
IBM
Xavier Chotteau
ITSM Lead Architect, IBM Global Technology Services WW
Gestion de la sécurité SOA
TENDANCES LOGICIELLES D'ÉTÉ 2008
SESSION SPÉCIALE GESTION DES RISQUES OPÉRATIONNELS

Agenda

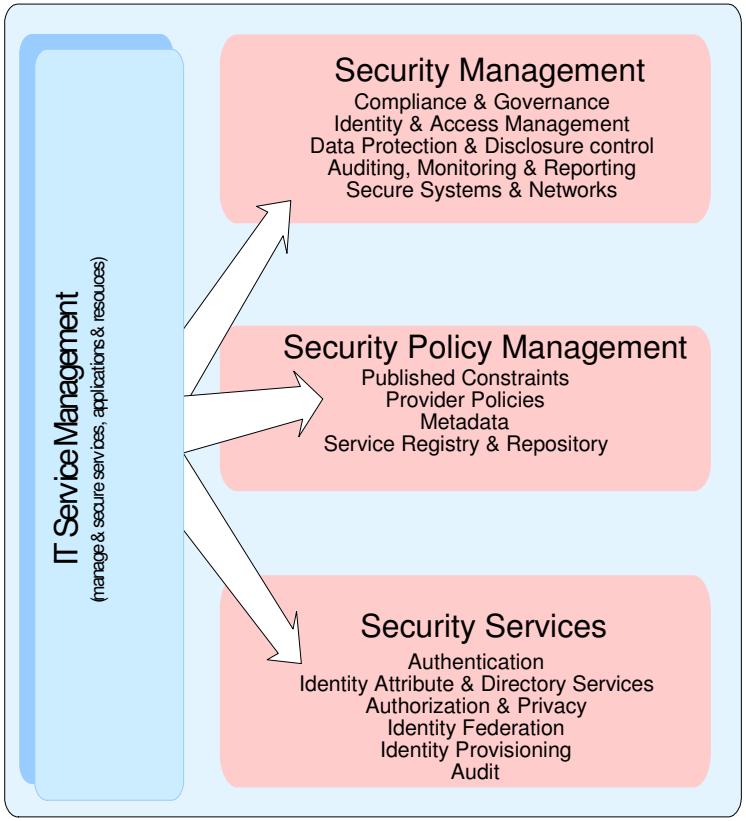
- Security management in SOA context
- SOA related security standards
- Tivoli-based SOA security solutions
- Recommendations to manage SOA security
- Questions & answers

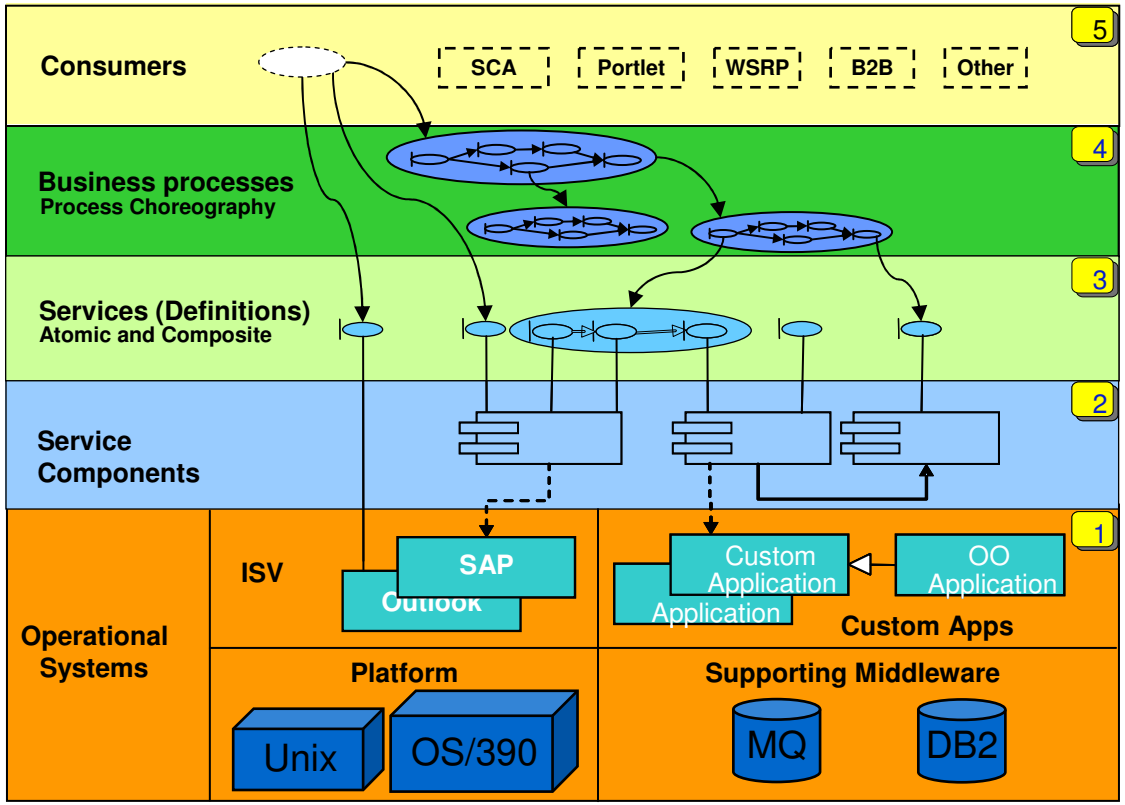
Security management in SOA Context

Security in a SOA context

- ***Business view on policies and relationships***
  - *Business policies about security to be factored into the lifecycle*
  - *Intra-enterprise or inter-enterprise have different trust relationships*
  - *Federation of services involves cross business (trust, technology, political) boundaries*
- ***Architectural approach***
  - *Loose coupling - Services invocations need to take policies into account*
  - *Flexibility and reuse - Interoperability (standards), Integration (framework-provider model)*
  - *Architecting mediations in a gateway model facilitates efficient trust management*
- ***Composite application development***
  - *Business driven application security – Tool support move up the lifecycle*
  - *Usage of patterns and templates to simplify security policy modeling*
- ***Management approach – policy and process***
  - *Policy and process driven security*
  - *Auditing, reporting, remediation, etc that tie into business processes*

SOA Security Reference Model





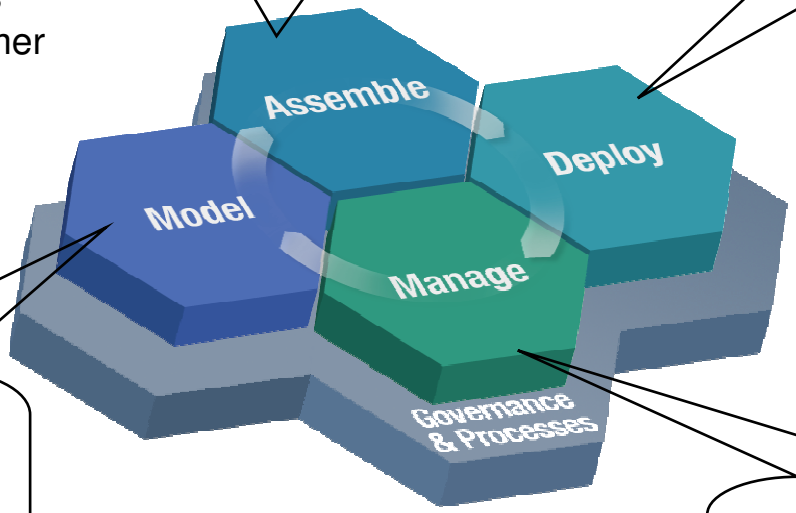
Security Encompasses all Aspects of SOA Lifecycle

Declare application security policies; build and **test secure applications**

Security Architects
Application Architects
Application Programmer

Configure infrastructure for application security; **integrate people, process and information**

Application Administrator
Security Administrator
Security Developer



Security Policy Officer
Security Auditor
Business Analyst

Define business and **corporate security** policies; **model security** requirements and **application security**

IT Administrator
Security Administrator
Operator

Manage application security; manage identities and monitor for compliance

Security management considerations for SOA

- SOA introduces additional security concerns:
  - How do we **authenticate and authorize** the **service requester**?
  - How to we **authenticate and authorize** the **source of the message**?
  - Is the client authorized to send this **message content**?
  - Can we ensure **message integrity** & **confidentiality**?
  - How do we **audit** the access to services?
  - How do we leverage **Web services security standards**?
  - How do we **propagate identities** with trusted service providers?
- XML-based web services may **expose backend systems** in unintended ways. Applications (services) are security unaware.
- SOA security may require multiple **layers of enforcement**
- **Traditional security devices do not secure XML/SOAP**
- Security practices must be aligned with business processes.
- Security is a service managed by the infrastructure.

SOA security standards

Common XML threats in a SOA environment

SOA and Web Services runs on Web-based technology, so it inherits all the security risks of the Web:

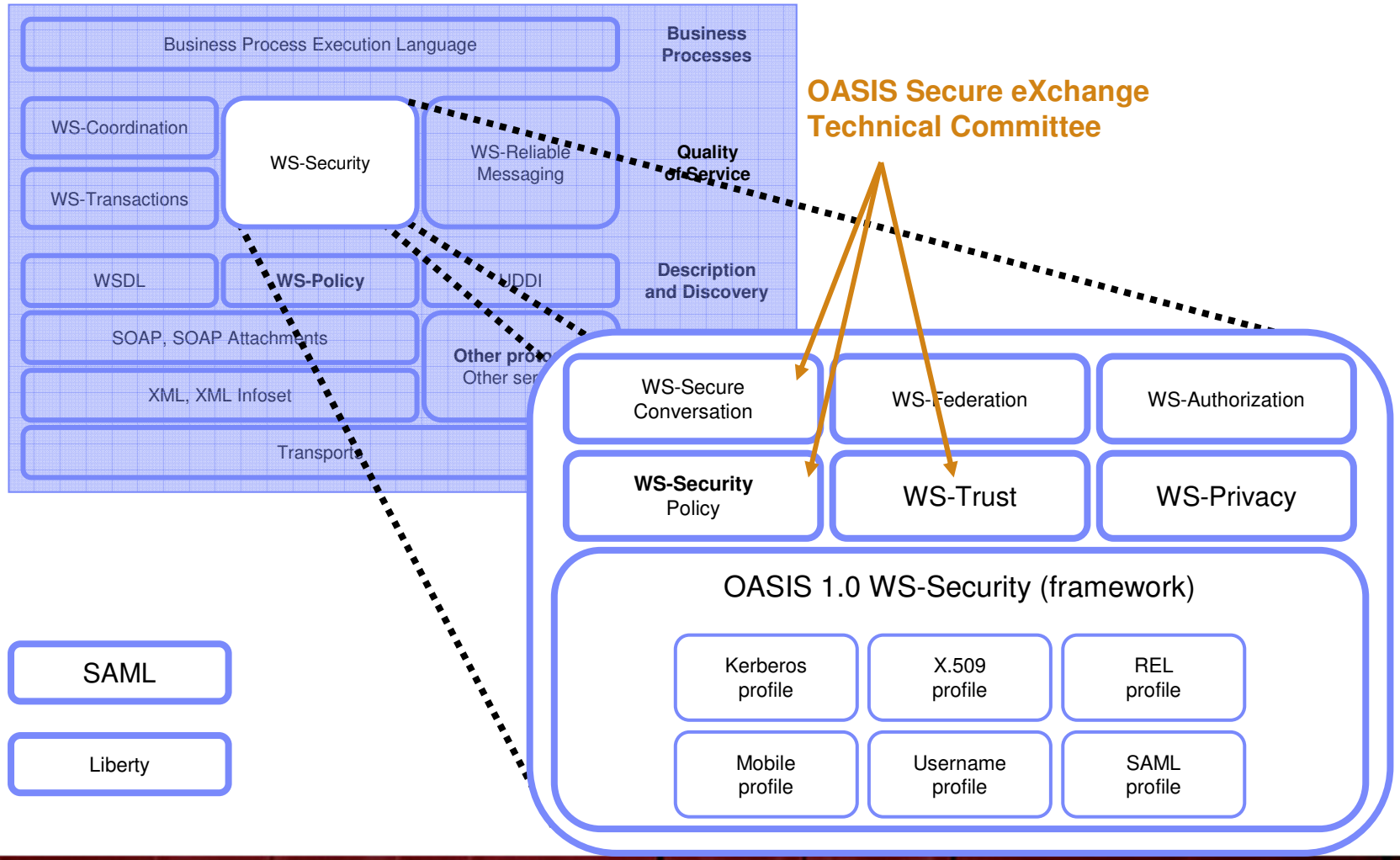
• **xDoS (XML Denial of Service)**: SOAP jumbo payloads, Recursive elements, Mega-tags, Coersive parsing, Public key DoS, XML flood, Resource hijack.

• **Unauthorized access to Service registry**: Dictionary attack, Falsified message, XML replay attack.

• **Data integrity/confidentiality through SOAP messages**: Message/data tampering, Message snooping, SQL/XPath/XSLT injection, WSDL enumeration, Routing detour / Man-in-the-middle, Spoofing

• **System compromise through SOAP messages**: Malicious include, Memory space breach, XML encapsulation, X-Virus.

WS-Security Model



WS-Policy

- Is an extensible **syntax** for identifying capabilities, requirements, and general characteristics of entities
- Is a collection of policy assertions (e.g. authentication scheme, protocols, QoS characteristics, encryption requirements, security token lifespan, security token type, etc.)
- Does NOT specify how the policies are associated with entities

WS-Federation

- Specifies how federation is implemented
- Describes how existing web services security is implemented **to provide SSO**, trust, and attribute management
- Is primarily concerned with relationship between federated parties
- WS-Federation Active (web services enabled)
- WS-Federation Passive (not web services enabled)
- Provides standards-based secure digital identity and trust platform for web services platforms

WS-Trust

- Is a framework for trust model interoperability
- Extends WS-Security to support issuance, exchange, and **validation of security tokens**
- Enables cross domain issuance and dissemination of security credentials

WS-Privacy

- Specifies how privacy language can be embedded within WS-Policy descriptions
- Is a model used by WS-Security to **associate privacy claims in messages**
- Enables WS-Trust to evaluate both user preferences and organizational privacy claims

WS-Authorization

- Is a framework for **managing authorizations**
- Defines how access policies are defined and managed

WS-Secure Conversation

- Extends WS-Security and WS-Policy to provide **secure communication** between web services
- Focuses on message authentication
- Is a mechanism for establishing and sharing security contexts
- Describes the **method for extract keys from security contexts**

WS-Security Policy

- Describes *how* messages should be secured
- Is a set of assertions for **SOAP message security**, WS-Trust, and WS-Conversation
- Supports multiple token types and encryption methods

WS-Provisioning

- APIs and schema for interoperability between provisioning solutions
- Is **based on directory concepts**
- Leverages WSDL and XML schema

Security Assertions Markup Language (SAML)

- Is developed by consortium of vendors, including IBM, under the direction of OASIS
- Is intended to provide standards for **interoperability between vendors for SSO**
- Is XML formatted assertion
- Includes user identity information
- Is vendor neutral
- Versions 1.0 and 1.1 focused on SSO
- Version 2.0 supports full user lifecycle management
- Version 2.0 influenced by Shibboleth and **Liberty** ID-FF 1.2

eXtensible Access Control Markup Language (XACML)

It is the common language for **communicating access control policies** and requirements and supports the following functions:

- Policy definition
- Attribute requirements for policy evaluation
- Policy evaluation
- Policy enforcement

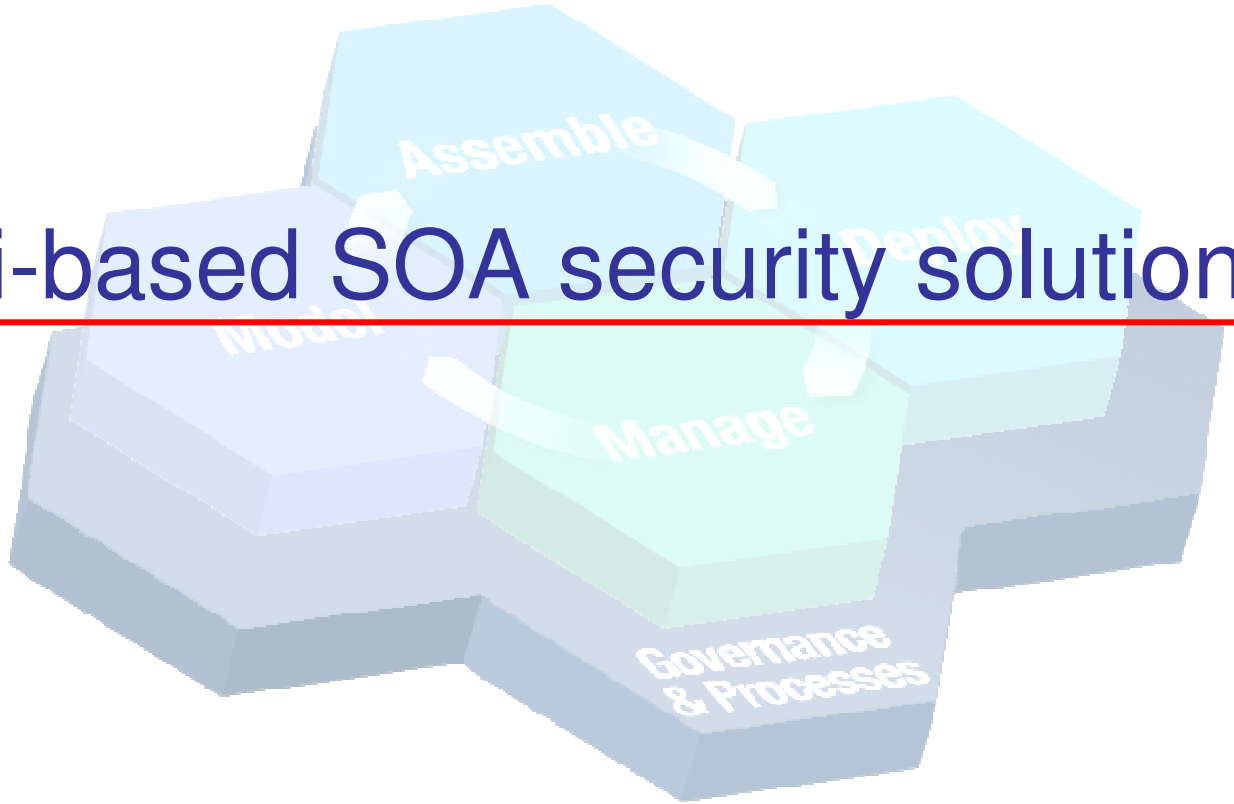
Java Authorization Contract for Containers (JACC)

- Defines new Permission classes for EJB and **Web permissions in J2EE deployment** descriptors
- Provides interfaces and rules allowing **authorization providers to communicate with J2EE application containers**
- **Removes access decisions from the application servers**
- Provides standards to allow authorization providers to interface with application servers

Service Provisioning Markup Language (SPML)

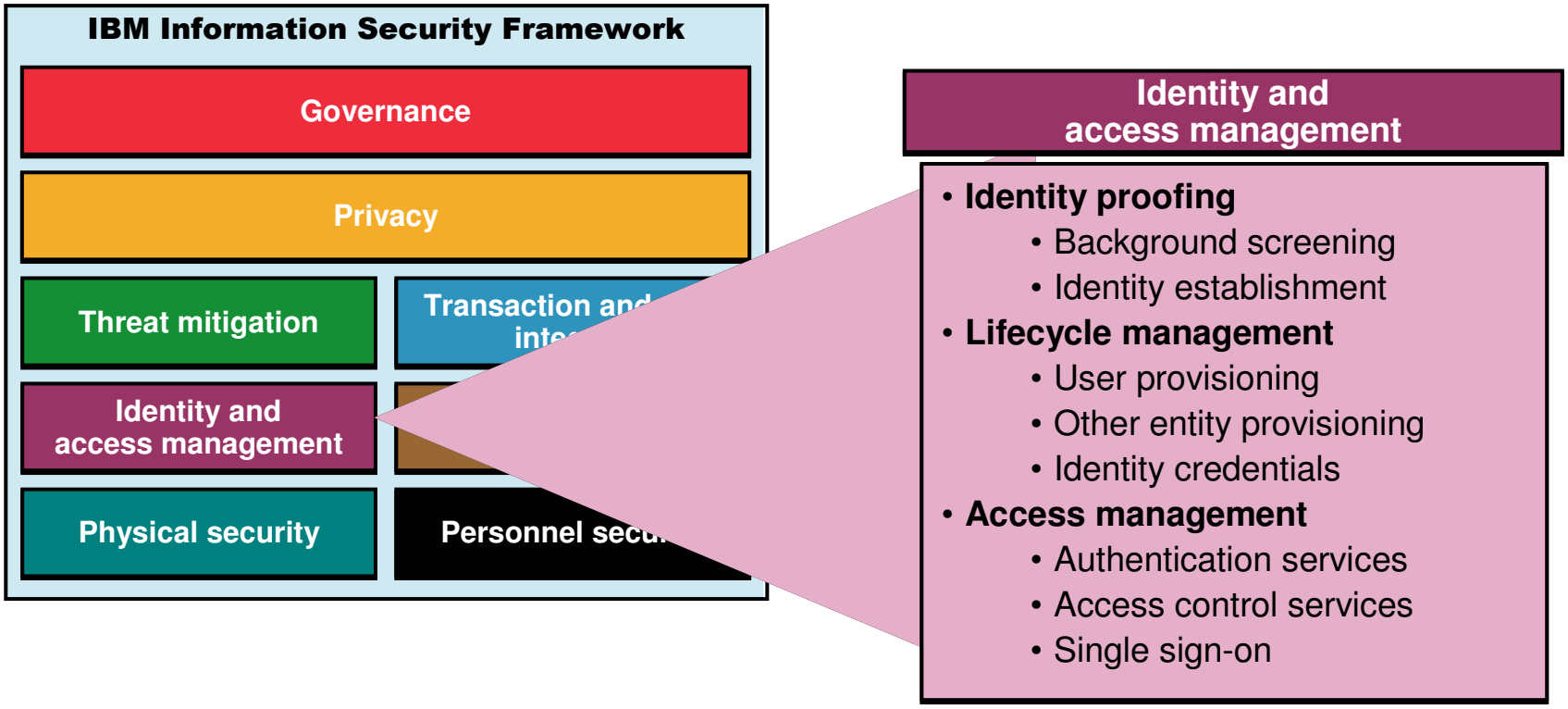
- Provides XML framework for **managing provisioning**, **identity information**, and system resources between organizations
- Version 2.0 ratified by OASIS in April, 2006
- Defines four primary elements for provisioning:
  - Requesting Authority (RA): Originator of the identity
  - Provisioning Service Provider (PSP): Accepts and processes provisioning requests from the RA (e.g. ITIM)
  - Provisioning Service Target (PST): The provisioning target (e.g. AD)
  - Provisioning Service Object (PSO): The provisioned target (e.g. AD Id)

Tivoli-based SOA security solutions



Information Security Framework Capability reference model

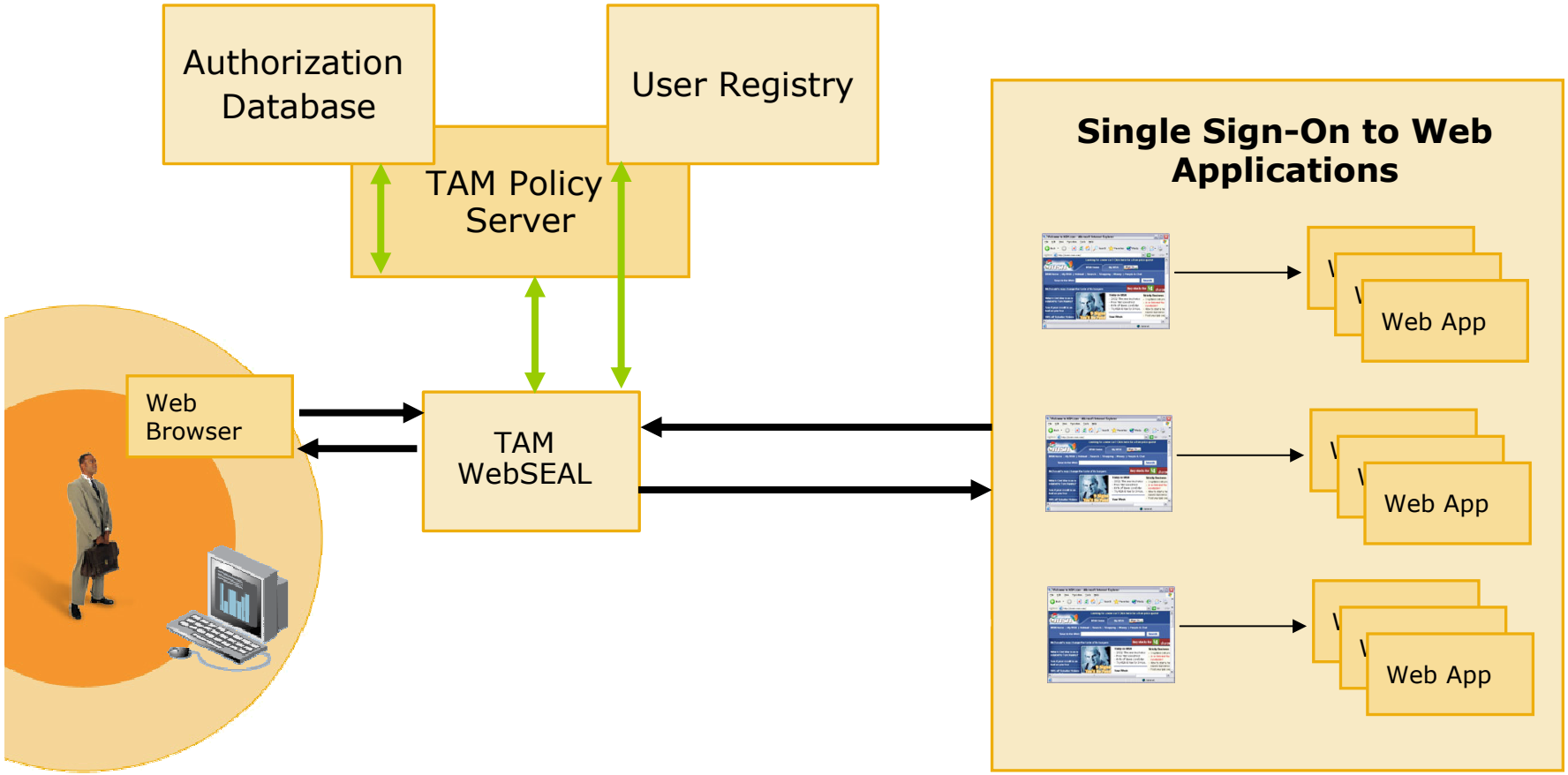
IBM Information Security Framework



Tivoli Access Manager

- Centralized authentication, access, and auditing
- Enables SSO
- Common security model
- Foundation for identity federation
- Policy driven
- Centralized administration
- Integrates with Tivoli identity management

Web Server Example

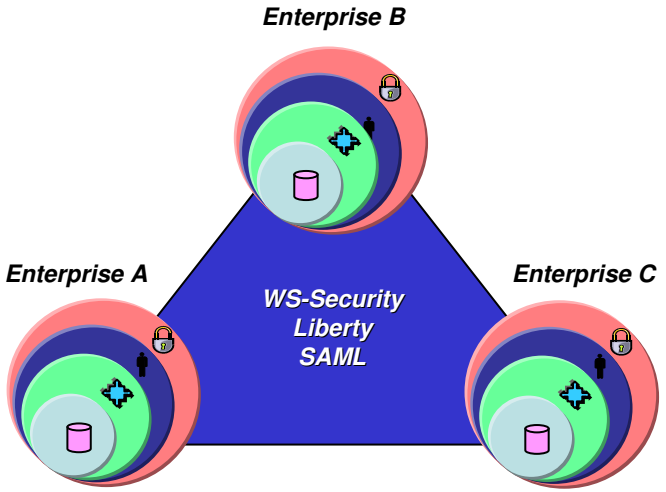


Federated Identity Management

- **Definition**
  - **An "identity federation" is a federation in which identity management (authentication, access control, auditing, and provisioning) is distributed between the partners based on their role within the federation.**
  - **An Identity Federation can allow users from one federation partner to *seamlessly* access resources from another partner in a secure and *trustworthy* manner.**

- **Roles**
  - **End user**
  - **Identity Provider (IdP)**
  - **Service Provider (SP)**

- **Functions**
  - **Single Sign-On/Sign-Off (incl. "global" sign-off)**
  - **Provisioning/De-provisioning**
  - **Account Linking/De-linking**

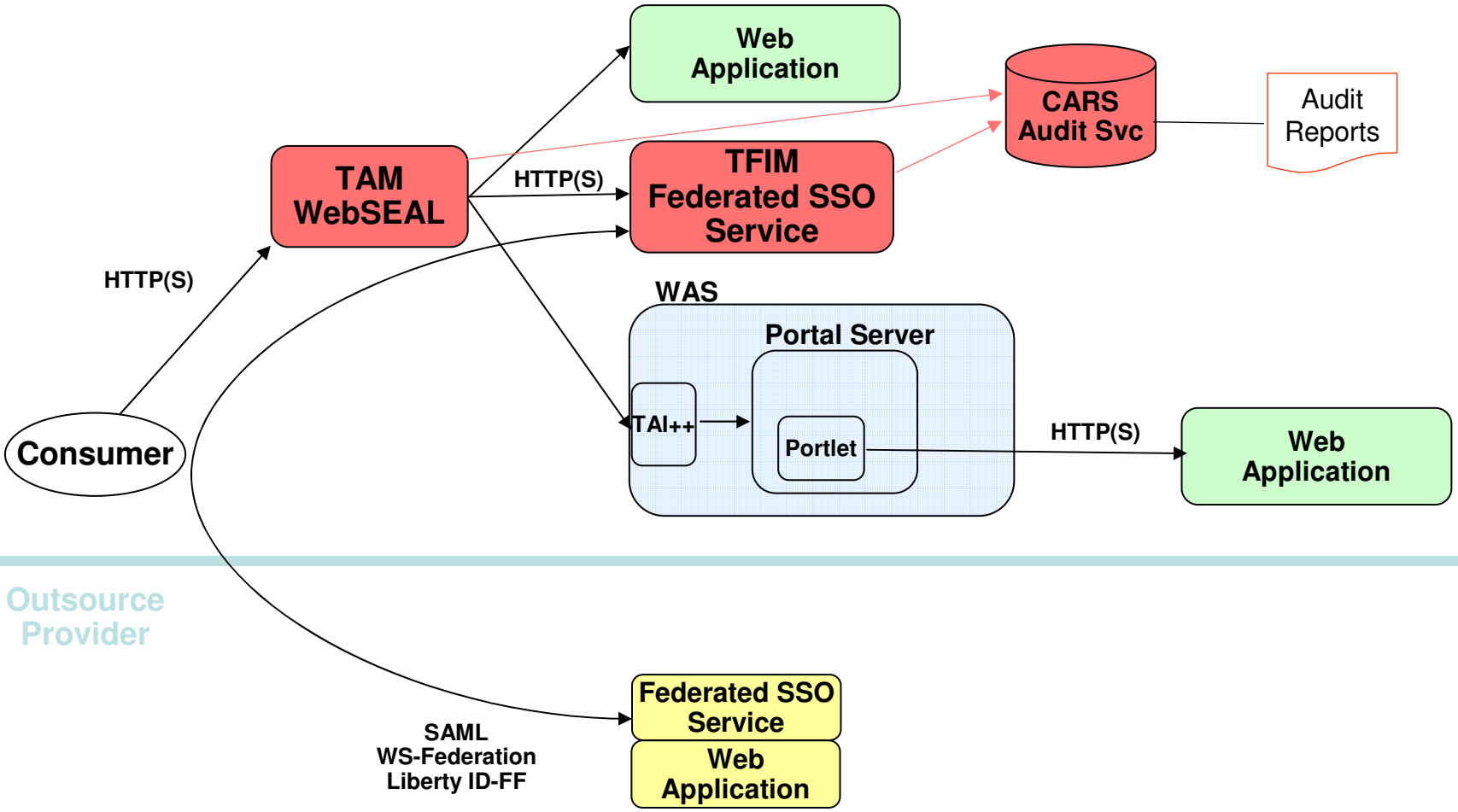


Tivoli Federated Identity Manager (TFIM)

- **Single sign-on** (SSO)
- **Identity mediation** for web services
- **Cross domain identity exchange** format mapping
- **Authorization service** interface
- Integrate **audit data collection** and reporting
- **Align with open standards and specifications** including Liberty, SAML, WS-Federation, WS-Security, and WS-Trust Security Token Services (STS)

- **Improve user experience** ; Allow collaboration with a wide variety of partner organizations
- **Minimize application impact**
- **Simplify administration** of security in cross-enterprise business processes by delivering "security as services"

Federated Architecture



XML Security: bar the front door with Datapower!

- **Legacy systems are not even aware of XML**
- **Schema Validation** and XML security practices **are resource intensive**
- XML is being used to **connect the most valuable resources**
- **XML Web Services Access Control**

- Sealed network-resident device
- Optimized hardware, firmware, embedded OS
- Single signed/encrypted firmware image, Cannot install arbitrary software
- High assurance, “default off” locked-down configuration
- Security vulnerabilities minimized (few 3 party components)
- Hardware storage of encryption keys, locked audit log
- No drives/USB ports, tamper-proof case
- FIPS level 3 HSM (option)
- Under evaluation by Common Criteria EAL4
- Large financial and government customers

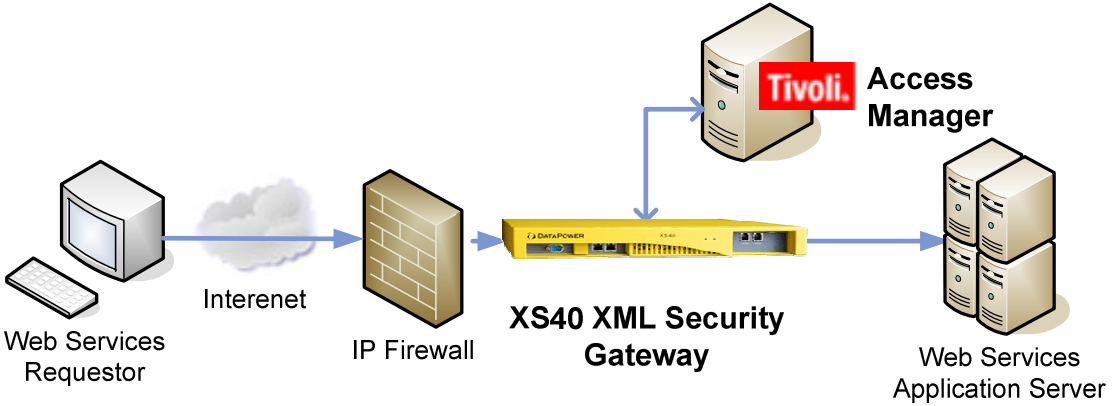
“The DataPower ... is the most hardened ... it looks and feels like a datacenter appliance, with no extra ports or buttons exposed and no rotating media. “ - InfoWorld

DataPower: Improved Security

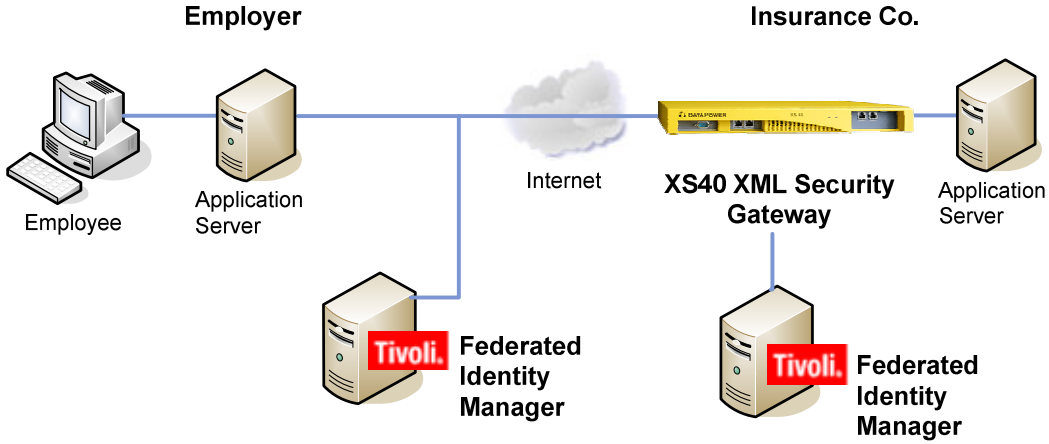
Use Datapower to:

- Filter, Validate, Transform, Encrypt/Decrypt XML Documents
- Sign Documents and/or Verify Signatures; Hardware storage of encryption keys
- Communicate with clients, servers and peers using SSL encryption
- Monitor and log activity, delivering log information to external managers
- Well-formedness checking
- Schema validation
- Filter based on IP criteria, SSL information, HTTP header, XPath on SOAP/XML
- Avoid XDoS

1) Use TAM for secure Web SSO and XML Web services



2) Use TFIM to allow third parties / users get information easily



Recommendations to manage SOA security

Recommendations to manage SOA Security

- Security authorization needs to be **granular at the service level; Control AAA with SSO and Federation Identity Mechanisms**
- **Work with the SOA application teams** to understand the **requirements**, the **trade-offs of security, performance and cost**
- Understand existing **corporate security policies** (especially approval and audit process) and apply them in the SOA environment
- Choose policy-based over programmatic approaches to allow **security decisions to be implemented at service invocation**
- Consider **XML appliances to accelerate security processing**:
  - Use WS-* standards
  - Filter, Validate, Transform, Encrypt/Decrypt XML messages
  - Mask internal resources. Time stamp all messages
  - Secure logging; Sign all messages and Verify Signatures; Use hardware storage of encryption keys
  - Communicate with clients, servers and peers using SSL encryption
  - Monitor and log activity, delivering log information to external managers
  - Check well-formdness of incoming requests and Schema validation
  - Filter messages based on IP criteria, SSL information, HTTP header, XPath on SOAP/XML
  - Protect against XDoS
  - Invoke external access, identity managers and anti-X-virus

IBM

Merci pour votre attention

Links for More Information on Tivoli Security

- Federated Identity Management and Web Services Security with IBM Tivoli Security Solutions
  - http://www.redbooks.ibm.com/abstracts/SG246394.html?Open
- Enterprise Security Architecture Using IBM Tivoli Security Solutions
  - http://www.redbooks.ibm.com/abstracts/sg246014.html?Open
- Service Oriented Architecture – SOA
  - http://www-306.ibm.com/software/solutions/soa/