OASIS

DESIGN
DEVELOP
DEPLOY

Catalyst 2002 SAML InterOp

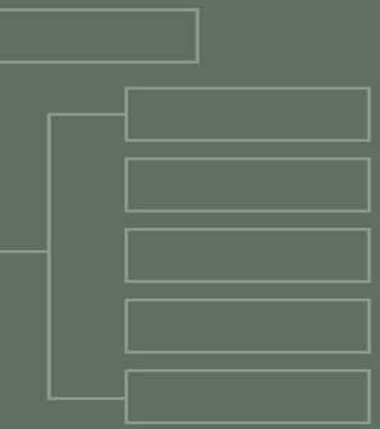
July 15, 2002
San Francisco

Prateek Mishra
Netegrity

OASIS

Agenda

- SAML Intro
- SAML Status
- SAML InterOp Details
- Relationship to other efforts



DESIGN
DEVELOP
DEPLOY

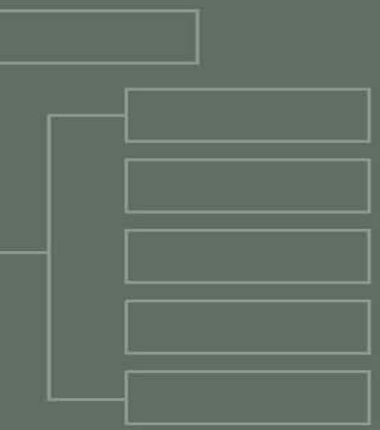
What is SAML?

- Security Assertion Markup Language

- Framework for exchange of security-related information - e.g. assertions
- These assertions about authentication and authorization are expressed as XML documents

What problem does it solve?

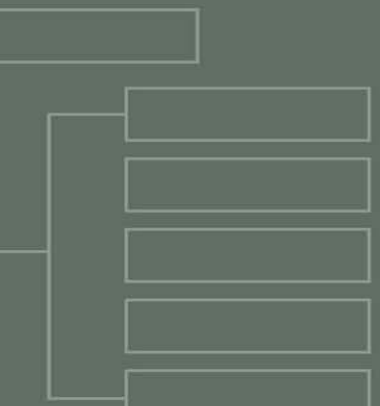
- Identity Federation
  - Provides technology to allow a business to securely interact with users originating from its vendors, suppliers, customers etc.
- Fine Grained Authorization
  - Users may authenticate at one site and be authorized by another



OASIS

What are SAML Profiles?

- A “profile” describes how SAML should be used to solve some business problem
- Web browser profiles for Single-Sign On
  - Part of SAML 1.0
- WS-Security profile for securing web services
  - Currently under development by the SSTC

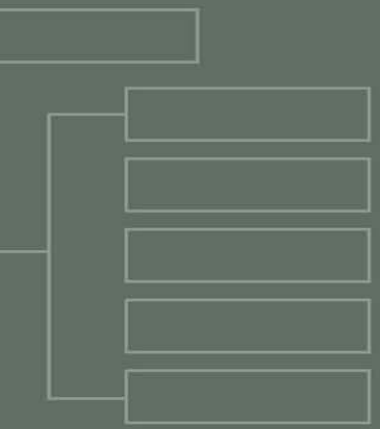


DESIGN
DEVELOP
DEPLOY

OASIS

SAML is NOT…

- A new form of authentication
- An alternative to WS-Security
- Limited to legacy applications
- Limited to web browser applications
- Limited to web services security



DESIGN
DEVELOP
DEPLOY

SAML Status

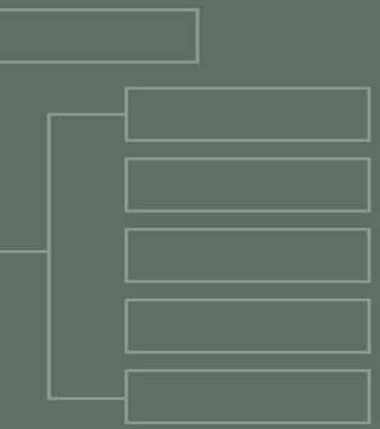
- Developed within OASIS by the security services technical committee (SSTC)
- SSTC voted to accept as committee specification on 16 April 2002
- Submitted to OASIS for acceptance as an OASIS standard on 28 May 2002
  - Anticipate approval 1 Nov 2002
- Several products available today with many announced for near future

OASIS

SAML InterOp Details

- 12 Vendors --- Baltimore Technologies, Crosslogix, ePeople, Entegrity Solutions, IBM/Tivoli, Netegrity, Novell, Oblix, OverXeer, RSA Security, Sigaba, Sun Microsystems

- Each vendor implements the SAML web browser profile for SSO

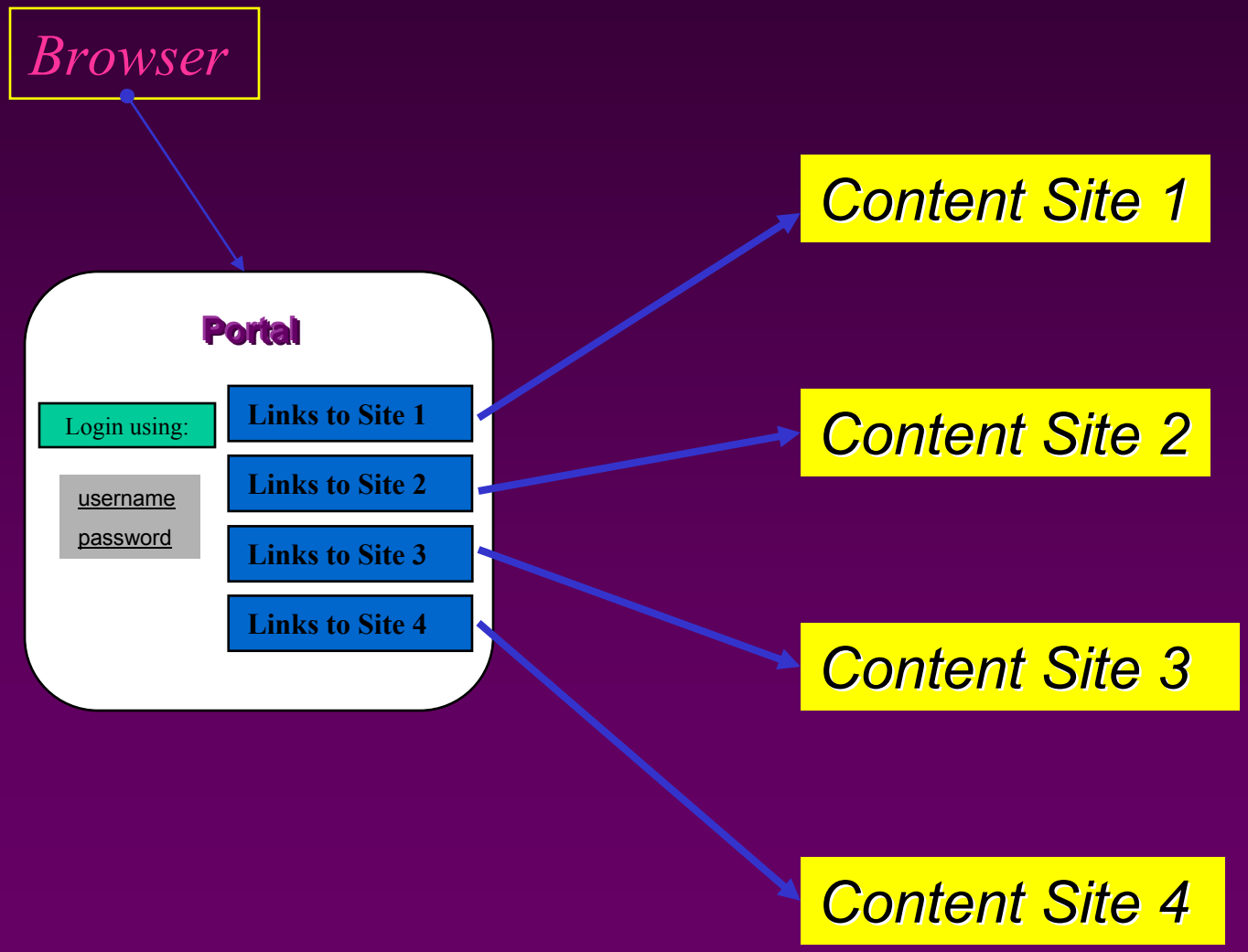


DESIGN
DEVELOP
DEPLOY

Types of Sites in the InterOp

- Portal Site
  - Simulates a govt. or enterprise portal
  - User logs into portal and selects services or content available from “other” sites
- Content (Application) Site
  - Simulates a service or content provider
- Most vendors implement both types of sites

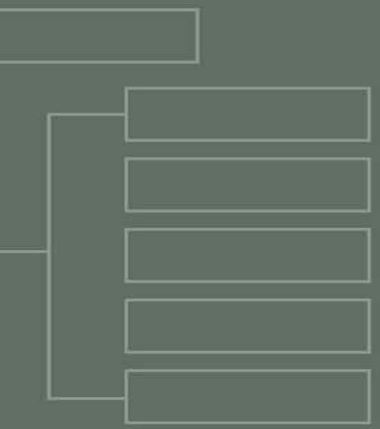
interOp Flows



OASIS

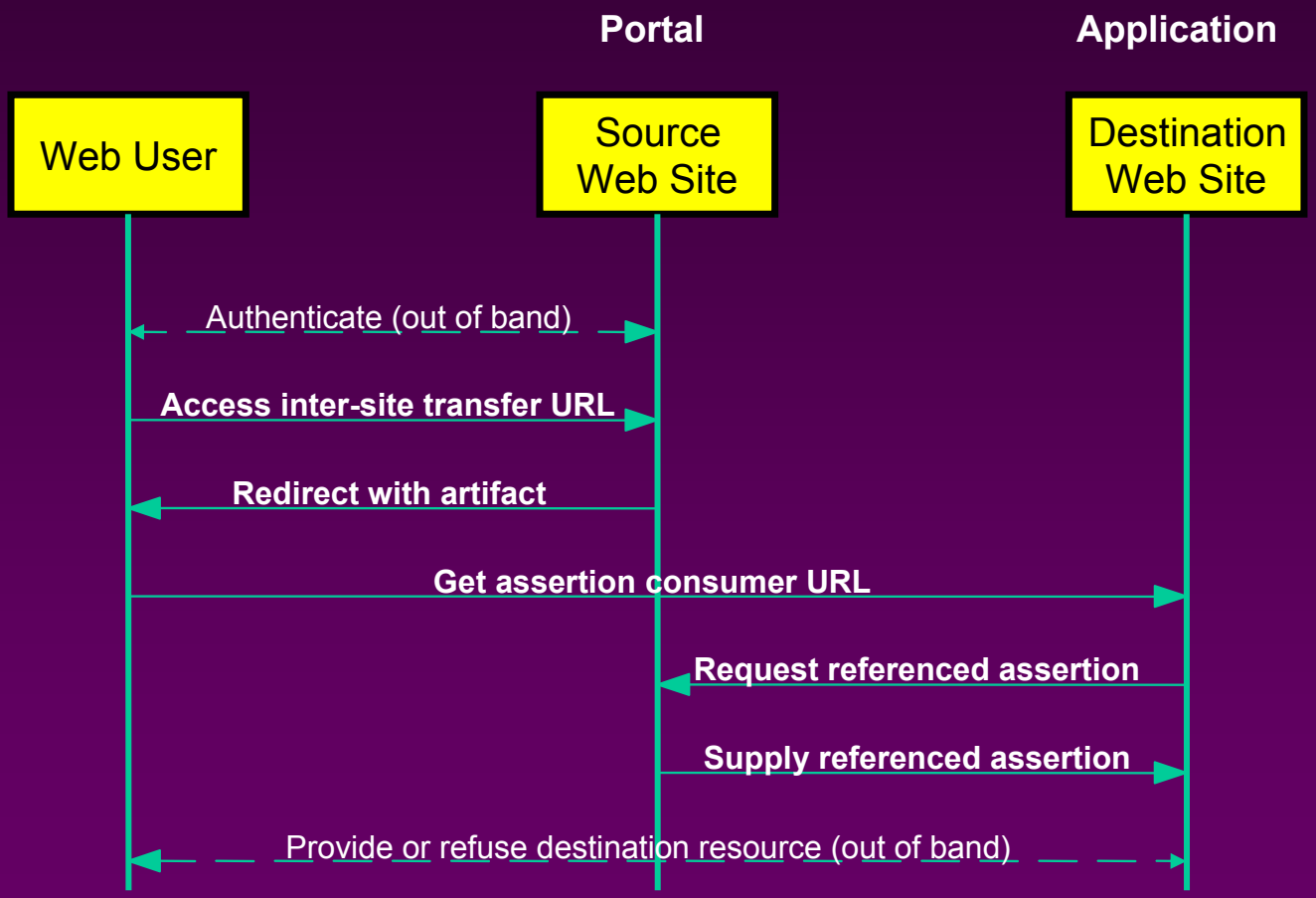
Demonstration Scenario

- Sign on to any portal
- Click thru to any content site
- Content site will display user attributes transmitted from portal and generate appropriate content



DESIGN
DEVELOP
DEPLOY

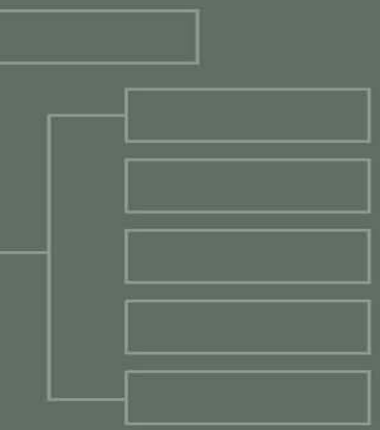
InterOp Message Exchange



OASIS

Browser Profile vs. MS Passport

- MS Passport requires use of single site where users must authenticate
  - SAML browser profile allows user's to authenticate at their "home site" portal
- MS Passport requires proprietary software at content site
  - Software from any vendor implementing SAML browser profile can be used at portal or content sites



DESIGN
DEVELOP
DEPLOY

OASIS

SAML and Liberty Alliance

- Builds on SAML and Web Browser Profiles
- Explicit policy framework for federation
- Adds additional protocol layers
  - logout, where-are-you-from service

DESIGN
DEVELOP
DEPLOY

OASIS

Credits

- Hard work by all demo participants
- Equipment and Software provided by: RSA Security, SUN Microsystems, Baltimore Technologies
- Special thanks to: Don Bowen, Rob Philpott, Irving Reid

DESIGN
DEVELOP
DEPLOY

InterOp Users

- User: alice, Password: alice
  MemberLevel: bronze
- User: ravi, Password: ravi
  MemberLevel: silver
- User: joe, Password: joe
  MemberLevel: gold