



the
POWER
of
JAVA™



Building Secure and Trusted Web Services Using Project Tango



Kumar Jayanti, Jiandong Guo, Venugopal K

Sun Microsystems, Inc.

www.sun.com

TS-3473

Copyright © 2006, Sun Microsystems Inc., All rights reserved.

2006 JavaOneSM Conference | Session TS-3473 |

java.sun.com/javaone/sf

Goal of the Talk

Learn how to build Secure Web Services
using Project Tango (WSIT)

Agenda

Security in Web Services

Trust, SecureConversation and
SecurityPolicy

Security With WSIT NetBeans™ Module

A Sample Scenario

Future RoadMap

Q&A

Agenda

Security in Web Services

Trust, SecureConversation and
SecurityPolicy

Security With WSIT NetBeans™ Module

A Sample Scenario

Future RoadMap

Q&A

Security in Web Services

Some terms

- Integrity: Was it altered before I got it?
- Confidentiality: Only visible to intended recipient ?
- Authentication: Are you who you say you are?
- Non-repudiation: Can you claim you didn't send it even if you really did?
- Authorization: Are you allowed to have it?
- Auditing: Can I prove what happened?
- Trust: Do I trust you?

Security in Web Services (Nature of XML Web Services)

- Point of interaction is more over the internet, (coupled with Open Standards and Human Readable Data)
- Interaction between partners with no previously established relationship
- Program to program interaction (as opposed to human to program interaction)
- Message Processing Intermediaries
 - The original author wrote the payload, but many intermediate senders may touch the message

Security in Web Services

- Securing Web Services with SSL/HTTPS
 - Point-to-point encrypted communication with known trusted parties
 - Authentication of the parties and confidentiality of the data in motion
 - Not granular enough: it encrypts everything
 - Retaining cryptographically secured Identity end-to-end?
 - Other transports for Web Services?

Security in Web Services

- Standards for Web Services security
 - The pace of application and service creation is increasing
 - How can we make it easier for developers to add high quality security features
 - Not just Application level integration but infrastructure integration
 - Web services security infrastructure can take advantage of XML's granularity
 - Encrypting or signing selected portions
 - Hardware appliances could accelerate these functions

Security in Web Services

- OASIS Web Services Security Version 1.1
 - Security metadata in SOAP Header
 - Does not address
 - Policy
 - Protocols/mechanisms for establishing trust
 - Notion of a secure session
- Security-related applications can themselves become web services
 - Providers of security, identity (security token services)

Agenda

Security in Web Services

**Trust, SecureConversation and
SecurityPolicy**

Security With WSIT NetBeans Module

A Sample Scenario

Future RoadMap

Q&A

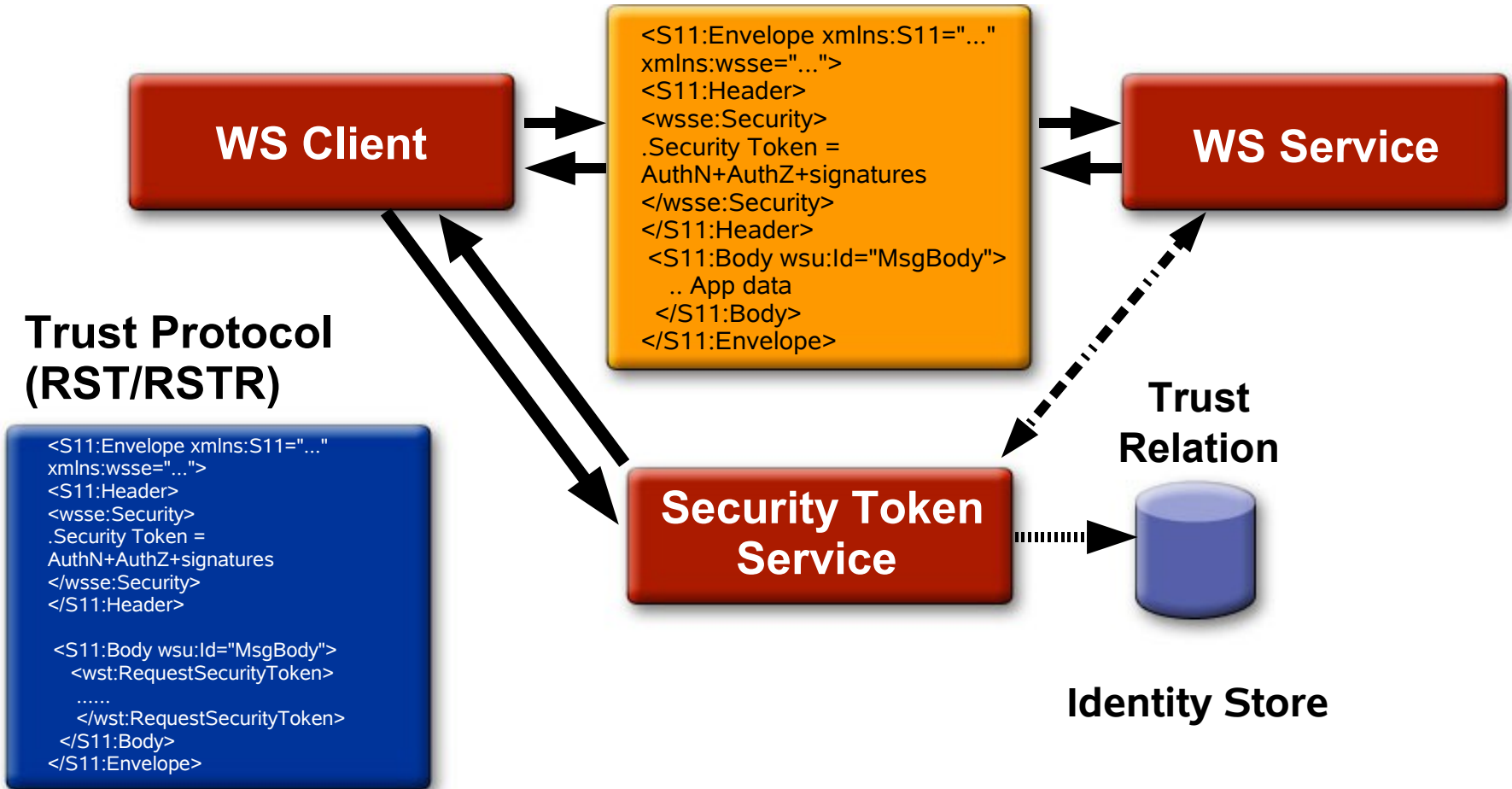
WS Trust

- A security token contains assertions about user identities, attributes and credentials
- A protocol framework for establishing and accessing Security Token Service as a trust authority for issuing, renewing, canceling and validating security tokens
- Mechanism for brokering and assessing the presence of trust relationship
- Built on the general framework of WS-Security
- Implementation based on specification draft, 02/2005
- Standard being developed in OASIS WS-SX committee

WS Trust

- Support issuance of security tokens
- Integrated with WS-Security and WS-SecurityPolicy
- Provide a framework for building Security Token Services
- Leverage Sun Java™ System Access Manager and Federation Manager to provide a concrete Security Token Service as Identity Provider in Web Services for authentication, access control, token issuance, single sign on, etc.

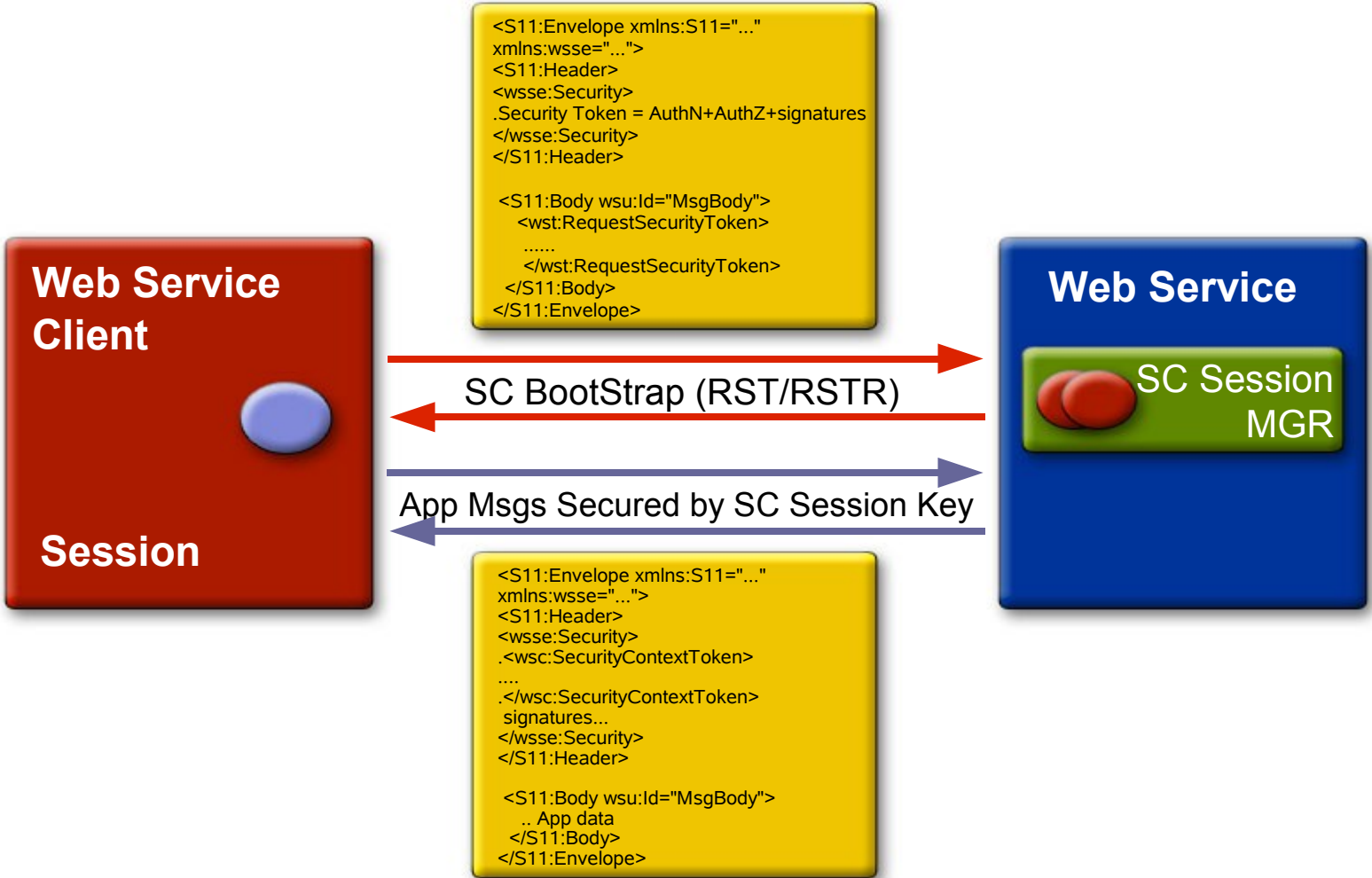
WS Trust



WS Secure Conversation

- Issues with WS-Security with multiple messages exchange
 - Performance
 - Security
- Define security session in terms of a security context and Key Derivation mechanism
- Security Context refers to an authentication state and negotiated keys for signing and encrypting keys
- The session concept is similar to SSL, IPSec, etc.
- Implementation based on the specification draft, 02/2005
- Standard being developed in the OASIS WS-SX TC

WS Secure Conversation (Cont.)



WS Secure Conversation (Cont.)

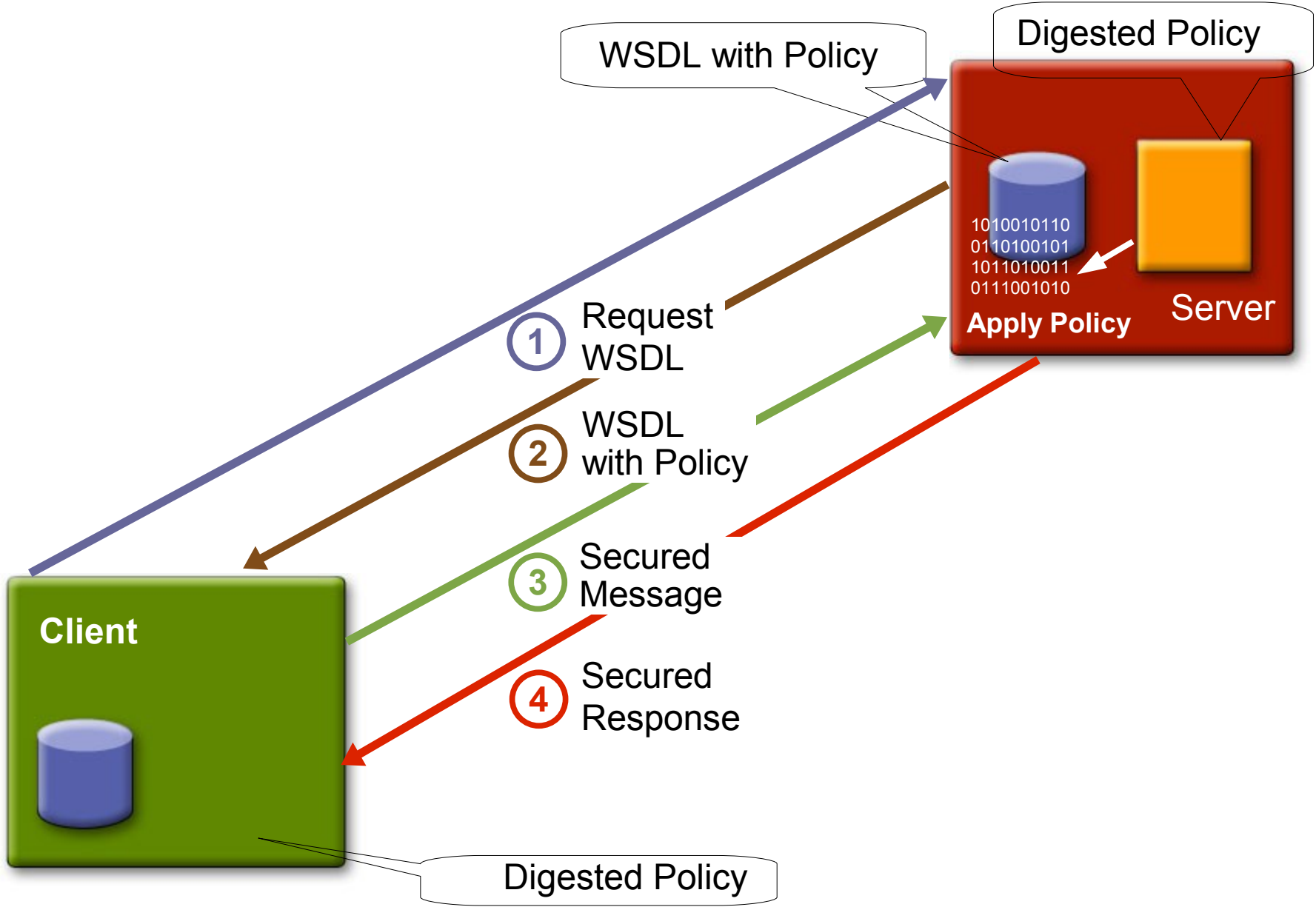
- Three components:
 1. Security Context Token represents a Security Context
 2. Establishing and managing the security context based on the WS-Trust framework
 3. Key derivation mechanism
- Support Security Context Token issuance and cancellation

WS Security Policy

- Security, Trust and SecureConversation expressed using assertions
- WS SecurityPolicy July 2005 Ver 1.1 editorial draft
- Advantages
 - Service governs and publishes security requirements
 - Conveys security features supported by the service
 - Enables interoperability

WS Security Policy

- WS Security Assertions
 - Binding assertions
 - Protection assertions
 - Token assertions
 - Supporting tokens
 - (Signed/Endorsing/SignedEndorsing)SupportingTokens
- WSIT Security Configuration
 - Keystores, CallbackHandlers, Validators



Agenda

Security in Web Services

Trust, SecureConversation and
SecurityPolicy

Security With WSIT NetBeans Module

A Sample Scenario

Future RoadMap

Q&A

DEMO

NetBeans IDE Tooling Support



Agenda

Security in Web Services

Trust, SecureConversation and
SecurityPolicy

Security With WSIT NetBeans Module

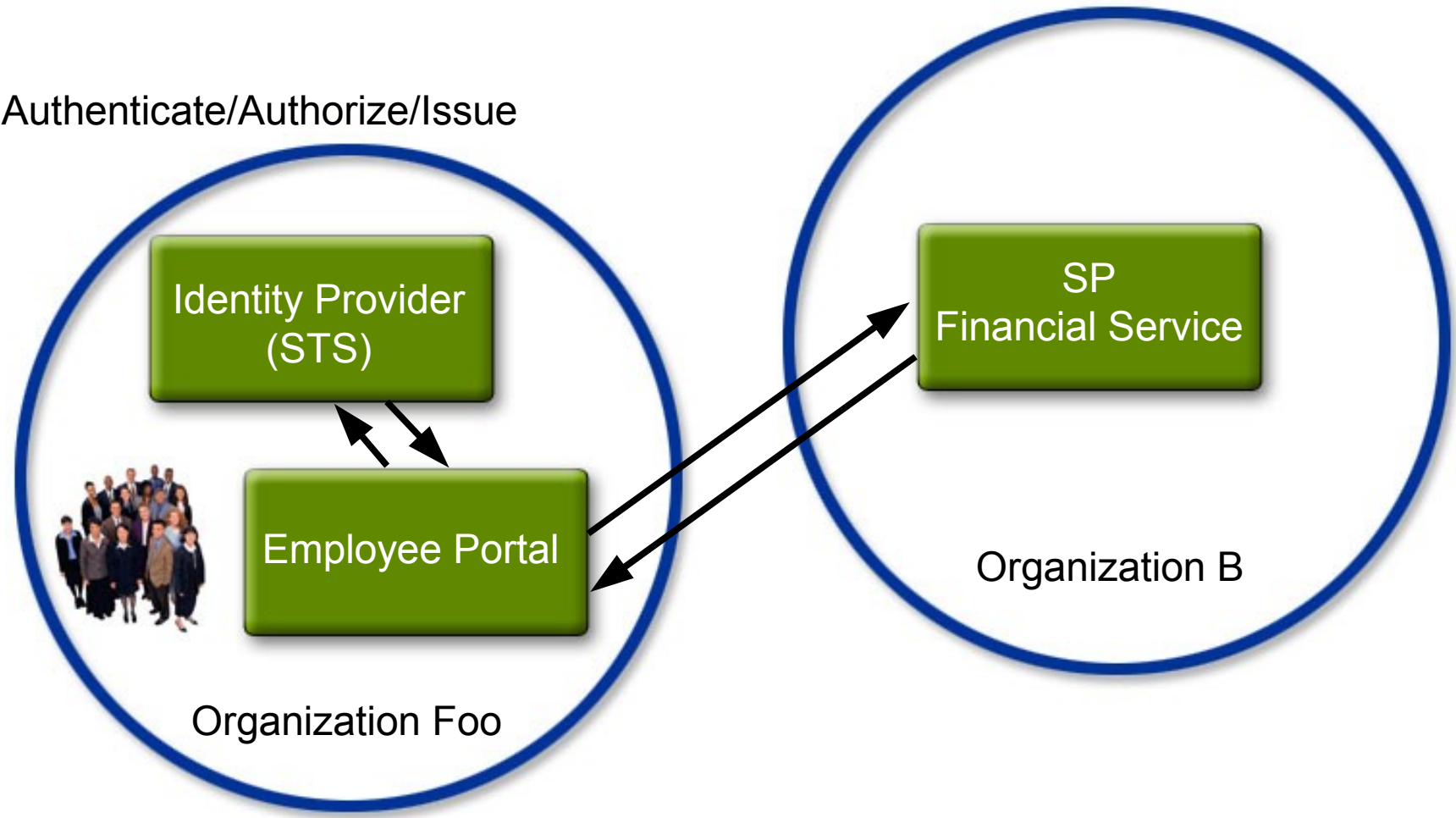
A Sample Scenario

Future RoadMap

Q&A

Demo Scenario

Authenticate/Authorize/Issue



DEMO

Scenario



Agenda

Security in Web Services

Trust, SecureConversation and
SecurityPolicy

Security With WSIT NetBeans Module

A Sample Scenario

Future RoadMap

Q&A

Where We Are Today...

- Open Source (wsit.dev.java.net)
 - Community centered around the Project GlassFishSM community
- Sun's next generation Web Services technology
- Interoperable with Microsoft Indigo (WCF)
- No change in JAX-WS Programming Model
 - Big leap from where we were 8 months ago
- WSIT NetBeans IDE for development, configuration and deployment
- WS-SX support

Future RoadMap

- Delivered into Project GlassFish (Sun Java System AS 9.1)
- Delivered into Java Enterprise System
- First class interoperability between Sun's Java Products and Windows Operating environments supporting WCF*
- Stateful Security Session and using security context in web farms
- Optimized runtime
- Integration with Sun Java System Access Manager and Federation Manager products and SAML 2.0 tokens

Call To Action

- Test Drive Web Services Interoperability
java.sun.com/webservices/interop
- WSIT (whiz-it): Download! Contribute!
wsit.dev.java.net
- Get the FREE Project GlassFish Open Source Application Server
java.sun.com/javaee/glassfish
- Download NetBeans IDE
websvc.netbeans.org/wsit
- Visit 'The Aquarium'—Virtual watercooler for WSIT and Project GlassFish
Blogs.sun.com/theaquarium

Q&A

<code />

Thank You





the
POWER
of
JAVA™



JavaOne
Part of the Network for Business Success

Building Secure and Trusted Web Services Using Project Tango



Kumar Jayanti, Jiandong Guo, Venugopal K

Sun Microsystems, Inc.

www.sun.com

TS-3473