IBM SOA Executive Summit

Moving Ahead With SOA

SOA Security Management

Venkat Raghavan

SOA on your terms and our expertise

ON DEMAND BUSINESS™

Agenda

1. Context for SOA Security Management
2. Current Security Models for Composite Applications
3. Security as Services – shift to Service-centric Security
4. Products and Offerings

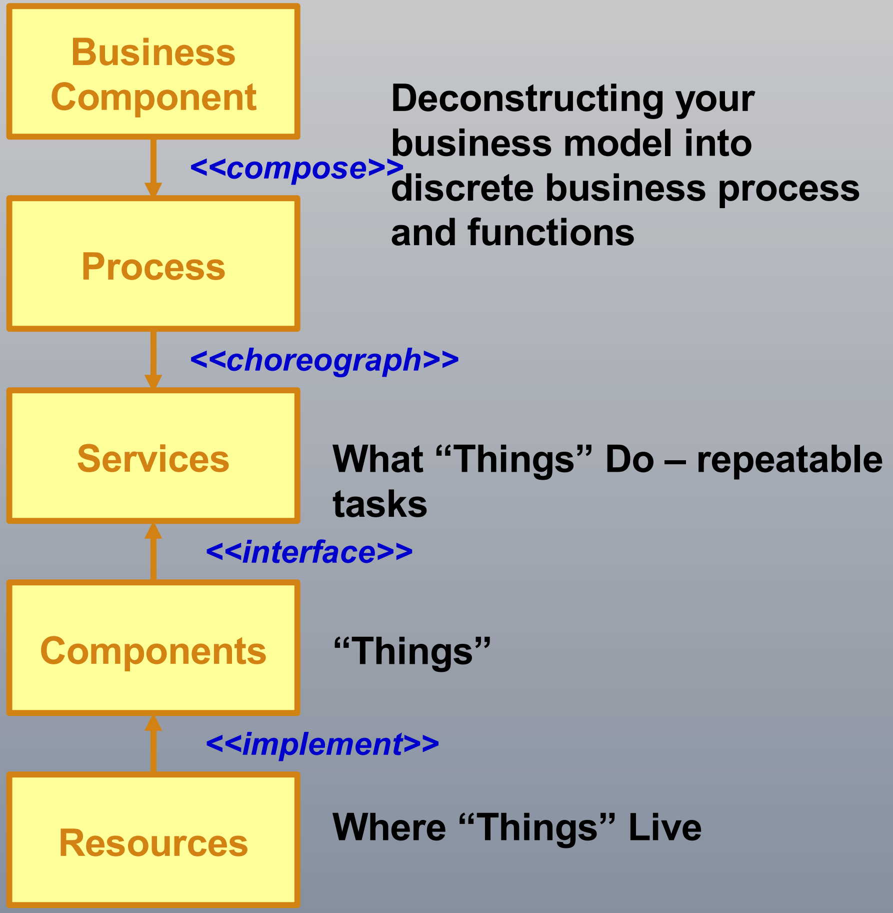
Defining Service Oriented Architecture

Different Things to Different People

	Roles
A *model of the business* that is based on services as the base functional component	**Business**
An *architectural style* which requires a service provider, requestor and a service description. It addresses characteristics such as loose coupling, reuse and simple and composite implementations.	**Architecture**
A *programming model* complete with standards, tools, methods and technologies such as Web services	**Implementation**
A *set of agreements* that specify quality of service and drive key business and IT metrics.	**Operations**

Examples of “Services”

- Business Process Services (composite services):
  - createSalesOrder
  - reconcileAccount
- Business Transaction Services:
  - checkOrderAvailability
  - createBillingRecord
- Business Function Services:
  - calculateDollarValueFromYen
  - getStockPrice
- Technical Function Services:
  - auditEvent
  - checkUserAuthorization



Deconstructing your business model into discrete business process and functions

What “Things” Do – repeatable tasks

“Things”

Where “Things” Live

Context for SOA – Insurance Company scenario

- Specializing in Auto insurance –product expansion to offer automobile, home, life and Identity Theft insurance
- Using new brokers to cross-sell – goal is to sell to 20% of its existing customer base these new insurance products over 3 years
- Sales through multiple-channels - phone-based, Web, new reseller and distributor channels using a new CRM system
- Improve Service levels for multi-product customers – flexible pricing, discounts
- Reduce costs by shifting lot of the F2F customer processes to Web-based self-service – catalogs, plan selection, enrollment and billing

- Products – Home, Auto and Life
- People – Customers, Resellers, Brokers, Call center reps
- Federation of Brokers
- User to Service Relationships & Data
- Governance – Are we executing against out business objectives?

SOA Security Context: SOA will require a shift from Resource-centric security to securing end to end Services

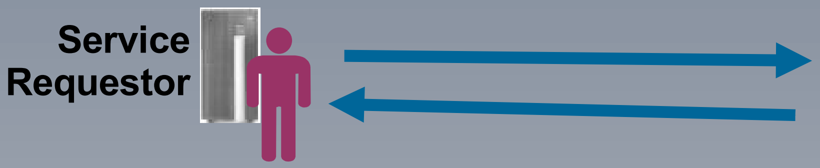
Common Security Questions in an SOA context?

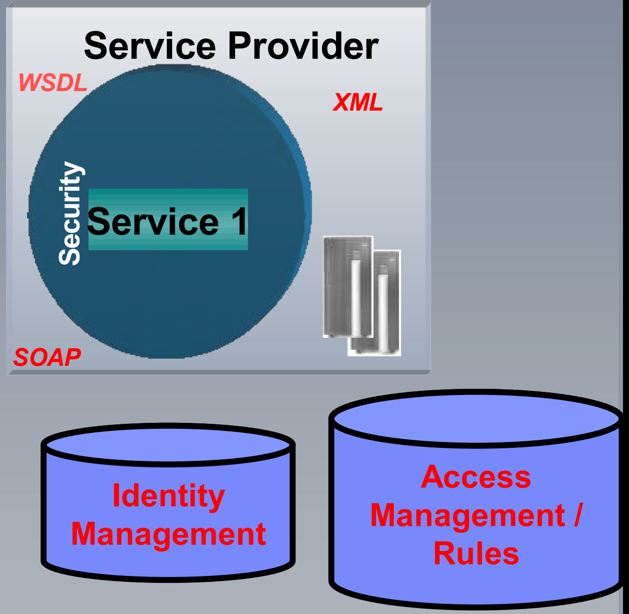
- How do we provision access rights and entitlements to SOA services?
- How do services **“identify”** and “authenticate” Users ?
- How do services enforce access control – Gold vs. Platinum ?
- How do services **associate** user or identity context?
- How do services enforce user specific rules to services across multiple channels ?
- How do we implement role-based access to services ? (Portal Context)
- How can we protect Service integrity by detecting & preventing **unauthorized changes**?
- How do we integrate SOA security with new Application components: Message Broker, Process Servers across vendor solutions ?
- How can we deliver end-to-end security, transactional audit and compliance for services?

Major Insurance Company Scenario

- Consumers
- Resellers
- Brokers
- Employees
- Call Center Reps

A Service will need all Aspects of Security & Compliance





Runtime

- User Identification, Service Identification
- User Authentication, Service Authentication
- Role-based Access to Service
- User Authorization
- Auditing & Compliance

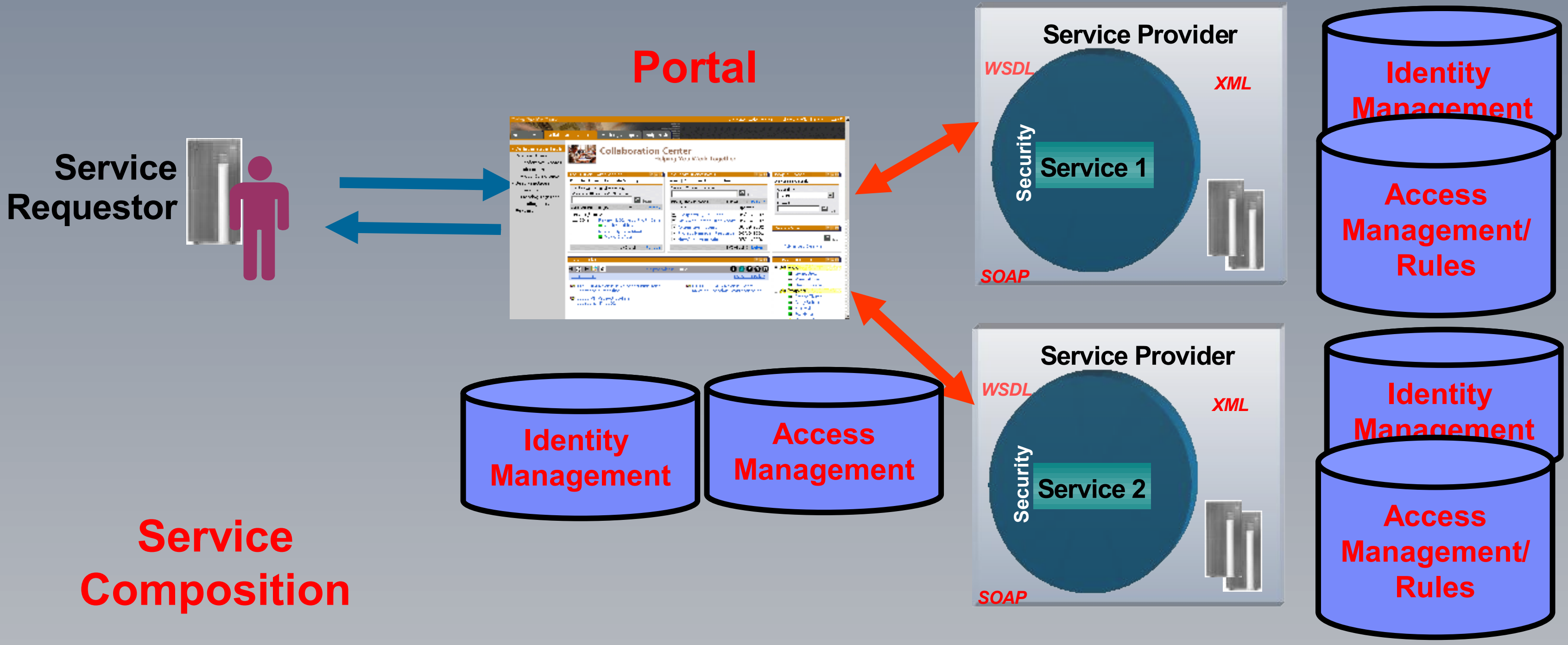
Management

- User-Service Provisioning
- Federated Identity Management
- Policy Management & Administration

Challenges

- Multiple User Registries
- Multiple Security Domains
- Multiple Application Platforms
- Multiple Protocols: HTTP, SOAP, MQ, JMS, SMS, MMS, SIP
- Security Mediations / Enforcement Points: DMZ, Web Container, App Container, ESB, Process Server
- Confidentiality, Integrity and Availability

Service Composition – Security Challenges in composing Services



Technical Challenges

- Multiple User Registries
- Multiple Security Domains
- Multiple Application Platforms
- Multiple Protocols: HTTP, SOAP, MQ, JMS, SMS, MMS, SIP
- Security Mediations / Enforcement Points: DMZ, Web Container, App Container, ESB, Process Server
- Confidentiality, Integrity and Availability

Agenda

1. Context for SOA Security Management

3. Current Security Models for Composite Applications

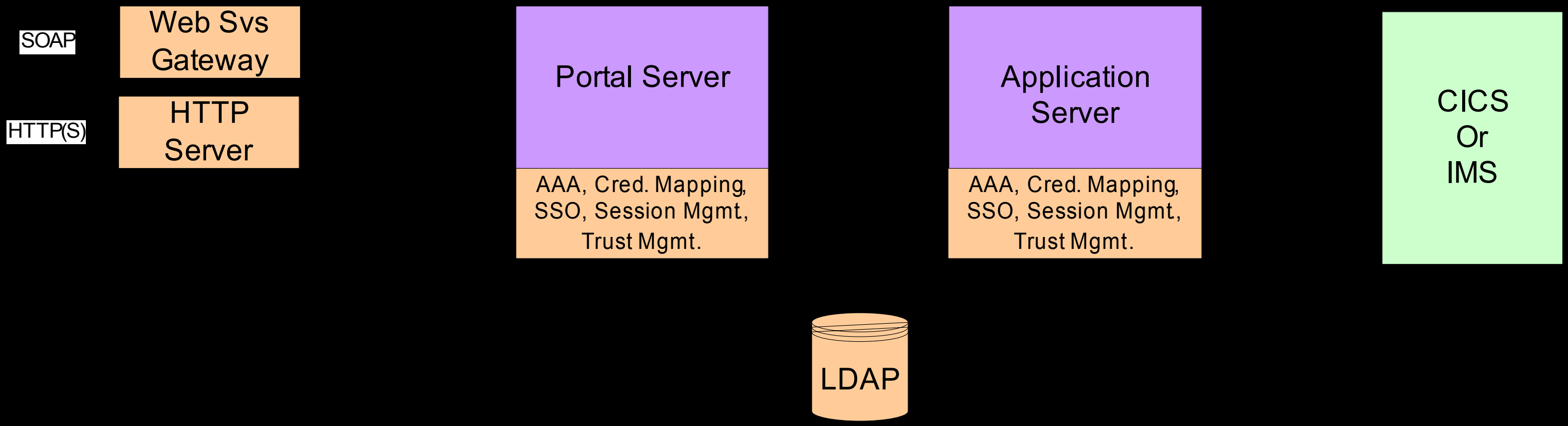
5. Security as Services – shift to Service-centric Security
6. Products and Offerings

Components of Application Security

- Authentication
- Authorization
- XML Threat Protection
- Auditing
- Single Sign-On
- Session Management
- Credential Management
- Trust Management

Tivoli Access Manager

DataPower XS40



SOAP

Web Svs Gateway

HTTP(S)

HTTP Server

Portal Server

AAA, Cred. Mapping, SSO, Session Mgmt, Trust Mgmt.

Application Server

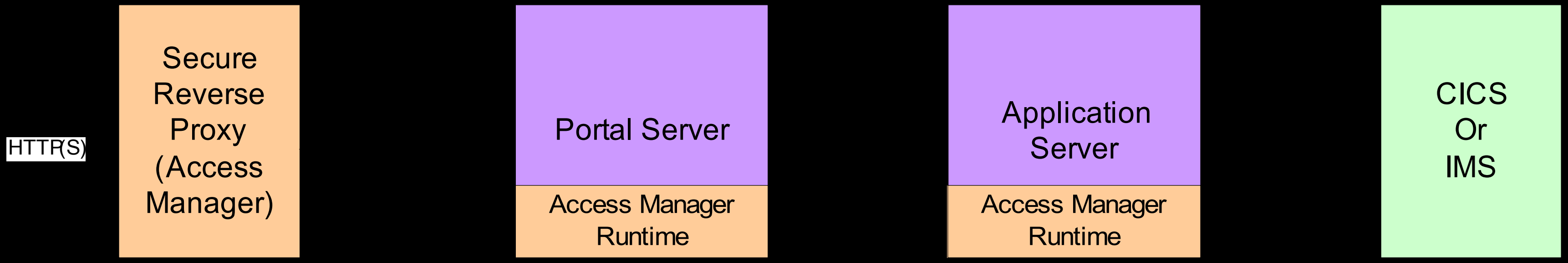
AAA, Cred. Mapping, SSO, Session Mgmt, Trust Mgmt.

CICS Or IMS

LDAP

Authentication Services

External Authentication G/W
- Proxy architecture is predominantly used



HTTP(S)

Secure Reverse Proxy (Access Manager)

Portal Server

Access Manager Runtime

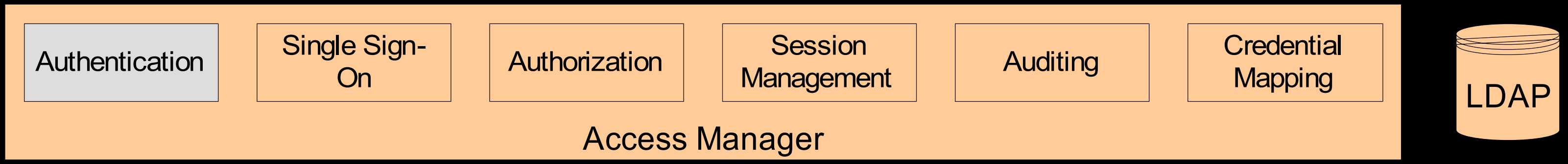
Application Server

Access Manager Runtime

CICS
Or
IMS

Container based Authentication
- JAAS LoginModule
- .NET Authentication Assembly

Programmatic Authentication
- TAM JAAS API (Java)
- TAM aznAPI (C)



Authentication

Single Sign-On

Authorization

Session Management

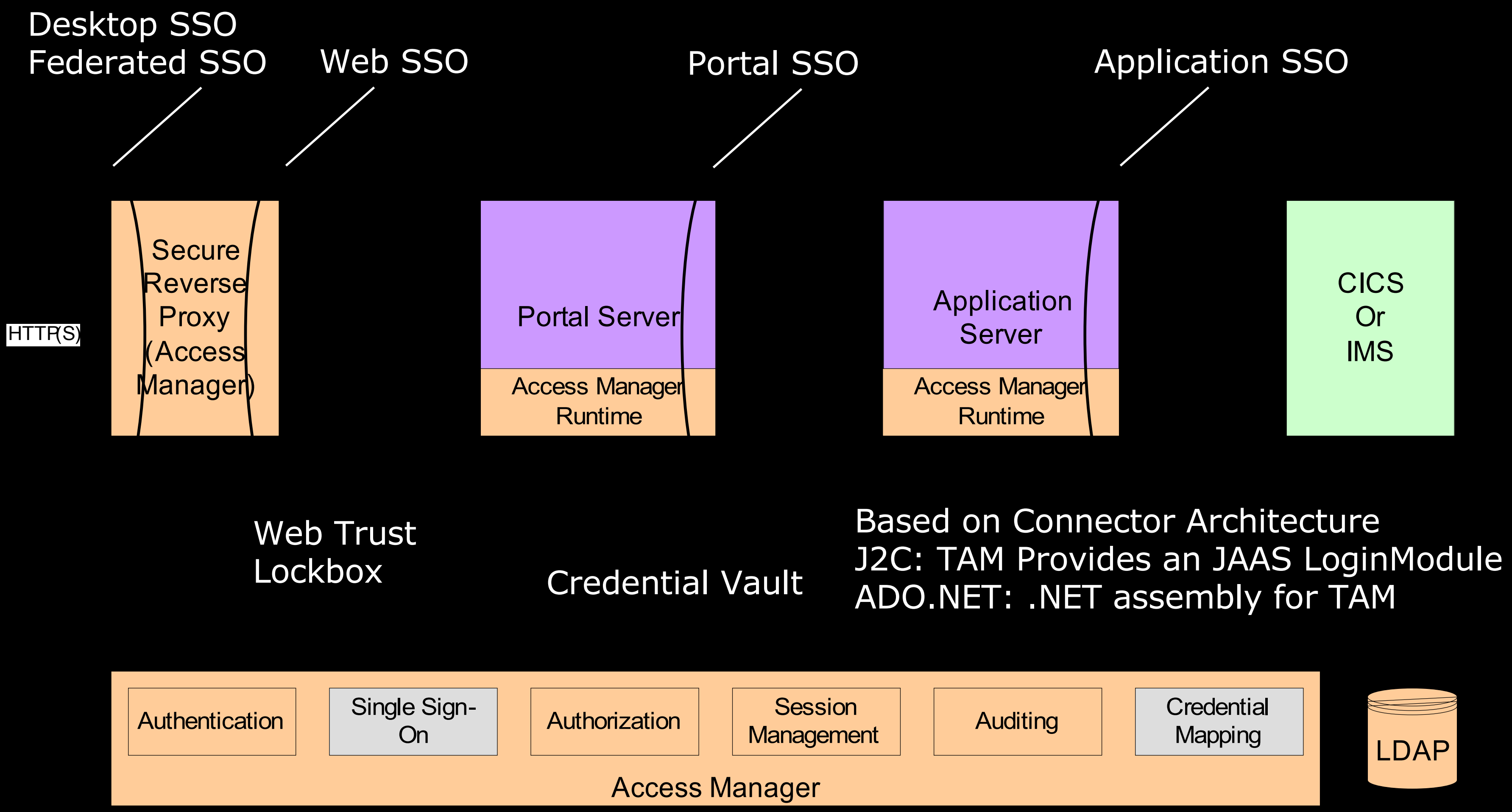
Auditing

Credential Mapping

Access Manager

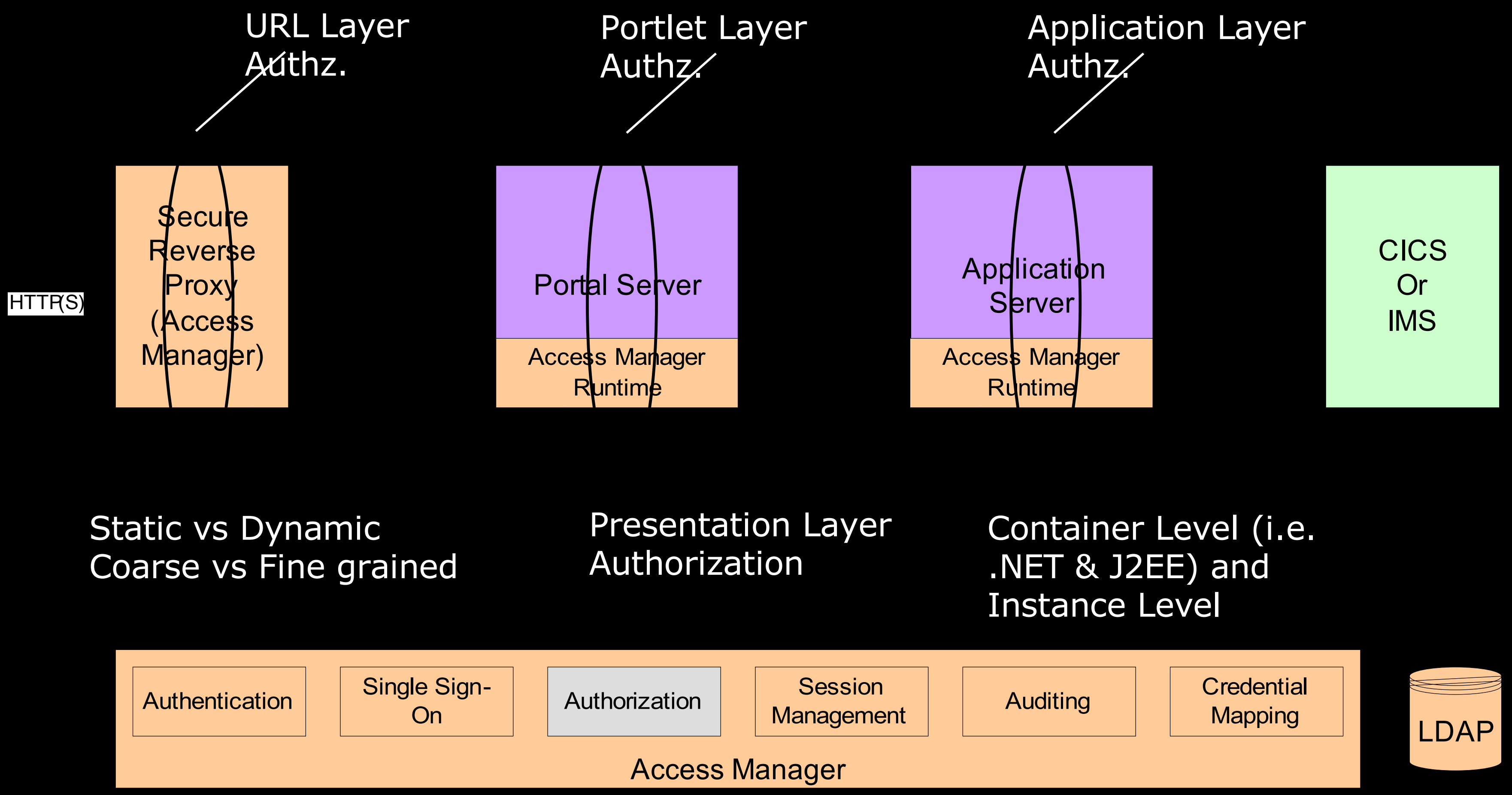
LDAP

Realms of Single Sign-On Services



Based on Connector Architecture
J2C: TAM Provides an JAAS LoginModule
ADO.NET: .NET assembly for TAM

Layers of Authorization Services



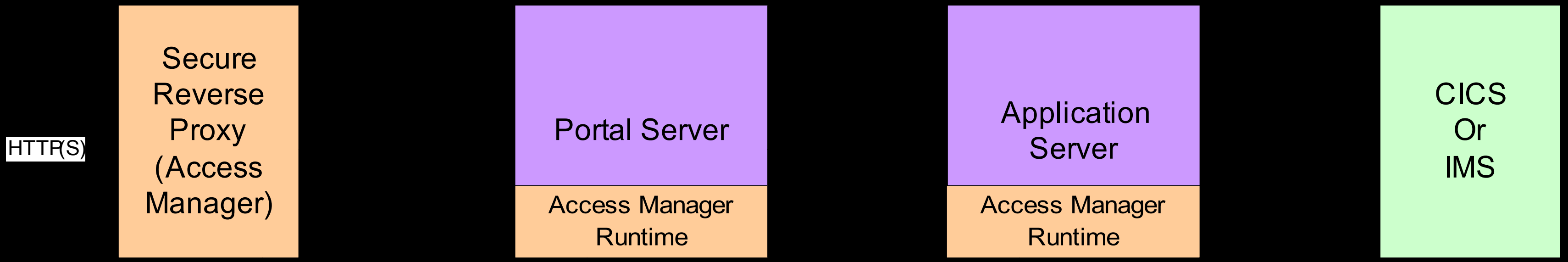
Static vs Dynamic
Coarse vs Fine grained

Presentation Layer Authorization

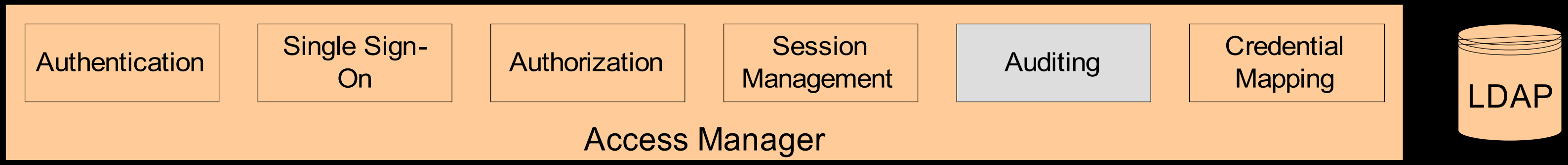
Container Level (i.e. .NET & J2EE) and Instance Level

Common Auditing and Reporting Services

Support for Consistent Reporting Capabilities
- Provides interfaces for custom report tables
- Choice of a reporting tool
- Facilitates cross-product audit reports



Support for Consistent Auditing
- Common Base Event (CBE) format auditable events
- Centralized collection point using Common Event Infrastructure (CEI)
- Consistent management of lifecycle of audit data



Agenda

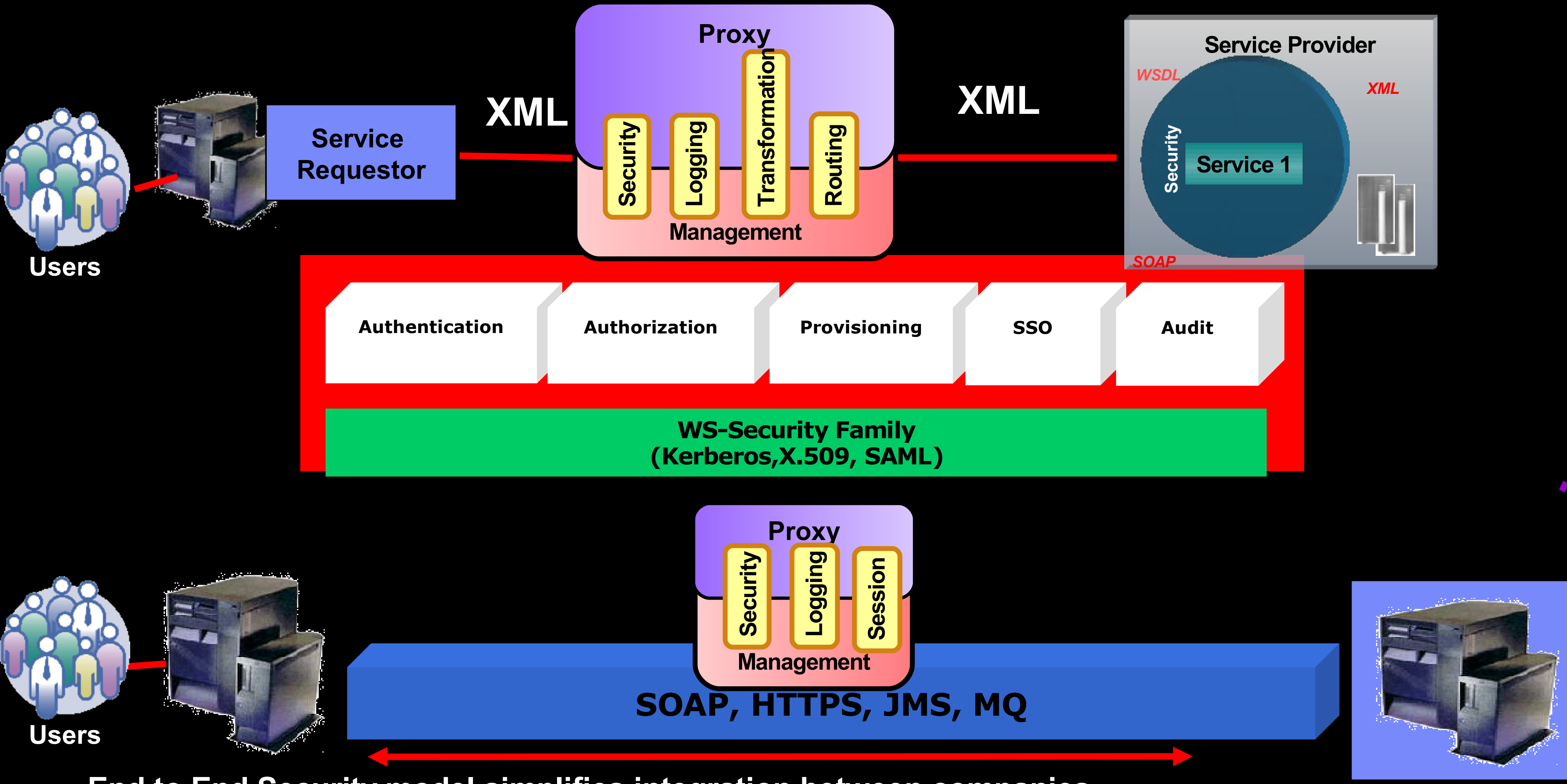
1. Context for SOA Security Management

3. Current Security Models for Composite Applications

5. Security as Services – shift to Service-centric Security

7. Products and Offerings

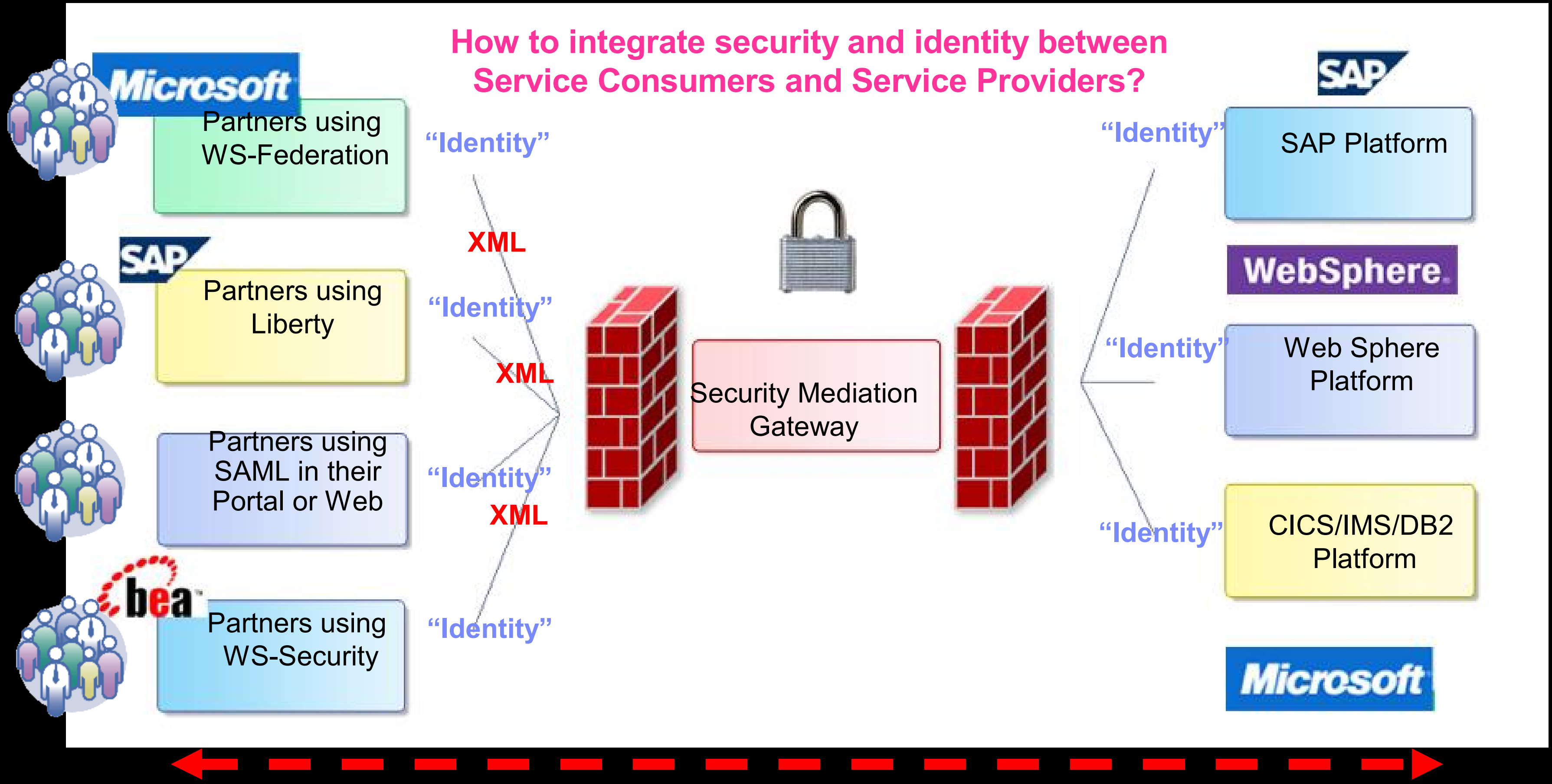
SOA Security – What's Changed ?



End to End Security model simplifies integration between companies

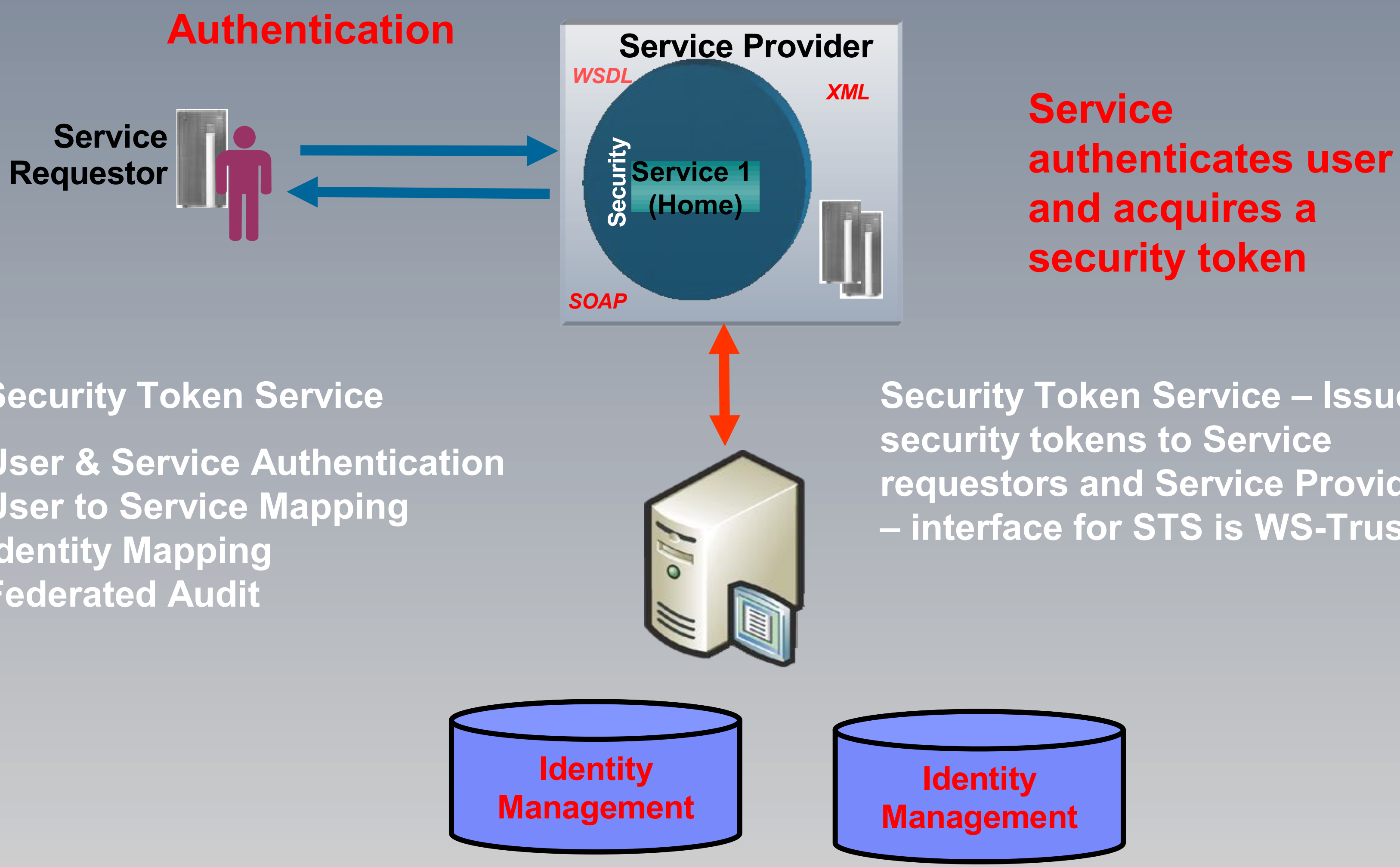
Each Web Services message can be individually authenticated, integrity & confidentiality protected and authorized

SOA - Security Mediation - XML and Federated Identity


How to integrate security and identity between Service Consumers and Service Providers?
Microsoft
Partners using WS-Federation
SAP
Partners using Liberty
Partners using SAML in their Portal or Web
bea
Partners using WS-Security
"Identity"
XML
"Identity"
XML
"Identity"
XML
"Identity"
Security Mediation Gateway
"Identity"
"Identity"
"Identity"
SAP
SAP Platform
WebSphere
Web Sphere Platform
CICS/IMS/DB2 Platform
Microsoft

Federated Identity management is a key business process enabler for SOA

Concept: Security Token Service



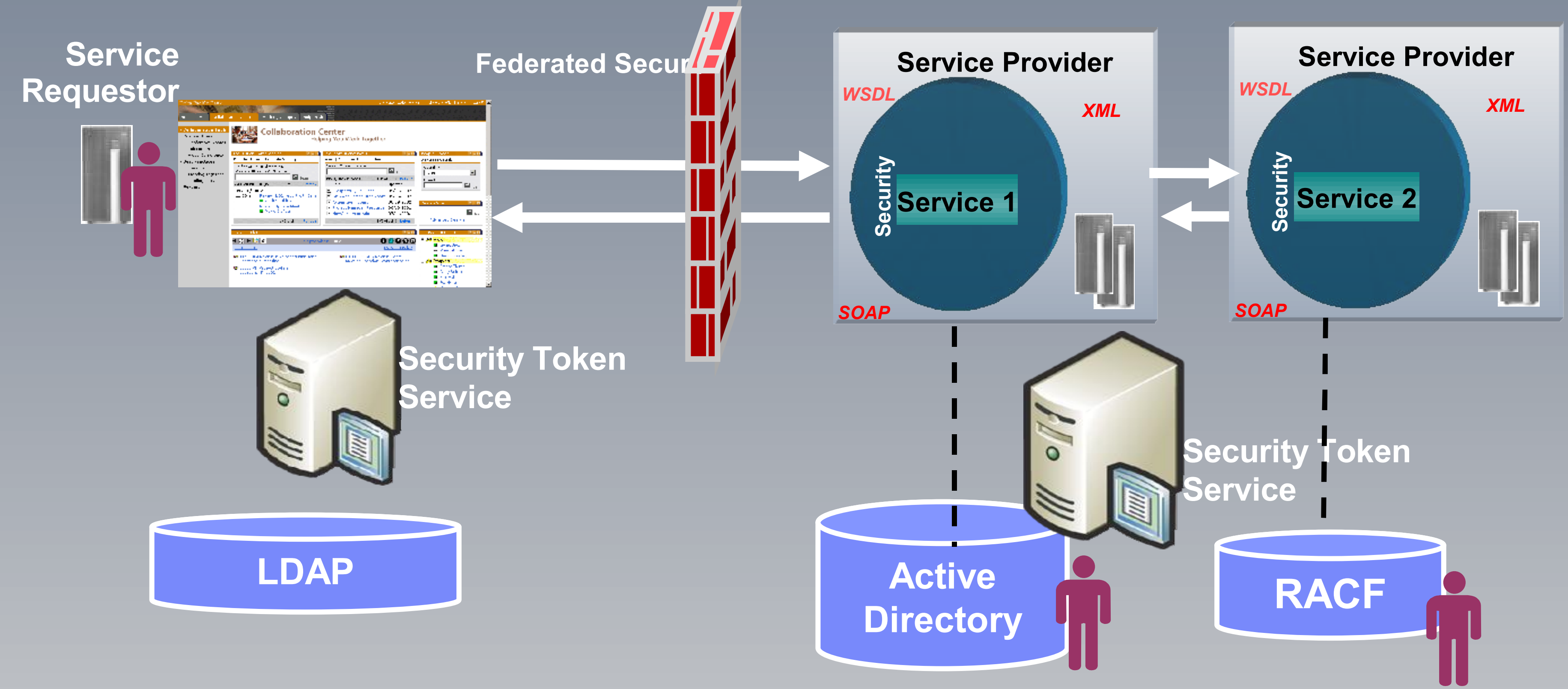
Service authenticates user and acquires a security token

Security Token Service

User & Service Authentication
User to Service Mapping
Identity Mapping
Federated Audit

Security Token Service – Issues security tokens to Service requestors and Service Providers – interface for STS is WS-Trust

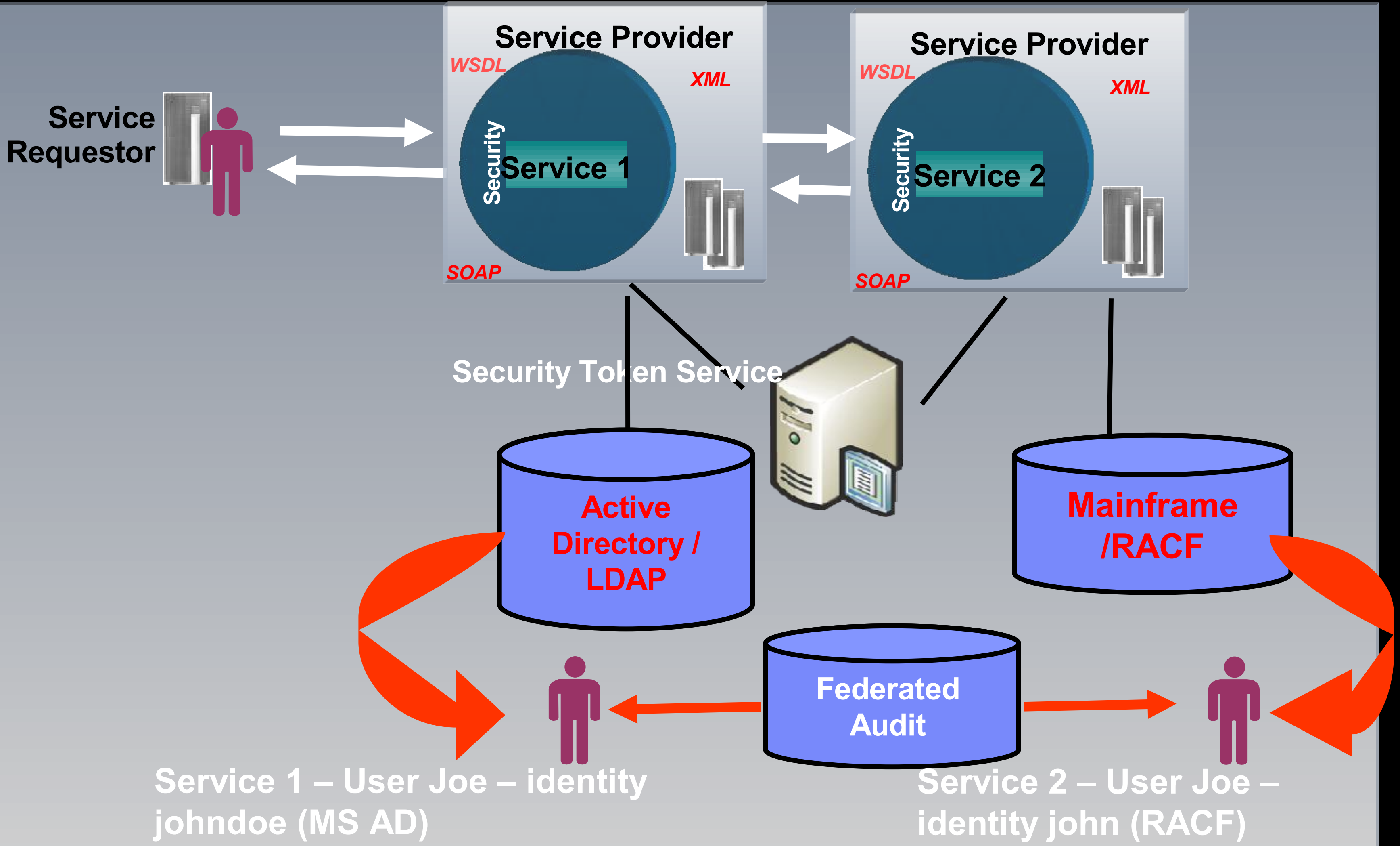
Concept: Federated Identity Management



1. User Signs On to Portal
2. Portal authenticates user credentials with LDAP Server
3. Service Requestor creates Security Token

1. Service 1 validates Token and maps identity to Sun Directory LDAP
2. Service 2 validates Token and maps to CICS/RACF

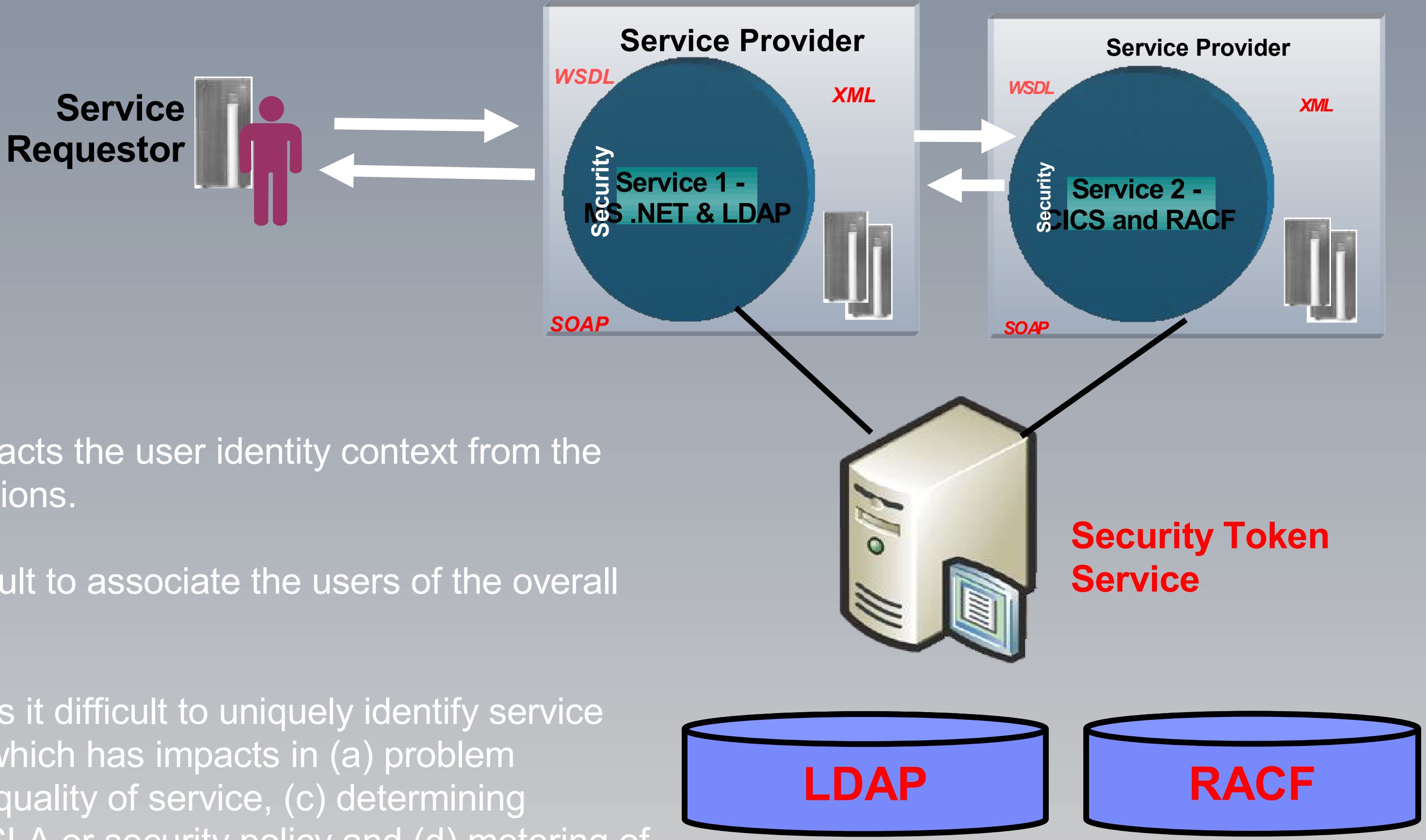
Concept: Federated Audit



Service 1 – User Joe – identity johndoe (MS AD)

Service 2 – User Joe – identity john (RACF)

Concept: Service to User Mapping

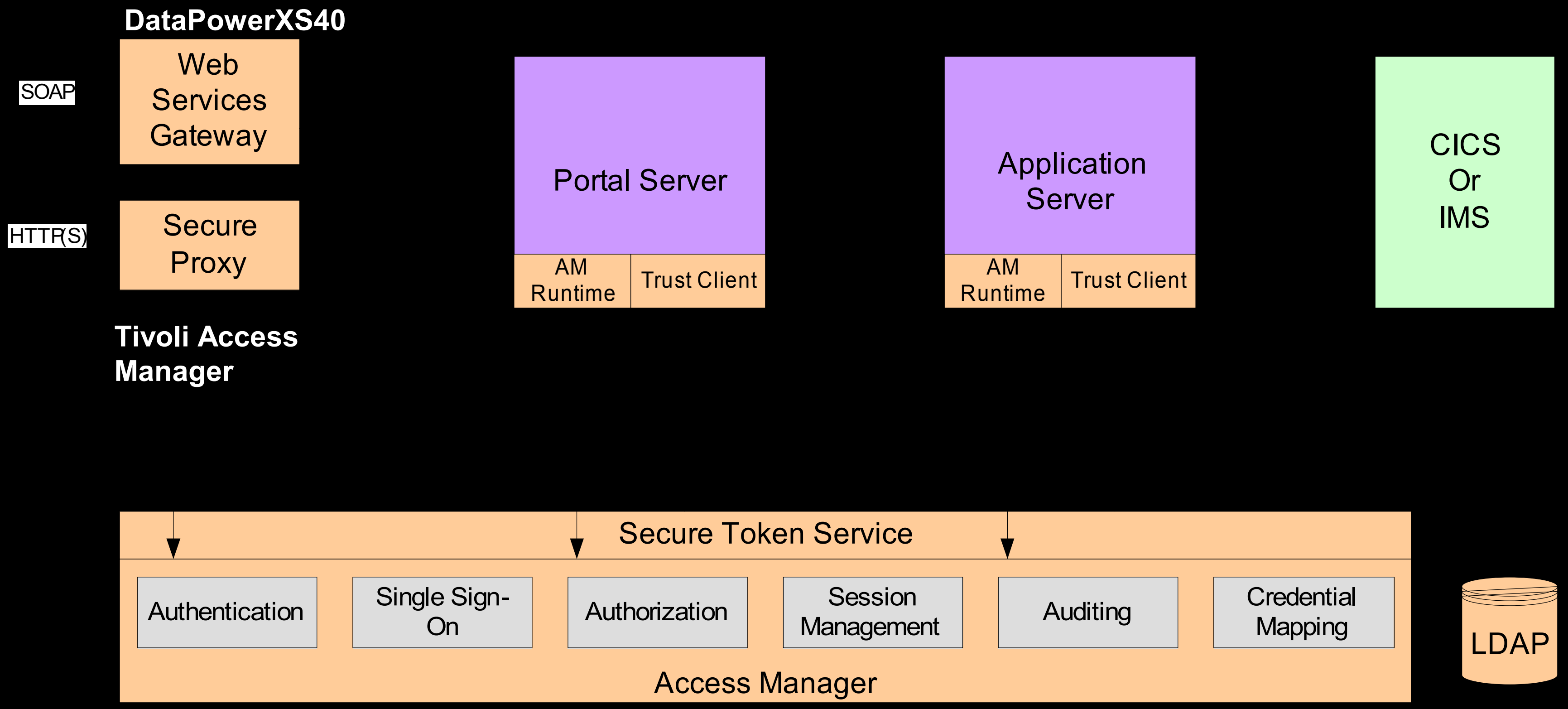


Each service abstracts the user identity context from the underlying applications.

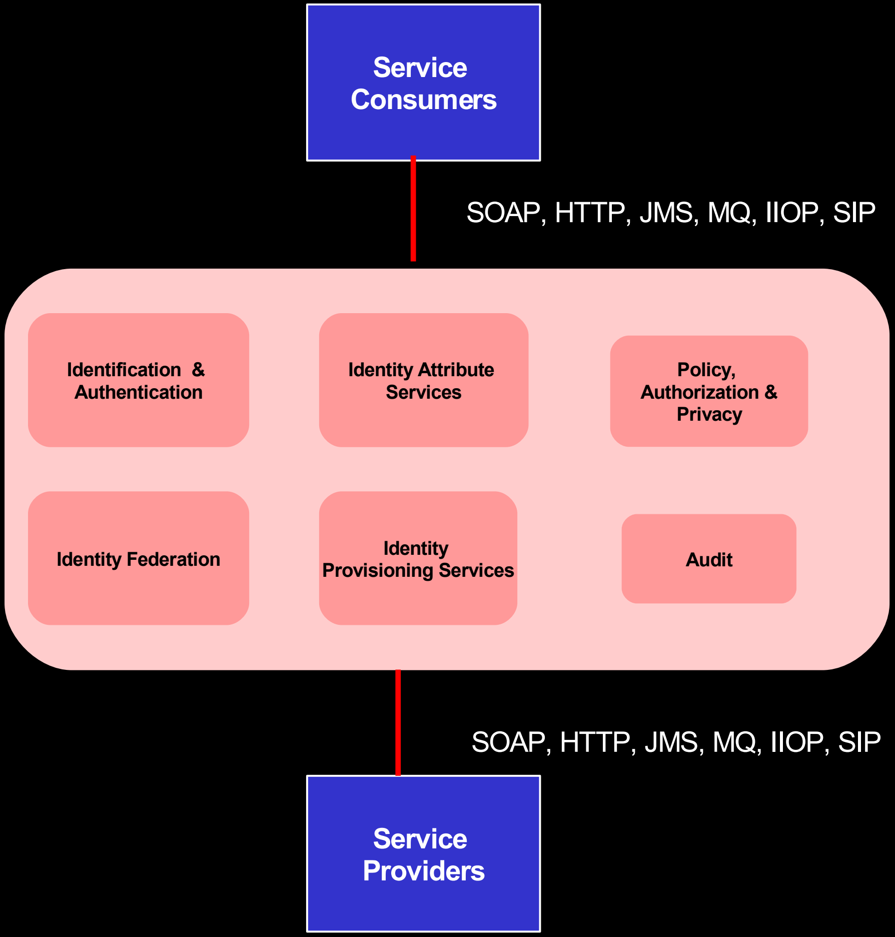
This makes it difficult to associate the users of the overall functionality.

This, in turn, makes it difficult to uniquely identify service calls or requests, which has impacts in (a) problem determination, (b) quality of service, (c) determining compliance to an SLA or security policy and (d) metering of service usage.

Application Security With Security Token Service



Security Services for SOA


Service Consumers
SOAP, HTTP, JMS, MQ, IIOP, SIP
Identification & Authentication
Identity Attribute Services
Policy, Authorization & Privacy
Identity Federation
Identity Provisioning Services
Audit
SOAP, HTTP, JMS, MQ, IIOP, SIP
Service Providers

Authentication: WS-Trust, WS-Security {Kerberos, SAML, PKI, SAF (RACF), LPTA}

Policy: XACML, WS-Policy – federates policies across Portal, ESB, Process Servers etc

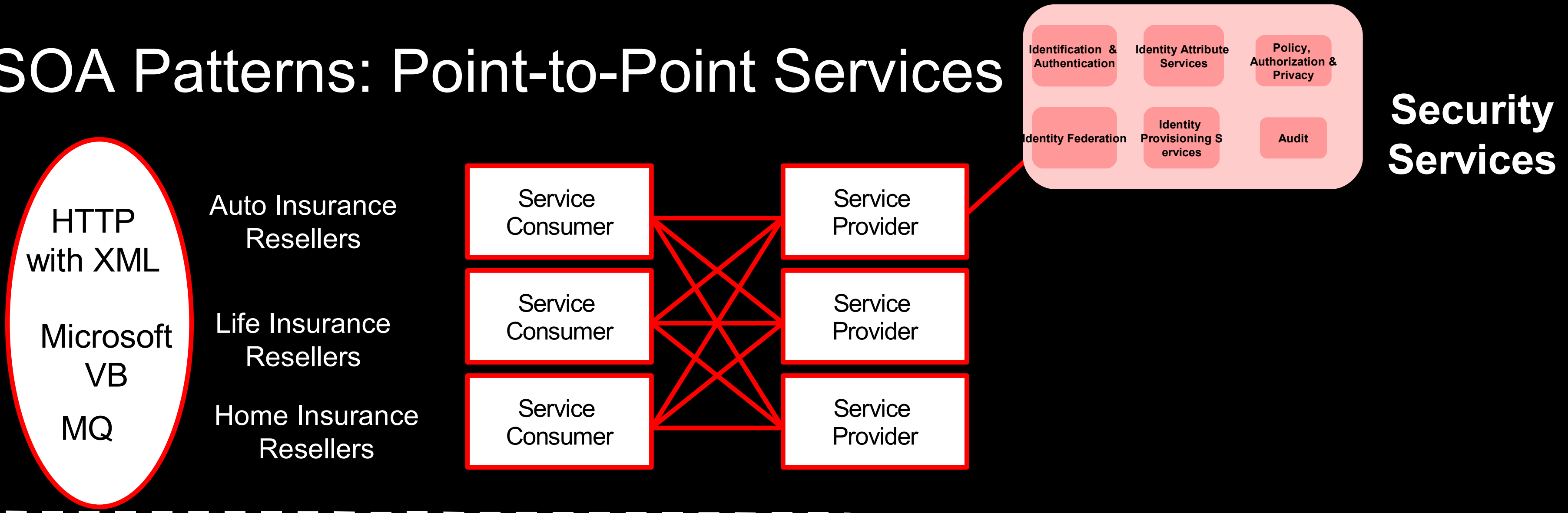
Audit: Common Base Event (CBE)

Privacy: Project Higgins

Federation: WS-Federation, WS-Trust, Liberty, SAML

- Security Services can be Applied to
  - Point to Point Web Services
  - Application Container
  - Enterprise Service Bus
  - Process Choreography

SOA Patterns: Point-to-Point Services



HTTP with XML

Microsoft VB

MQ

Auto Insurance Resellers

Life Insurance Resellers

Home Insurance Resellers

Service Consumer

Service Consumer

Service Consumer

Service Provider

Service Provider

Service Provider

Identification & Authentication

Identity Attribute Services

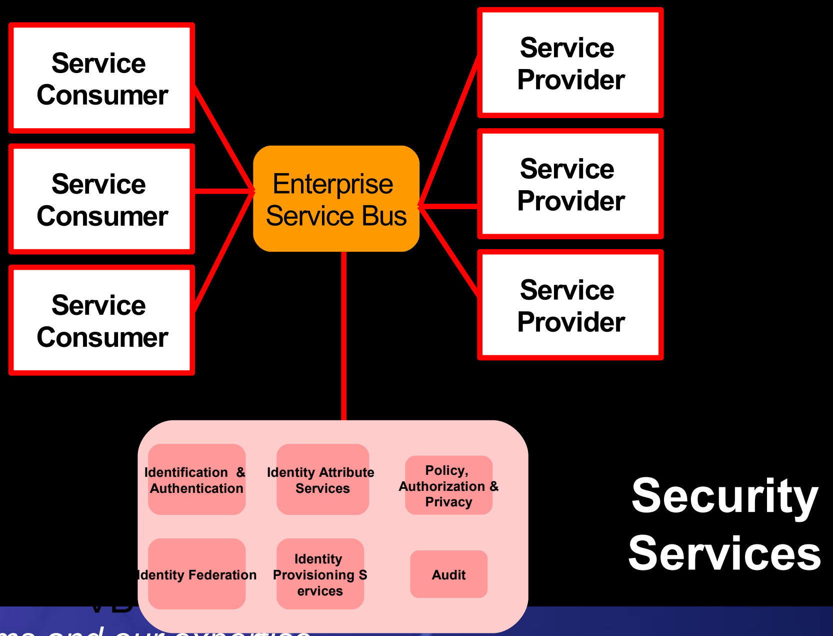
Policy, Authorization & Privacy

Identity Federation

Identity Provisioning Services

Audit

Security Services



Service Consumer

Service Consumer

Service Consumer

Enterprise Service Bus

Service Provider

Service Provider

Service Provider

Identification & Authentication

Identity Attribute Services

Policy, Authorization & Privacy

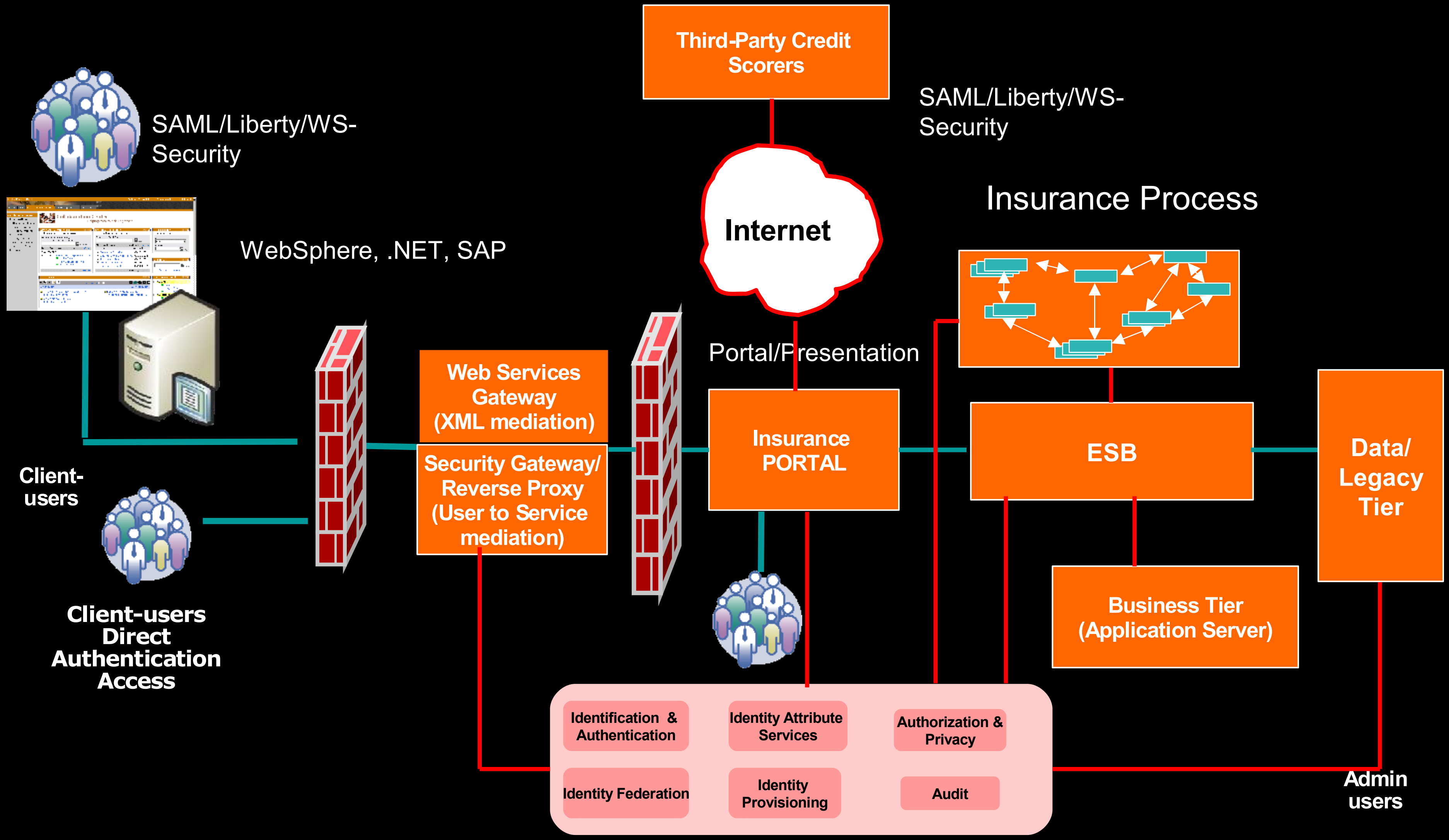
Identity Federation

Identity Provisioning Services

Audit

Security Services

Security Services for SOA – Application Pattern



SAML/Liberty/WS-Security

WebSphere, .NET, SAP

Client-users

Client-users Direct Authentication Access

Web Services Gateway (XML mediation)

Security Gateway/ Reverse Proxy (User to Service mediation)

Third-Party Credit Scorers

Internet

SAML/Liberty/WS-Security

Insurance Process

Portal/Presentation

Insurance PORTAL

ESB

Data/ Legacy Tier

Business Tier (Application Server)

Identification & Authentication

Identity Attribute Services

Authorization & Privacy

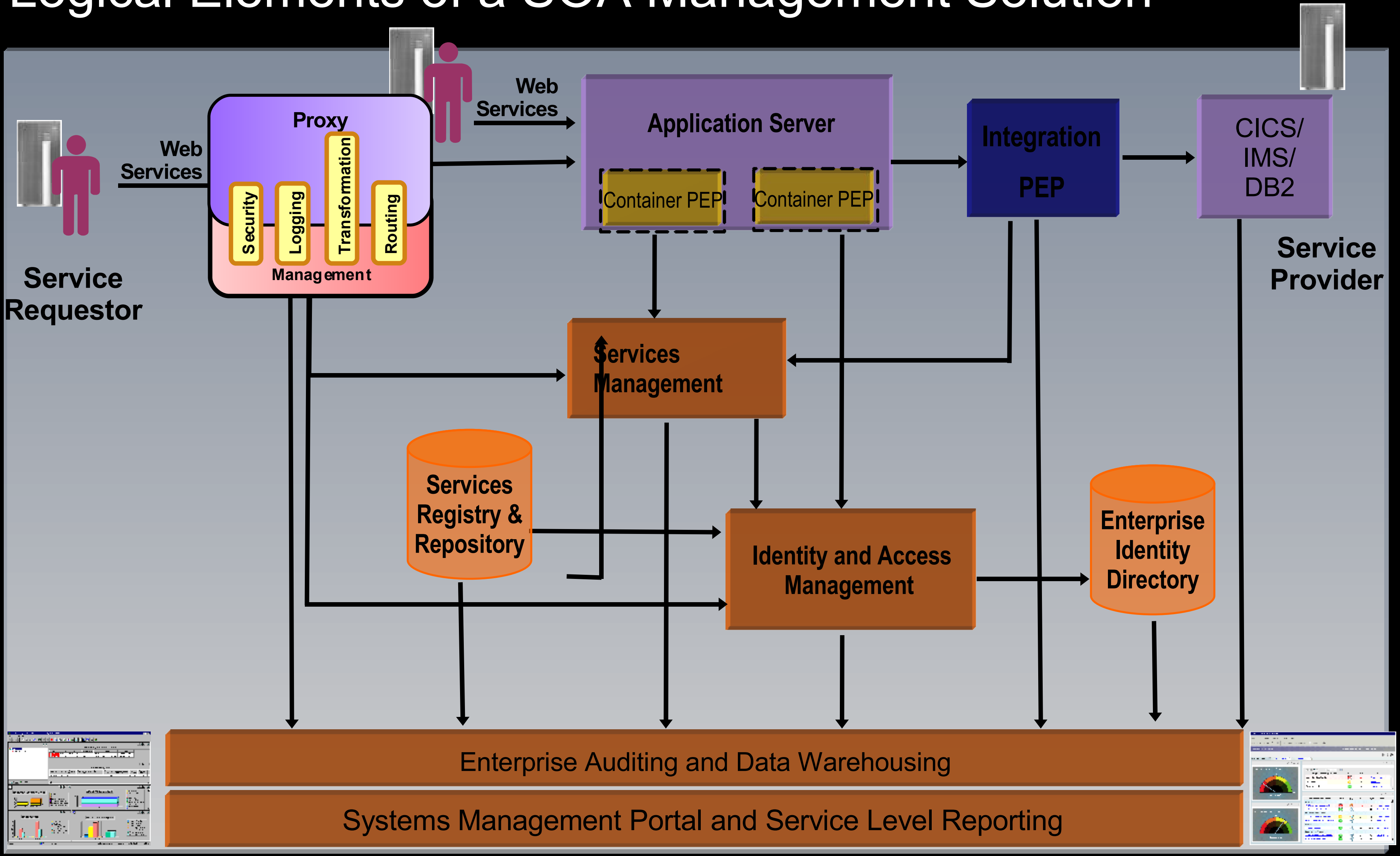
Identity Federation

Identity Provisioning

Audit

Admin users

Logical Elements of a SOA Management Solution



IBM Secure SOA Components

First Line of Defense

- Message Authentication
- XML Threat Protection
- XML message authentication
- Data Validation
- XML/SOAP Routing
- Signing and Encrypting messages
- Service Virtu
- Web Services Gateway

DataPower

- User to Service mediation
- HTTPS Reverse proxy
- Session Management
- Identity Federation
- Federated
- User and
- Coarse-grained Access Control
- Auditing
- Scale and performance
- Vulnerability Management
- Phising Attack Prevention

Tivoli Federated Identity Manager

Second Line of Defense

User Security Aggregation
Portal Service Orientation
Multi-Channel ACcess
Presentation Layer Security
Service Aggregation
Remote Portal Security
Security Mediations (Tokens)
Enterprise Identity Management
Auditing
Credential Vaulting
Federated Web Services Security
Portal SSO

Tivoli Access Manager

Third Line of Defense

BPEL Security
Enterprise Service Bus
Compliance and Audit
SO

Federated Identity Manager

J2EE Container Security
.NET Container Security
EJB Application Security
Credential Transformation
Legacy Security Integration (CICS)
Security Token Services

Access Manager

Identity Management, Service Management, Compliance, Governance

Tivoli Federated Identity Manager, Composite Application Manager for SOA

SOA Security Management – Standards Support

Function	Capability	Standard
Single Sign On	Single Sign On between Identity Providers and Service Providers	SAML 1.0, SAML 1.1, SAML 2.0
Identity Federation	LECP profile, SSO profiles (B/A, BP), Single Logout (SP initiated, IDP initiated), IDP Introduction, Federation Termination notification, (IDP initiated, SP initiated), RNI (IDP initiated, SP initiated)	Liberty ID FF 1.1
	IDP Complete, SP Complete	Liberty ID FF 1.2
	Web Single Sign-On Protocol Request SSO token from Identity Provider, Send Single Sign-On token to Service Provider, Single Logout, Push/Pull model SSO	WS-Federation
Authentication & Credential Brokering	Authentication of Users, Web Services Requestors and Providers	OATH, WS-Security - ID, SAML, Kerberos and X.509v3 profile WS-Trust
Policy Management	Policy management for Policy enforcement points across SOA lifecycle	WS-Policy, WS-SecurityPolicy
XML Threat Protection and Message Authentication	Authentication of messages, XML filtering and threat protection	WS-Security
Authorization	How do Web Services clients and Providers implement access control and authorization?	WS-Trust XACML Java 2 Security JACC
Message Integrity & Confidentiality	Can we ensure that messages are tamper-proof? How can we ensure that critical information within the message can be verified as originating from the right source?	WS-Security - XML Digital Signatures XML Encryption
User Provisioning	How do provision user credentials to services?	SPML
Federated User Provisioning	Issuance, management, revocation of identity credentials for B2B (users and services)	SPML, WS-Provisioning

SOA Security - Summary

- Security Services are an evolution of Composite Application Security to SOA
- SOA Security is an enabler for business flexibility – bringing People, Process and Data together using Role-based Access Control
- Security needs to be delivered as Services - Identity Management, Federated Audit, XML Security and Governance are critical building blocks of a SOA Security
- Federated Security is the "bridge" by which SOA enabled business process collaborate both within across enterprises
- IBM SOA Management Offerings
  - Tivoli Access Manager, DataPower SOA Appliances, Tivoli Federated Identity Manager and Tivoli Composite Application Manager for SOA are critical to SOA management and enforcement

THANK YOU

- Venkat Raghavan
  IBM Software Group
  vraghava@us.ibm.com