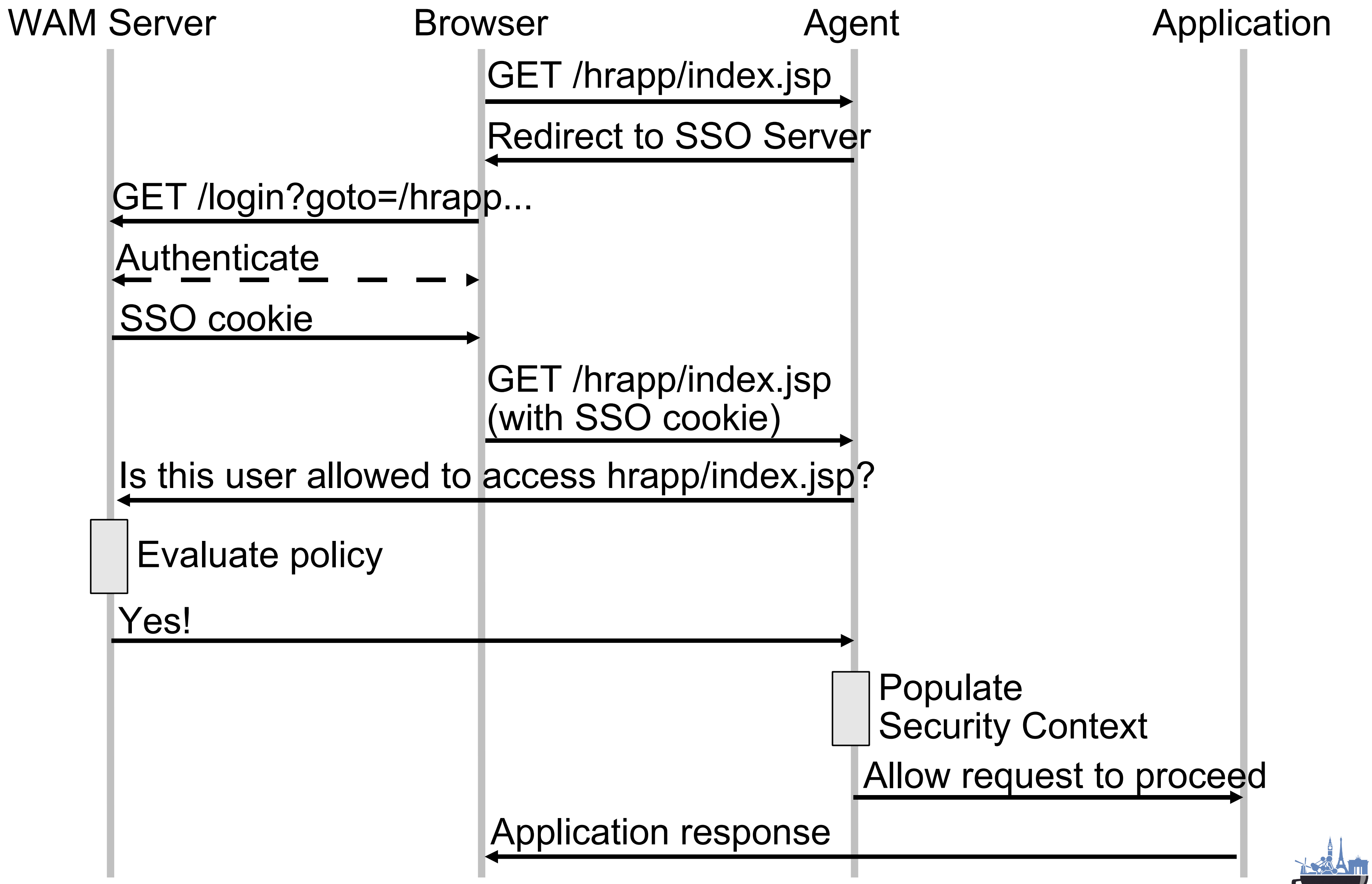
The Basic Use Case for Web Single Sign-On



Web Single Sign-On

- Factor authentication and authorization out of web applications into web access management (WAM) solution
- Can use browser cookies within a DNS domain
- Proxy or Agent architecture implements role-based access control (RBAC)
- Users get single sign-on, IT gets control

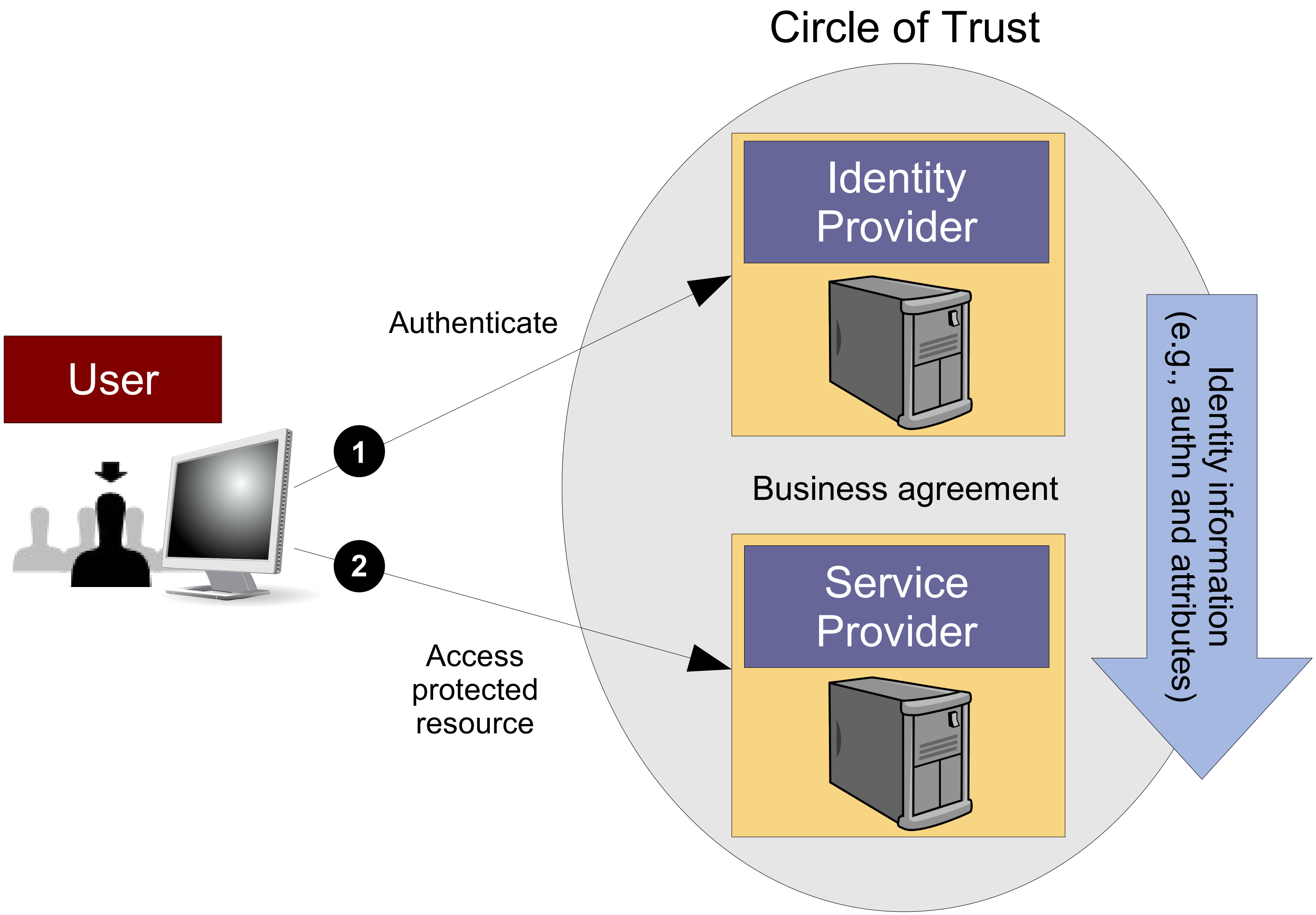
How it works


WAM Server
Browser
Agent
Application
GET /hrapp/index.jsp
Redirect to SSO Server
GET /login?goto=/hrapp...
Authenticate
SSO cookie
GET /hrapp/index.jsp
(with SSO cookie)
Is this user allowed to access hrapp/index.jsp?
Evaluate policy
Yes!
Populate
Security Context
Allow request to proceed
Application response

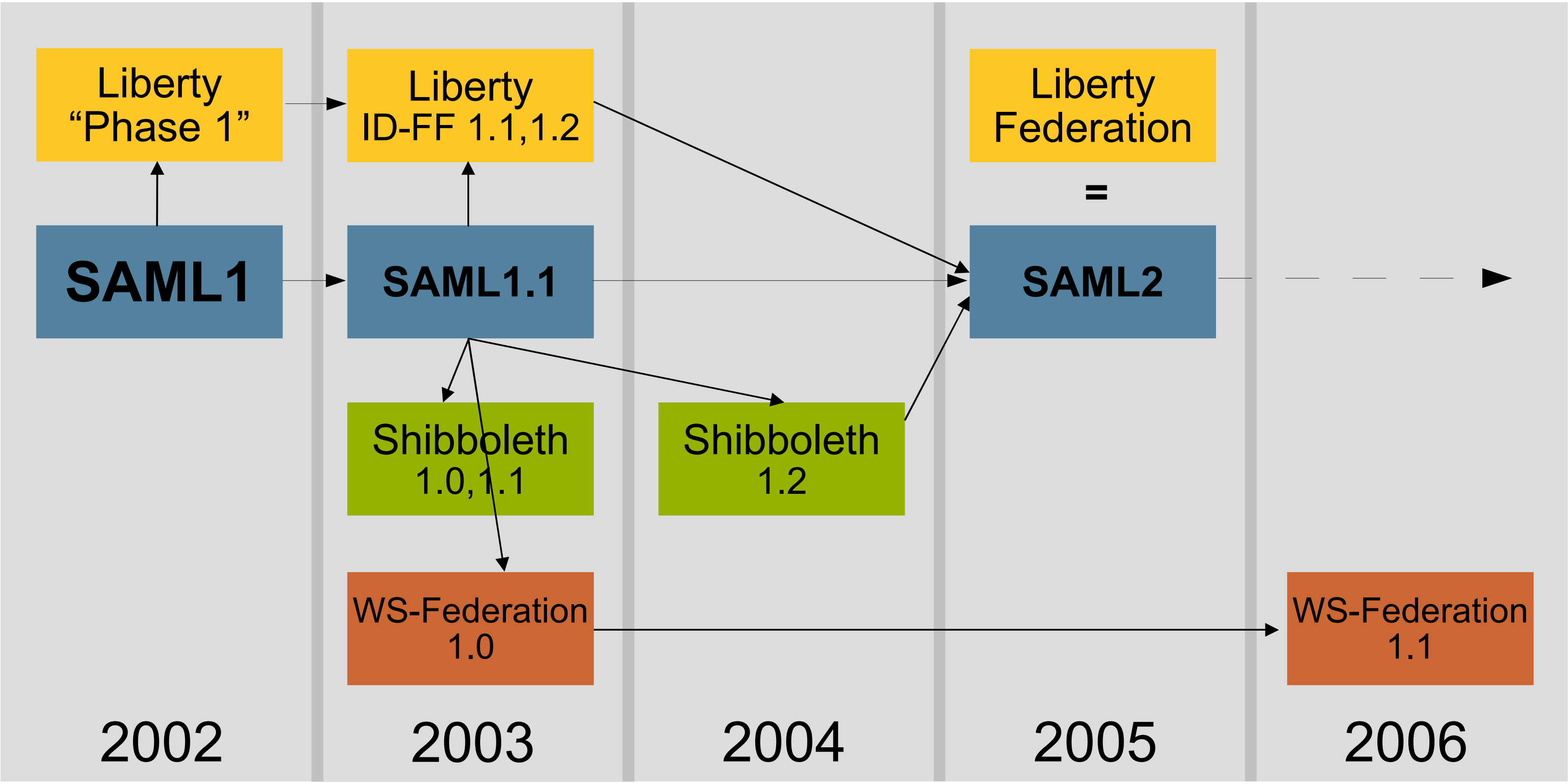
Single Sign-on *between* Enterprises

- Cookies no longer work
  - Need a more sophisticated protocol
- Can't mandate single vendor solution
  - Need standards for interoperability

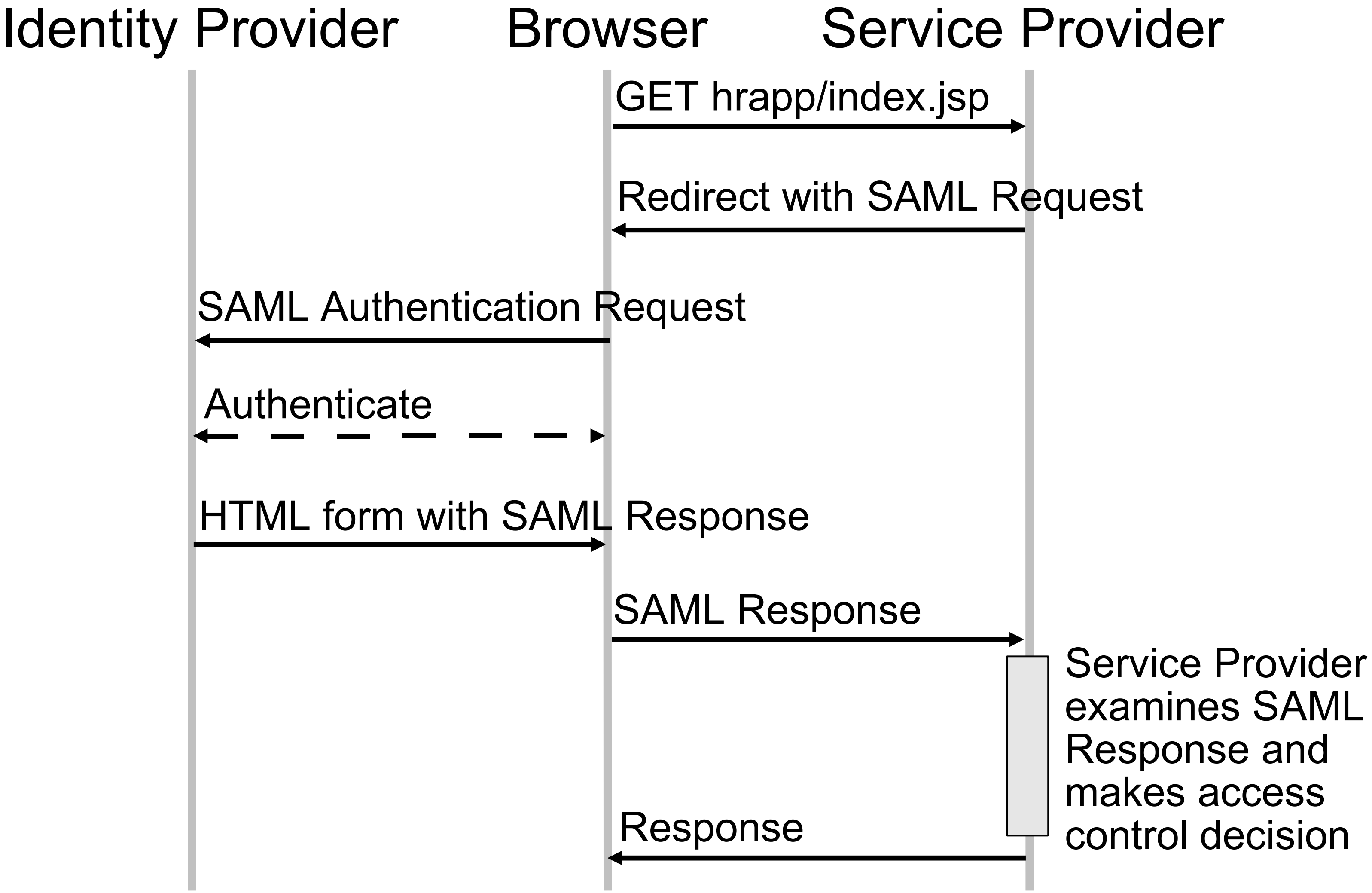
SSO Between Enterprises



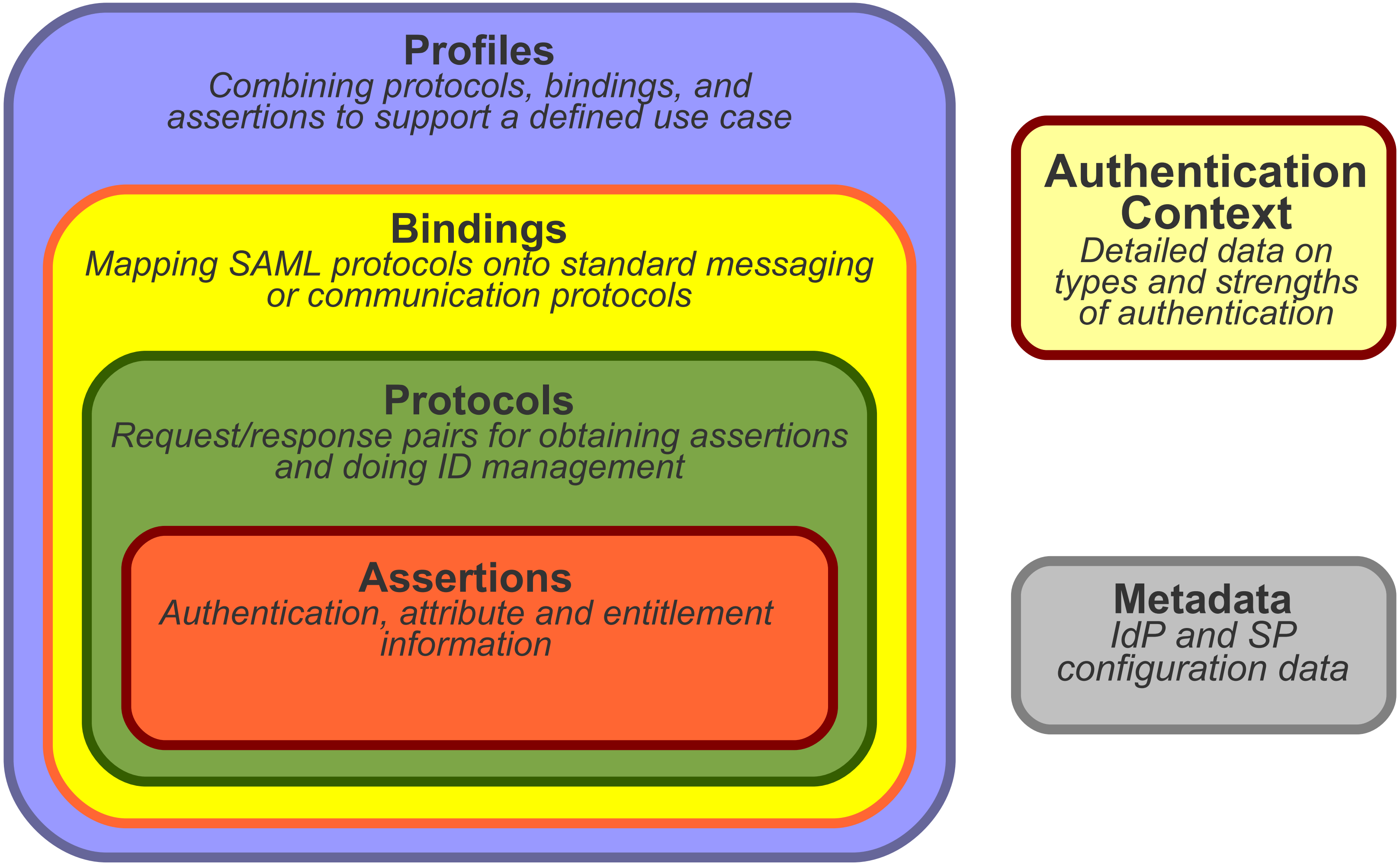
Single Sign-On Standards



SAML 2.0 SSO Basics


Identity Provider
Browser
Service Provider
GET hrapp/index.jsp
Redirect with SAML Request
SAML Authentication Request
Authenticate
HTML form with SAML Response
SAML Response
Service Provider examines SAML Response and makes access control decision
Response

SAML 2.0 Concepts



Profiles
Combining protocols, bindings, and assertions to support a defined use case

Bindings
Mapping SAML protocols onto standard messaging or communication protocols

Protocols
Request/response pairs for obtaining assertions and doing ID management

Assertions
Authentication, attribute and entitlement information

Authentication Context
Detailed data on types and strengths of authentication

Metadata
IdP and SP configuration data

SAML 2.0 Assertion

(Abbreviated!)

```
<Assertion Version="2.0" ID="..." IssueInstant="2007-11-06T16:42:28Z">
    <Issuer>https://someidp.com/</Issuer>
    <Signature>...</Signature>
    <saml:Subject>
        <saml:NameID Format="urn:oasis:...:persistent" ...>
            ZG0OZ3JWP9yduIQ1zFJbVVGHlQ9M
        </saml:NameID>
        <saml:SubjectConfirmation Method="urn:oasis:...:bearer">
            <saml:SubjectConfirmationData .../>
        </saml:SubjectConfirmation>
    </saml:Subject>
    <saml:Conditions
      NotBefore="2007-11-06T16:42:28Z" NotOnOrAfter="2007-11-06T16:52:28Z">
        <saml:AudienceRestriction>
            <saml:Audience>
                https://somesp.com/
            </saml:Audience>
        </saml:AudienceRestriction>
    </saml:Conditions>
    <saml:AuthnStatement AuthnInstant="2007-11-06T16:42:28Z" ...>
        <saml:AuthnContext>
            <saml:AuthnContextClassRef>
                urn:oasis:...:PasswordProtectedTransport
            </saml:AuthnContextClassRef>
        </saml:AuthnContext>
    </saml:AuthnStatement>
</saml:Assertion>
```

SAML 2.0 For The Java Developer

- Select a web access management product that implements SAML 2.0
  - Sun Java System Access Manager
  - Sun Java System Federation Manager
- Deploy
- Configure
- request.getHeader(“SOME_ATTRIBUTE”)

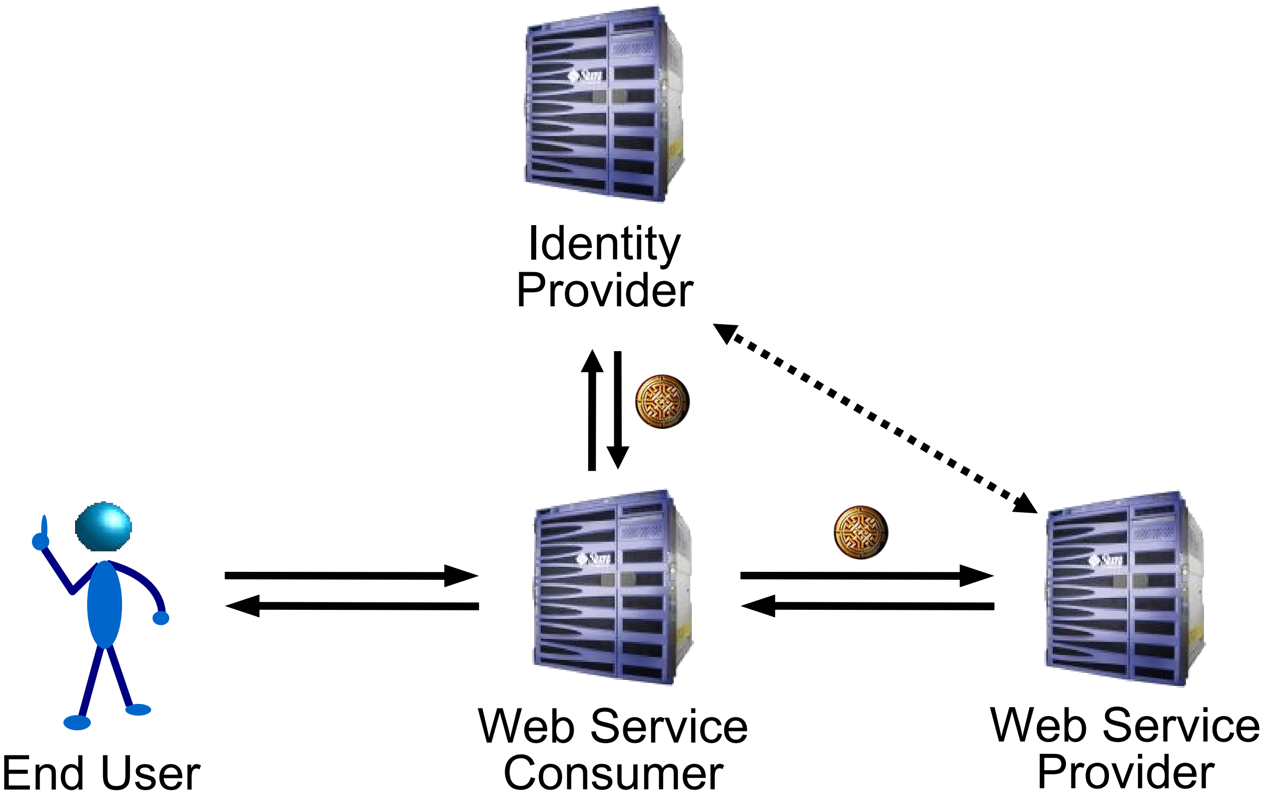
SAML 2.0 Vendor Adoption

- Sun, IBM, CA – all the usual suspects, except Microsoft
- OpenSAML (Internet2)
  - Java, C++
- OpenSSO (Sun)
  - Java, PHP, Ruby
- SimpleSAMLphp (Feide)
- LASSO (Entr'ouvert)
  - C/SWIG
- ZXID (Symlabs)
  - C/SWIG

SAML 2.0 Deployments

- Italy – Ministry of Transportation
- France – 'Mon Service Public', Bibliotheque Nationale
- Norway – 'MinSide', Feide
- US – General Services Administration (GSA) eAuthentication
- Google Apps for Your Domain
- Sun
  - BIPAC (political action committee)
  - Hewitt (outsourced HR)

Basic Web Services Security



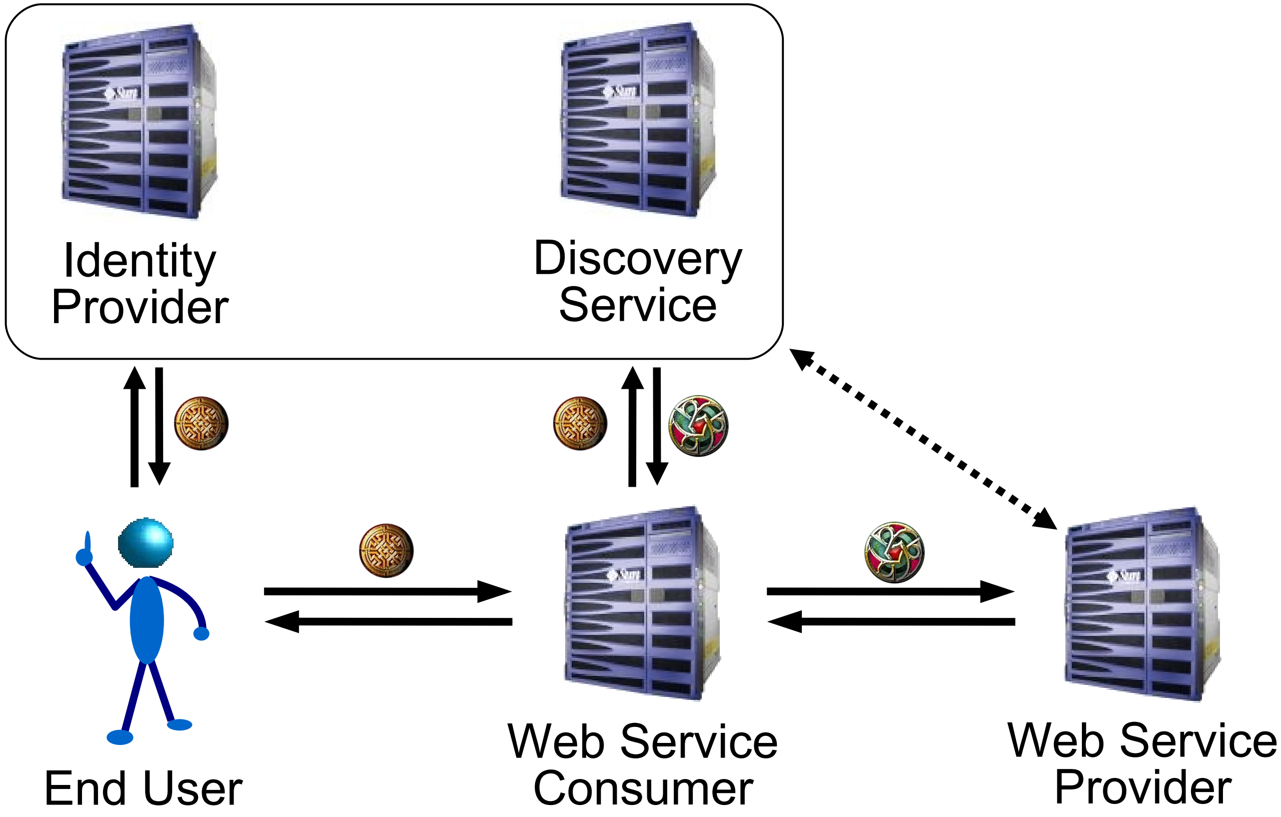
Message-level Security

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

Identity Web Services



Liberty Identity Web Services Framework (ID-WSF)

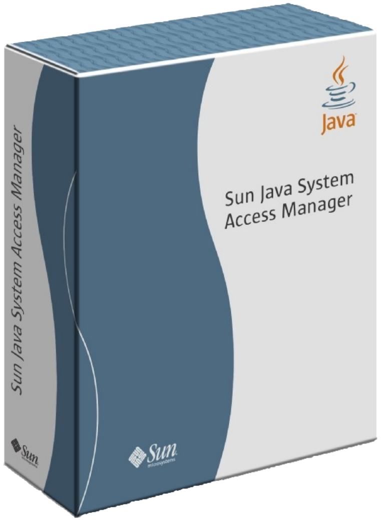
- Dynamic service discovery and addressing
- Common web services transport mechanisms to apply identity-aware message security
- Abstractions and optimizations to allow anything – including client devices – to host identity services
- Unified data access/management model for developers
- Flexibility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

ID-WSF @ Javapolis

- ID-WSF Session
  - C_12_04_05
  - Wednesday 12 Dec
  - 17:50
  - Room 4
- Just stay in your seat :-)

Mapping to Sun's 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


Java
Sun Java System Access Manager
Sun Java System Access Manager
Sun

OpenSSO

- Sun sponsored open source project
- Basis for the next commercial product
  - Sun Java System Federated Access Manager 8.0
- 500 project members, the vast majority outside Sun
- OpenSSO Session
  - C_13_09_03
  - Thursday 13 Dec
  - 15:10
  - Room 9

OpenSSO
Open Access . Open Federation

Summary

- SAML 2.0 is the 'universal solvent' for digital identity
- SAML 2.0 is the lingua franca for interoperability across organizations, vendors
- SAML 2.0 is used by millions of users

Concluding statement

SAML 2.0 is not rocket science!

Acknowledgment: Eve Maler

Resources

- Sun Java System Access Manager
  - www.sun.com/software/products/access_mgr
- OpenSSO
  - opensso.org
- OASIS Security TC
  - www.oasis-open.org/committees/security
- Liberty Alliance
  - projectliberty.org
- Superpatterns
  - blogs.sun.com/superpat

Q&A

View JavaPolis talks @ www.parleys.com

Thank you for your attention