# Security Architecture for Open Grid Services

# Overview

- Grid Security challenges
- Categorizing the Grid Security
- Web services security roadmap
- Building blocks
- Summary

# Grid Security Challenges

- Heterogeneous Distributed Environment
- Federated Security
  - Virtual Organizations
  - Federated Identity
  - Federated Trust
- End-to-end security
  - Multi-hop scenarios - multiple (un)trusted intermediaries
  - Security in hosting environment and its effect on the Grid
- Dynamic interactions
  - Dynamic policies, grouping, authorization, etc
- Support for multiple security mechanisms
- User driven service deployment and management

# Categorizing Security

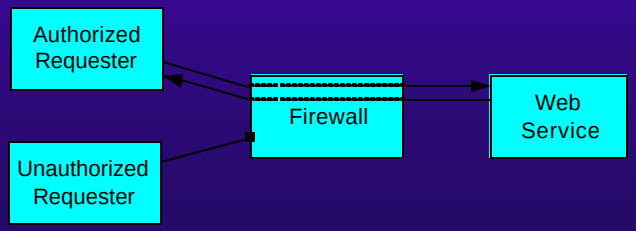
- Securing Grid Services
  - Credential/Identity Propagation
  - Policy
  - Integrity
  - Confidentiality
  - Authorization
  - Privacy
  - VO policies
- Grid Security Services
  - Identity Mapping
  - Authentication or Identity Service
  - Authorization
  - Profile/Wallet
  - Audit

# Web Services Security Roadmap

- IBM-Microsoft joint proposal (announced: April 11th; OASIS – June 27th)
- The roadmap presents our strategy for addressing security issues within a Web Services environment.
- It consists of one defined specification (WS-Security) and several planned composable specifications along with example scenarios.
- The proposed specifications build upon foundational technologies such as SOAP, WSDL, XML Digital Signatures, XML Encryption and SSL/TLS.
- This is the first Web services security model that brings together formerly incompatible security technologies such as public key infrastructure, Kerberos, and others.

# Scenarios

- To make the issues and solutions discussed in the roadmap as concrete as possible, several scenarios that reflect current and anticipated applications of web services.




- Direct Trust using Username/Password and Transport-Level Security
- Direct Trust using Security Tokens
- Security Token Acquisition
- Firewall Processing
- Issued Security Token
- Enforcing Business Policy
- Privacy
- Smart Clients
- Web Clients
- Mobile Clients
- Enabling Federation
- Validation Service
- Supporting Delegation
- Access Control
- Auditing

# Current/proposed specs

## Building on the SOAP Foundation


Today: describes SOA
extensions for secure
messaging, provides
foundation for other
building blocks

# WS-Security details

- Submitted to OASIS
- Enhancements to SOAP messaging
  - Provides quality of protection
  - Is a general purpose mechanism for associating security tokens with SOAP messages.
- Builds upon and interoperates with existing standards
  - SSL/TLS (transport)
  - IPSEC (network)
  - W3C XML Digital Signatures
  - W3C XML Encryption
- What is addressed?
  - Message integrity
  - Message confidentiality
  - Message authentication
  - Encoding security tokens
    - String subject names
    - Binary tokens
      - X.509 certs, Kerberos tickets
      - Other token formats (including XML-encoded tokens)
      - keys

# Current/proposed specs

## Building on the SOAP Foundation


Planned: will define how to express capabilities and constraints of securi policies

# Current/proposed specs

## Building on the SOAP Foundation


Planned: will describe the model for establishing both direct and brokered trust relationships (including third parties and intermediaries)

# Current/proposed specs

## Building on the SOAP Foundation


Planned: will be a model for how users state privacy preferences, and for how Web Services state and implement privacy practices

# Current/proposed specs

## Building on the SOAP Foundation

| | | |
|---|---|---|
| WS-Secure Conversation | | |
| WS-Policy | WS-Trust | WS-Privacy |
| WS-Security | | |
| SOAP Foundation | | |

Planned: will describe how to manage and authenticate message exchanges between parties including security context exchange and establishing and deriving session keys

# Current/proposed specs

## Building on the SOAP Foundation

| | | |
|---|---|---|
| WS-Secure Conversation | WS-Federation | |
| WS-Policy | WS-Trust | WS-Privacy |
| WS-Security | | |
| SOAP Foundation | | |

Planned: will describe how to manage and broker the trust relationships in a heterogeneous federated environment including support for federated identities

# Current/proposed specs

## Building on the SOAP Foundation

WS-Secure Conversation

WS-Federation

WS-Authorization

WS-Policy

WS-Trust

WS-Privacy

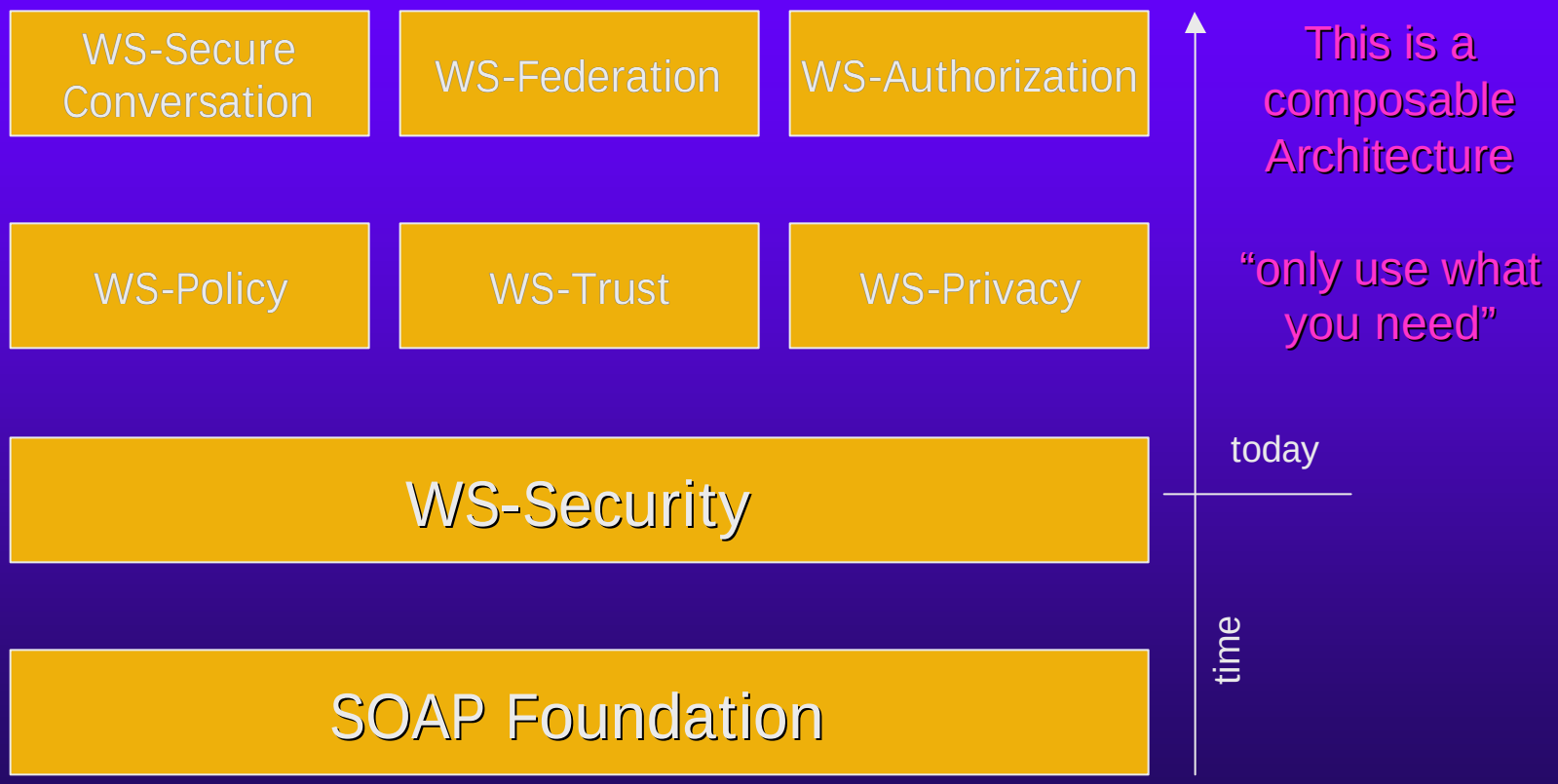
WS-Security

SOAP Foundation

Planned: will define how Web services manage authorization data and policies

# Current/proposed specs

## Building on the SOAP Foundation




This is a composable Architecture

"only use what you need"

# OGSA Security Components

Intrusion Detection

Anti-virus Management

Policy Management (authorization, privacy, federation, etc)

User Management

Key Management

Secure Conversations

**Credential and Identity Translation** (Single SignOn)

Access Control Enforcement

**Audit & Non-repudiation**

Service/End-point Policy

Mapping Rules

Authorization Policy

Privacy Policy

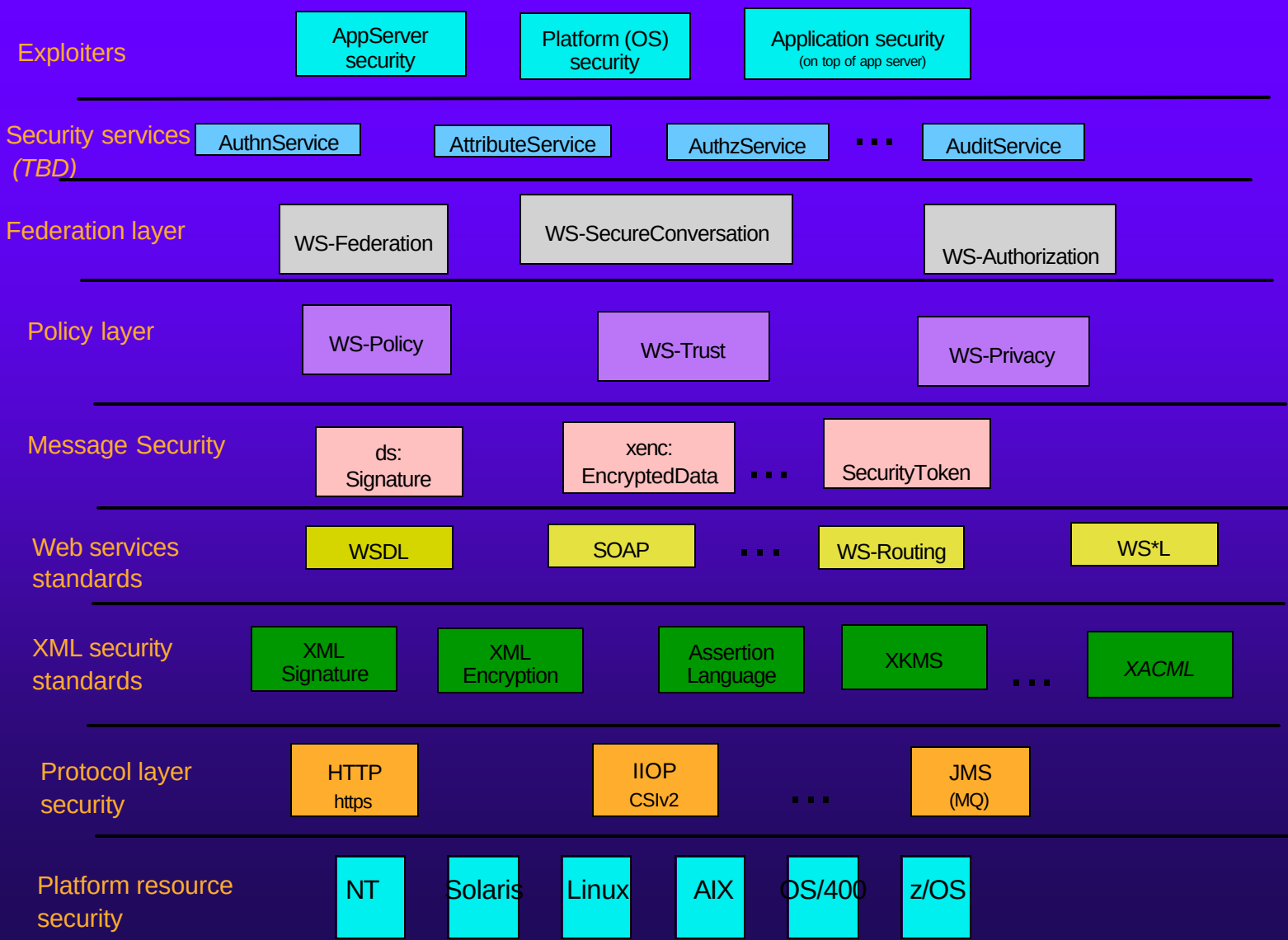
Policy Expression and Exchange

Bindings Security
(transport, protocol, message security)

Trust Model

Secure Logging

# Building Blocks



# Sample Scenario

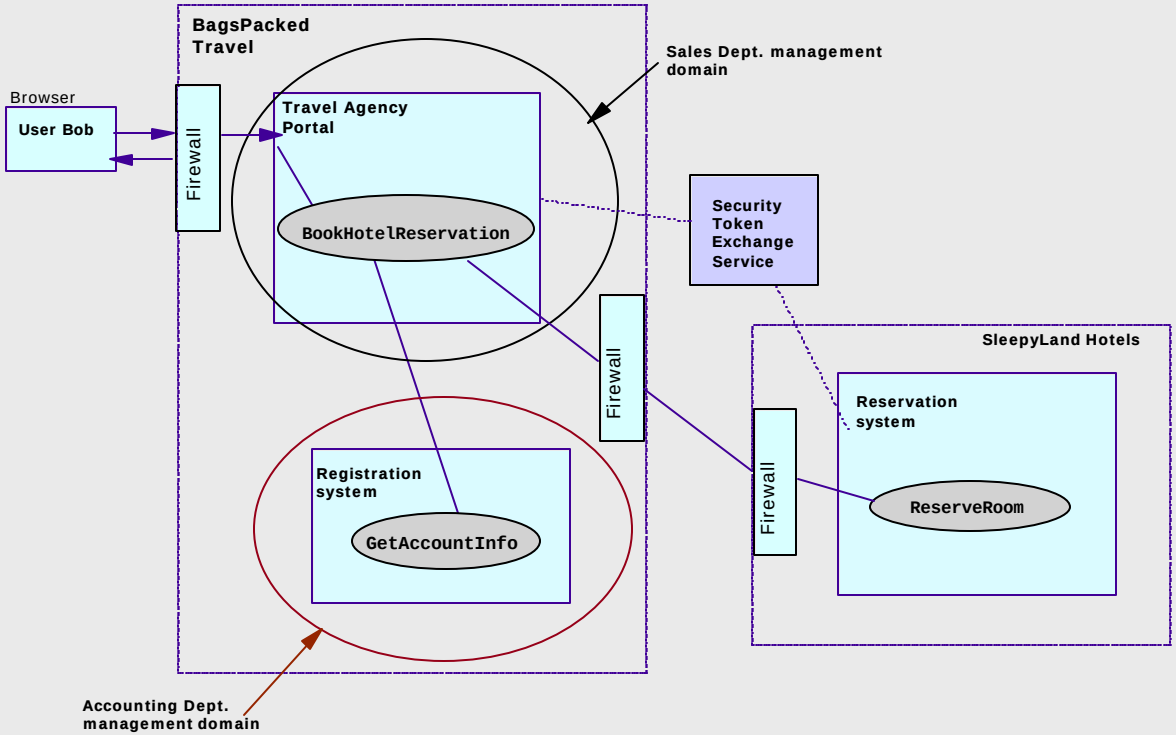



Figure 5: Service requests across virtual organizations

# Security Documents

- Proposed drafts
- Security Architecture for Open Grid Services
  - Capture high level requirements, components for OGSA Security
- OGSA Security Roadmap
  - Formulate requirements into specifications that need to be worked on
- Posted in http://www.globus.org/ogsa/Security

# Summary

- Securing Grid Services
  - Web services security roadmap
  - Grid security requirements
- OGSA Security
  - Architecture document
  - Roadmap document
  - GGF Workgroups