z/TPF V1.1

TPF Users Group - Spring 2009

Security Considerations in a Service Oriented Architecture (SOA)

Jason Keenaghan
Main Tent

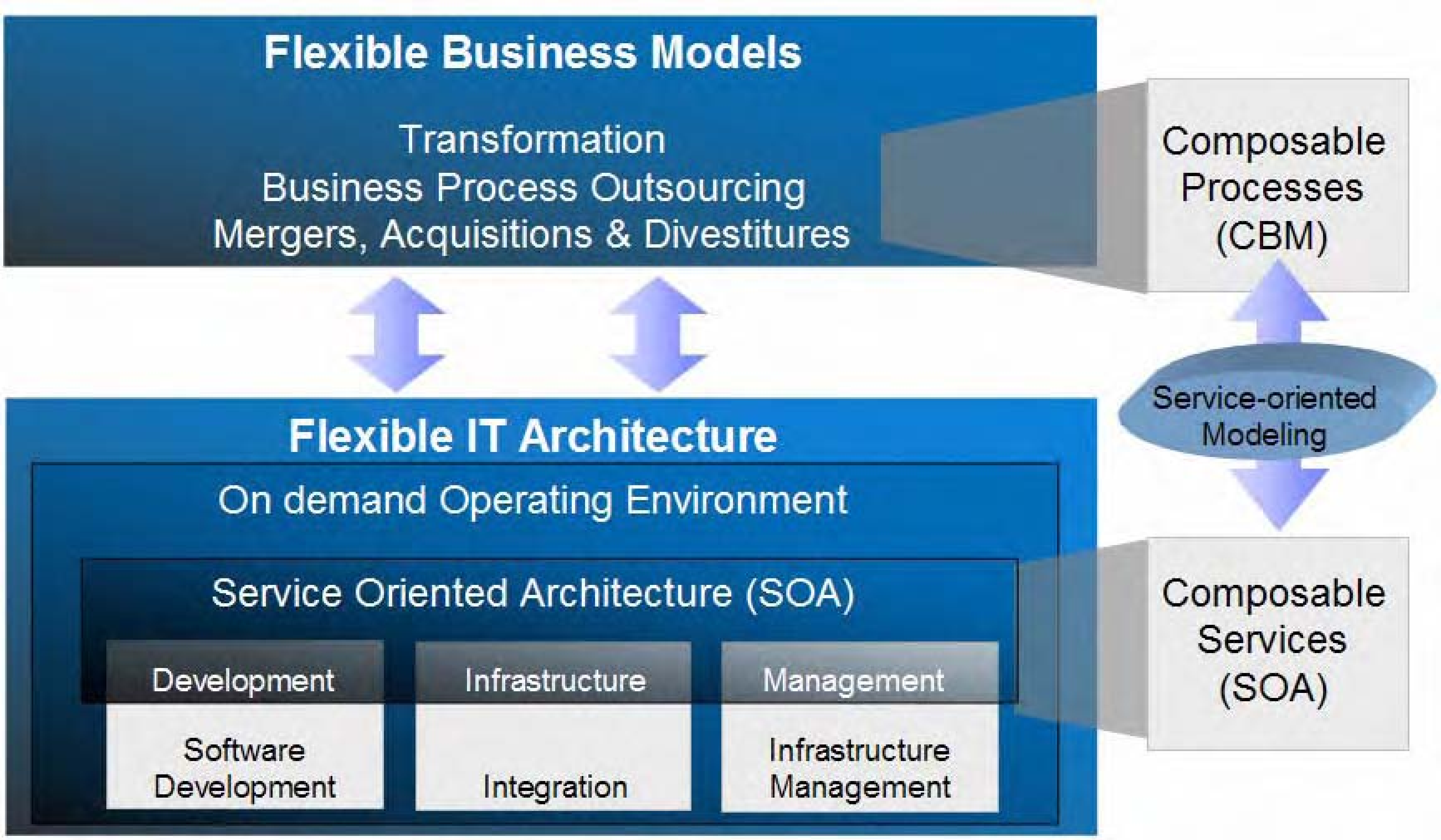
AIM Enterprise Platform Software
IBM z/Transaction Processing Facility Enterprise Edition 1.1.0

Any reference to future plans are for planning purposes only. IBM reserves the right to change those plans at its discretion. Any reliance on such a disclosure is solely at your own risk. IBM makes no commitment to provide additional information in the future.

Agenda

- (Re)Introduction to Service Oriented Architecture (SOA)
- The importance of building a secure SOA
- Web services security standards
- Applying SOA security standards to your business

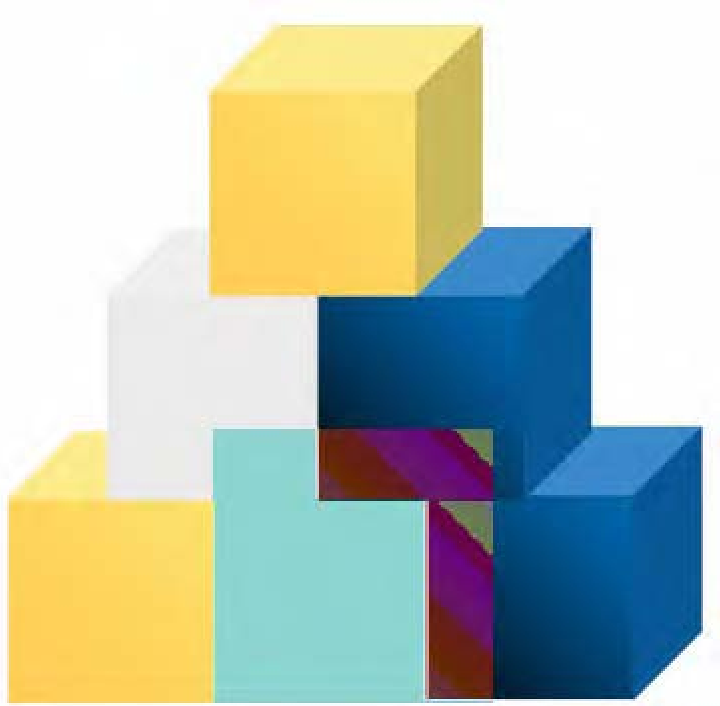
Today's enterprise requires business and IT agility


Flexible Business Models
Transformation
Business Process Outsourcing
Mergers, Acquisitions & Divestitures
Composable Processes (CBM)
Service-oriented Modeling
Flexible IT Architecture
On demand Operating Environment
Service Oriented Architecture (SOA)
Development
Infrastructure
Management
Software Development
Integration
Infrastructure Management
Composable Services (SOA)

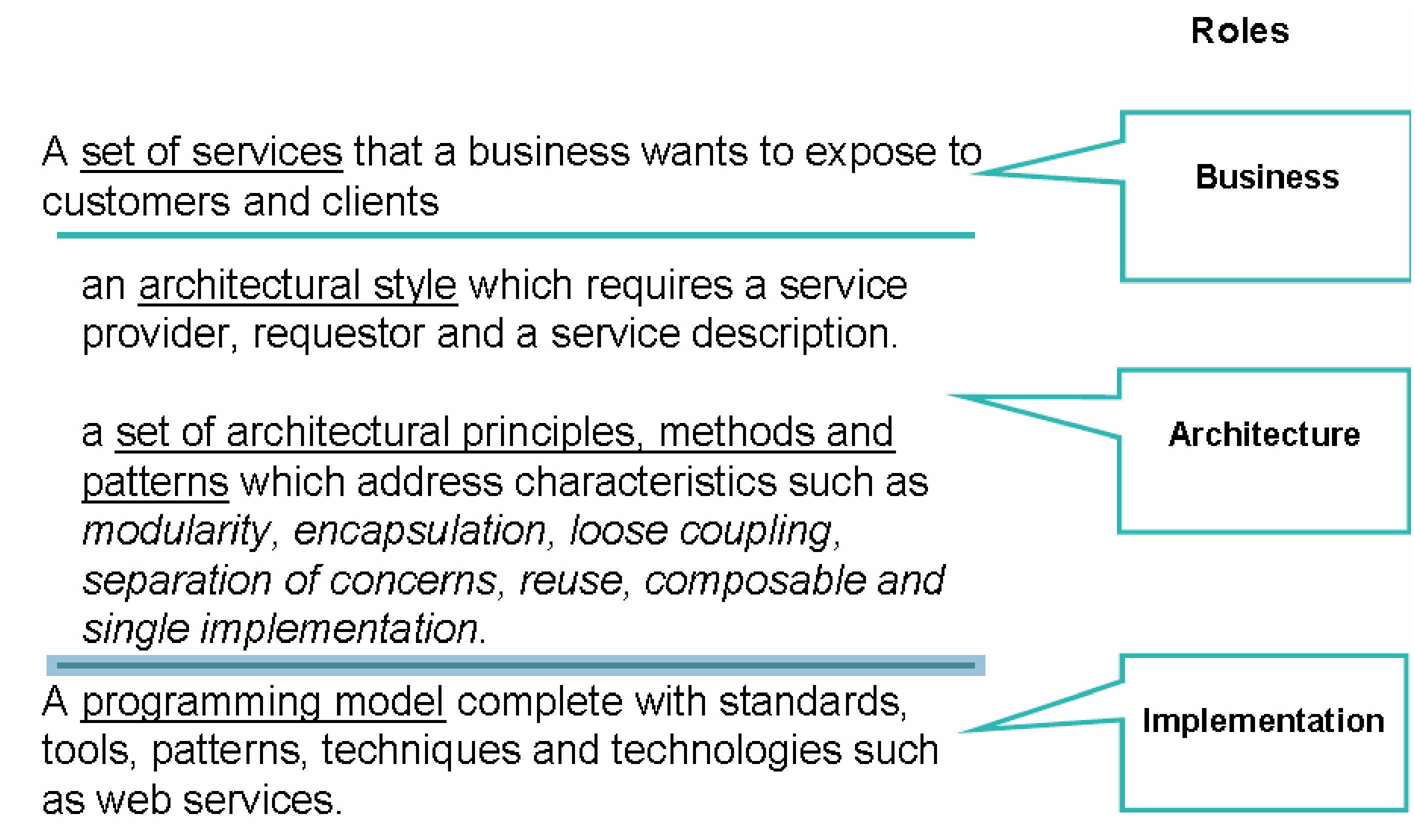
SOA is the key to bridging the needs of Business and IT

The flexibility to treat elements of business processes and the underlying IT infrastructure as secure, standardized components (services) that can be flexibly recomposed and combined to address changing business priorities.

- **Services are the building blocks**
  - Services are used to help **get the right information** to the right people at the right time
  - Services can be **flexibly re-combined** to deploy composite applications to address new opportunities
  - **Packaging business functions** from new and existing applications in a simple and standardized way creates services that are available for use
  - “A Service is a **discoverable software resource** which has a service description. This service description is available for searching, binding and invocation by a service consumer. The service description implementation is realized through a service provider who **delivers quality of service** requirements for the service consumer. Services can be **governed by declarative policies**.”



Three views on SOA



Roles

A set of services that a business wants to expose to customers and clients

an architectural style which requires a service provider, requestor and a service description.

a set of architectural principles, methods and patterns which address characteristics such as *modularity*, *encapsulation*, *loose coupling*, *separation of concerns*, *reuse*, *composable and single implementation*.

A programming model complete with standards, tools, patterns, techniques and technologies such as web services.

What is the SOA model?

Business Componentization

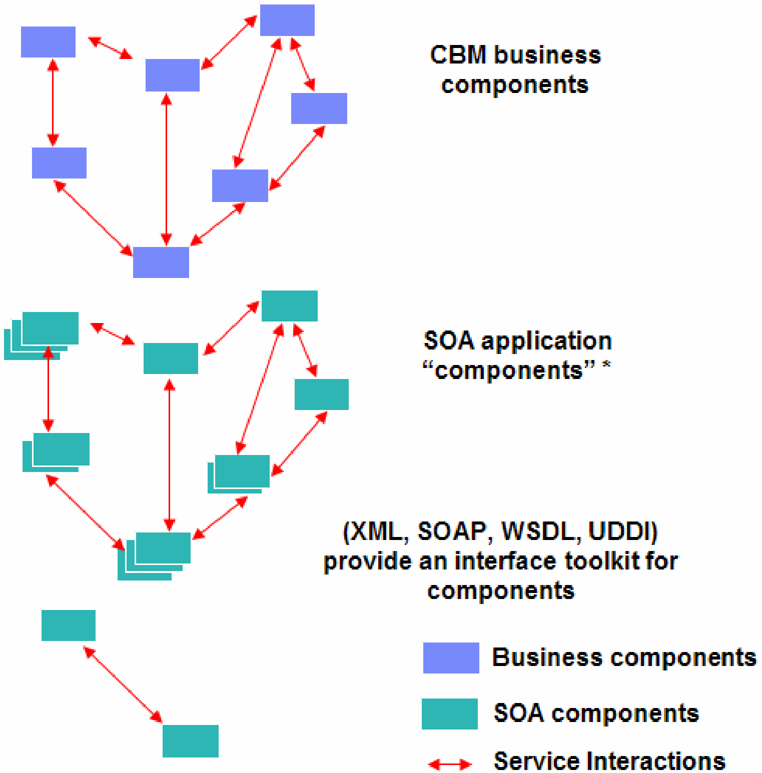
Re-defining today's monolithic enterprise processes as a set of standardized modular business process components

Service Oriented Architecture

An IT model which mirrors the interaction of business components through a set of IT applications implemented as real-time services that interact dynamically

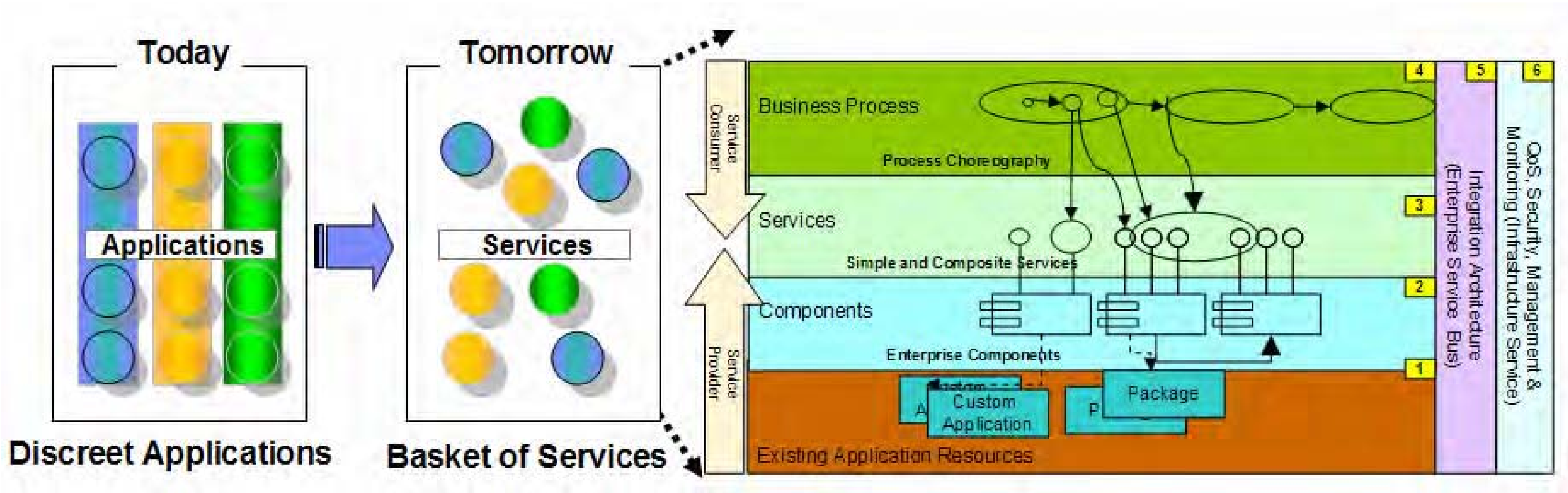
Web Services

A set of vendor neutral and platform agnostic standards that can be used to define how SOA components interact

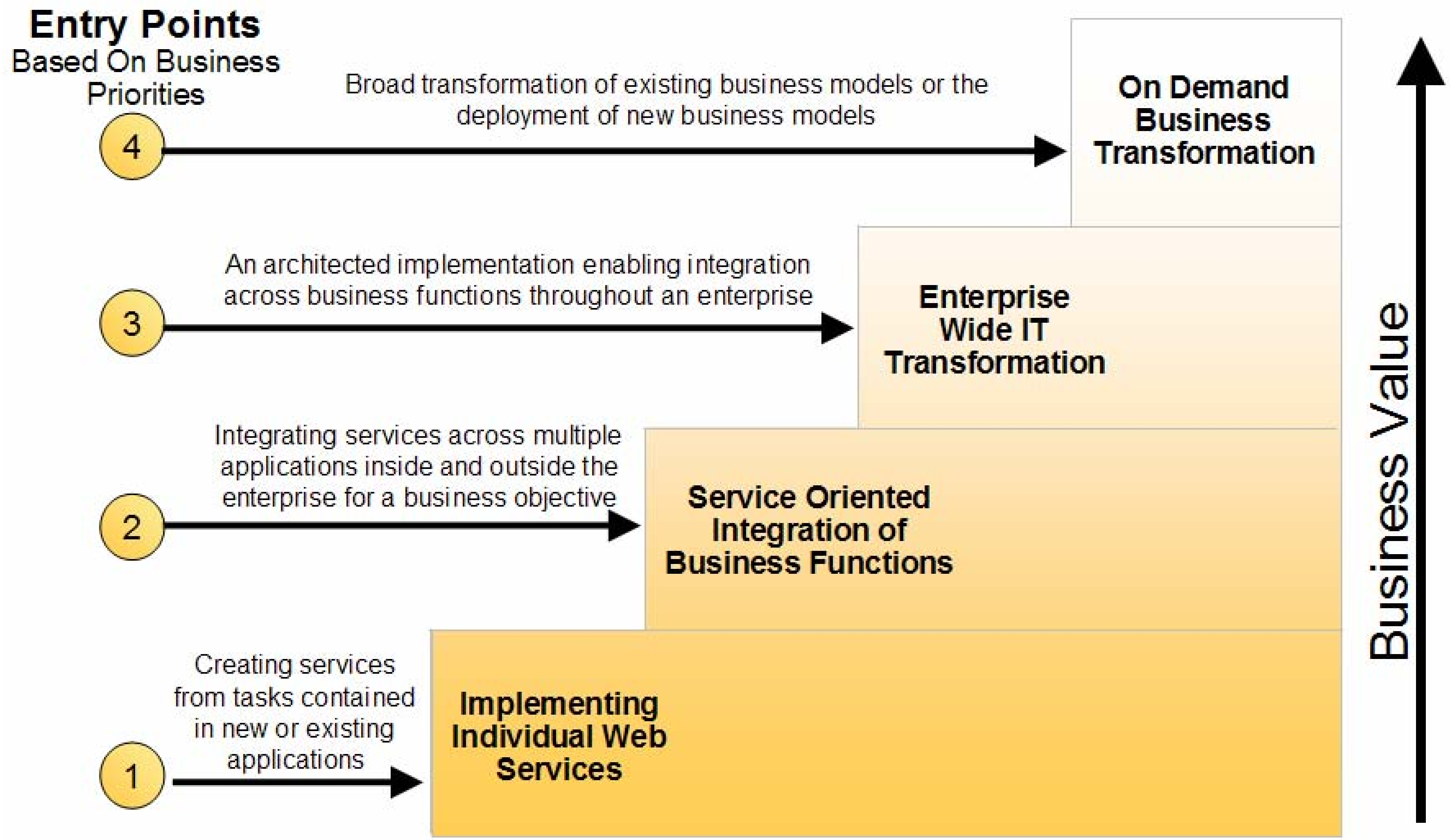

CBM business components
SOA application "components" *
(XML, SOAP, WSDL, UDDI) provide an interface toolkit for components
🟦 Business components
🟩 SOA components
↔ Service Interactions

* Each SOA application component may be made up of multiple applications

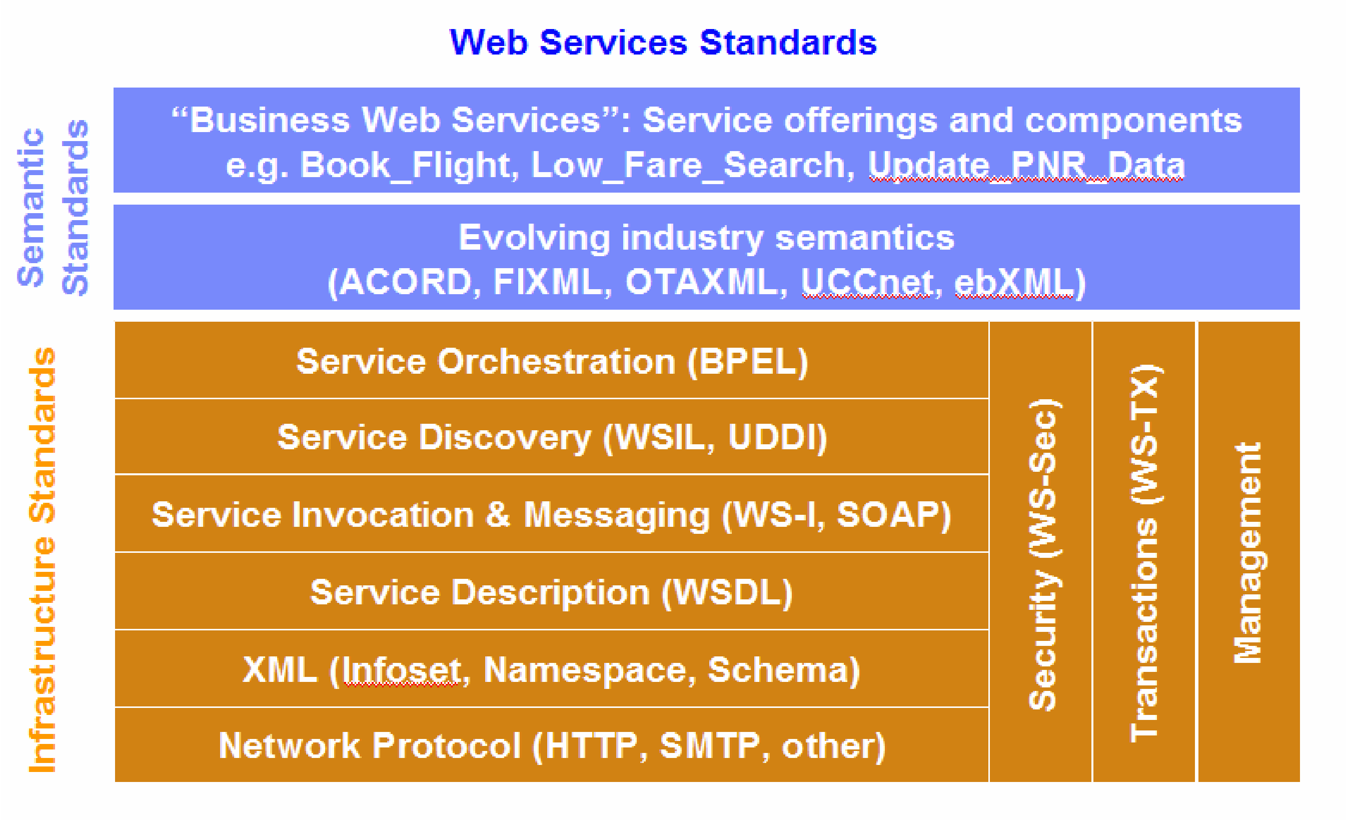
Vision of Service Oriented Architecture (SOA)



Organizations can take different paths to SOA adoption depending on business goals and IT constraints


Entry Points
Based On Business Priorities
4
Broad transformation of existing business models or the deployment of new business models
On Demand Business Transformation
3
An architected implementation enabling integration across business functions throughout an enterprise
Enterprise Wide IT Transformation
2
Integrating services across multiple applications inside and outside the enterprise for a business objective
Service Oriented Integration of Business Functions
1
Creating services from tasks contained in new or existing applications
Implementing Individual Web Services
Business Value

XML is the key to Web service implementation



Web Services Standards

Semantic Standards

“Business Web Services”: Service offerings and components
e.g. Book_Flight, Low_Fare_Search, Update_PNR_Data

Evolving industry semantics
(ACORD, FIXML, OTAXML, UCCnet, ebXML)

Infrastructure Standards

Service Orchestration (BPEL)

Service Discovery (WSIL, UDDI)

Service Invocation & Messaging (WS-I, SOAP)

Service Description (WSDL)

XML (Infoset, Namespace, Schema)

Network Protocol (HTTP, SMTP, other)

Security (WS-Sec)

Transactions (WS-TX)

Management

Agenda

- (Re)Introduction to
  Service Oriented Architecture (SOA)
- The importance of building a secure SOA
- Web services security standards
- Applying SOA security standards to your business

Security requirements from a business perspective

- *Reduce Risks:* **An exposure someone has as a result of a vulnerability being exploited**
- *Establish Trust:* **The extent to which someone who relies on a system can have confidence that the system meets its specifications (i.e., that the system does what it claims to do and does not perform unwanted functions)**
- *Reduce/Eliminate Liability:* **The thing every business is afraid of…something that causes a business to lose money**
- *Provide the Appropriate Asset Protection to offset the risk:* **Any information, system or resource that the business tracks as containing business value or liability**
- *Build stronger Business Relationships:* **Patterns of interaction around customers, partners, suppliers, and competitors**
- *Manage Corporate Security Policies:* **Regulatory compliance, and corporate governance, pass security audits**

Security requirements from an IT perspective

In any architectural solution, the following security requirements must be addressed, with no exceptions when it comes to Web services:

- ***Identification:*** **The party accessing the resource is able to identify itself to the system.**
- ***Authentication:*** **There exists a procedure to verify the identity of the accessing party**
- ***Authorization:*** **There exists a set of transactions the authenticated party is allowed to perform**
- ***Integrity:*** **The information is not changed on its way**
- ***Confidentiality:*** **Nobody is able to read the information on its way**
- ***Auditing:*** **All transactions are recorded so that problems can be analyzed after the fact**
- ***Non-repudiation:*** **Both parties are able to provide legal proof to a third party that the sender did send the information, and the receiver received the identical information**

Who or what is accessing your systems?

- **Greater focus on securing data and information**
  - Protecting data in transit and at rest
  - Apply consistent protection measures
  - Access to data by applications and services

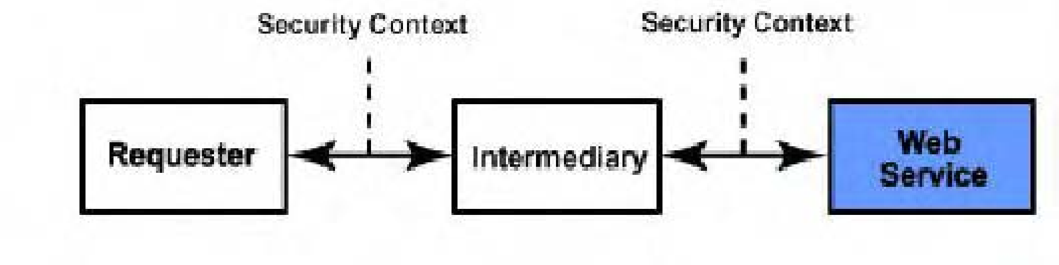
- **Entities, Identities – users, services**
  - Services have identities
  - Identities and/or credentials are propagated across services
  - Users and services are now subject to the same security controls
- **Organizational/enterprise boundaries**
  - Perimeter is obscure
  - Identities are managed across boundaries
  - Trust relationships are established across boundaries

Threats to message level security

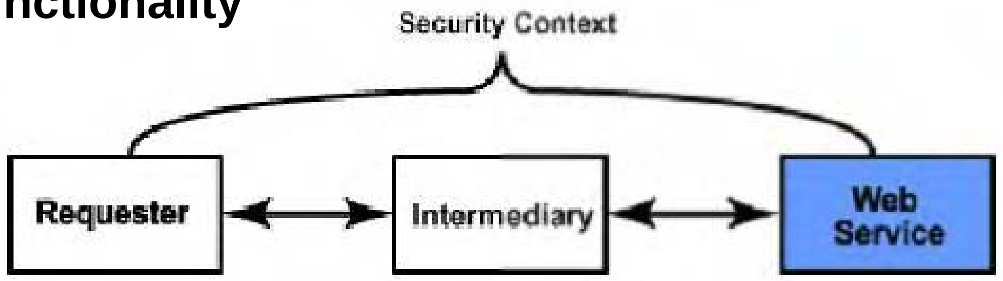
- *Message Alteration:* **Clear text messages may be changed**
- *Confidentiality:* **Messages may be read by external parties**
- *Man-in-the-middle:* **Original Requestor and Service Provider believe they are talking to each other, when in fact they are talking through a third party**
- *Spoofing:* **External party impersonates an authorized user and makes an unauthorized request**
- *Denial of Service:* **Preventing legitimate users from using a Web service**
- *Replay:* **An external party copies and later resends a message**

Point-to-point versus end-to-end security

- SSL/TLS offers several security features including authentication, data integrity, and data confidentiality, but only for individual hops



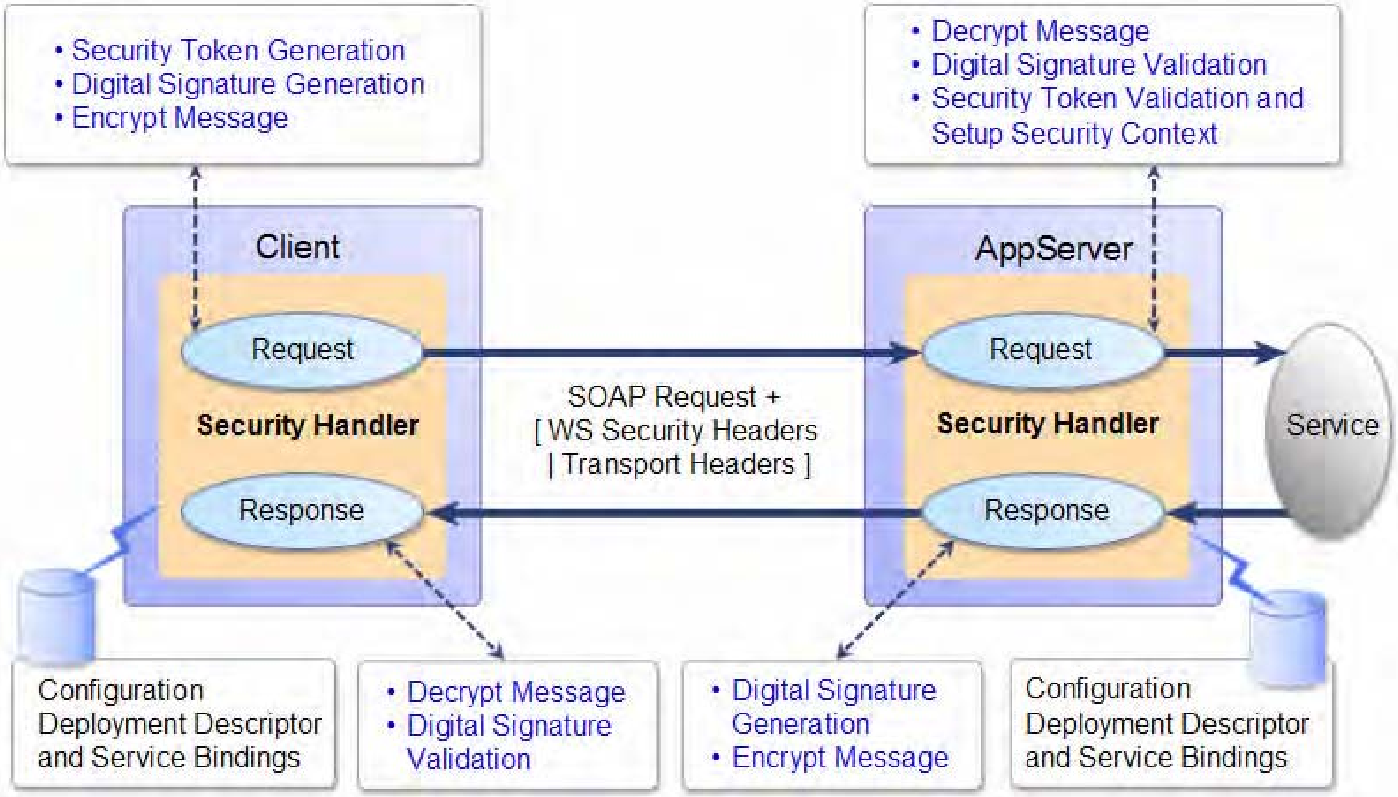
- What is needed in a comprehensive Web services security architecture is a mechanism that provides end-to-end security and greater functionality



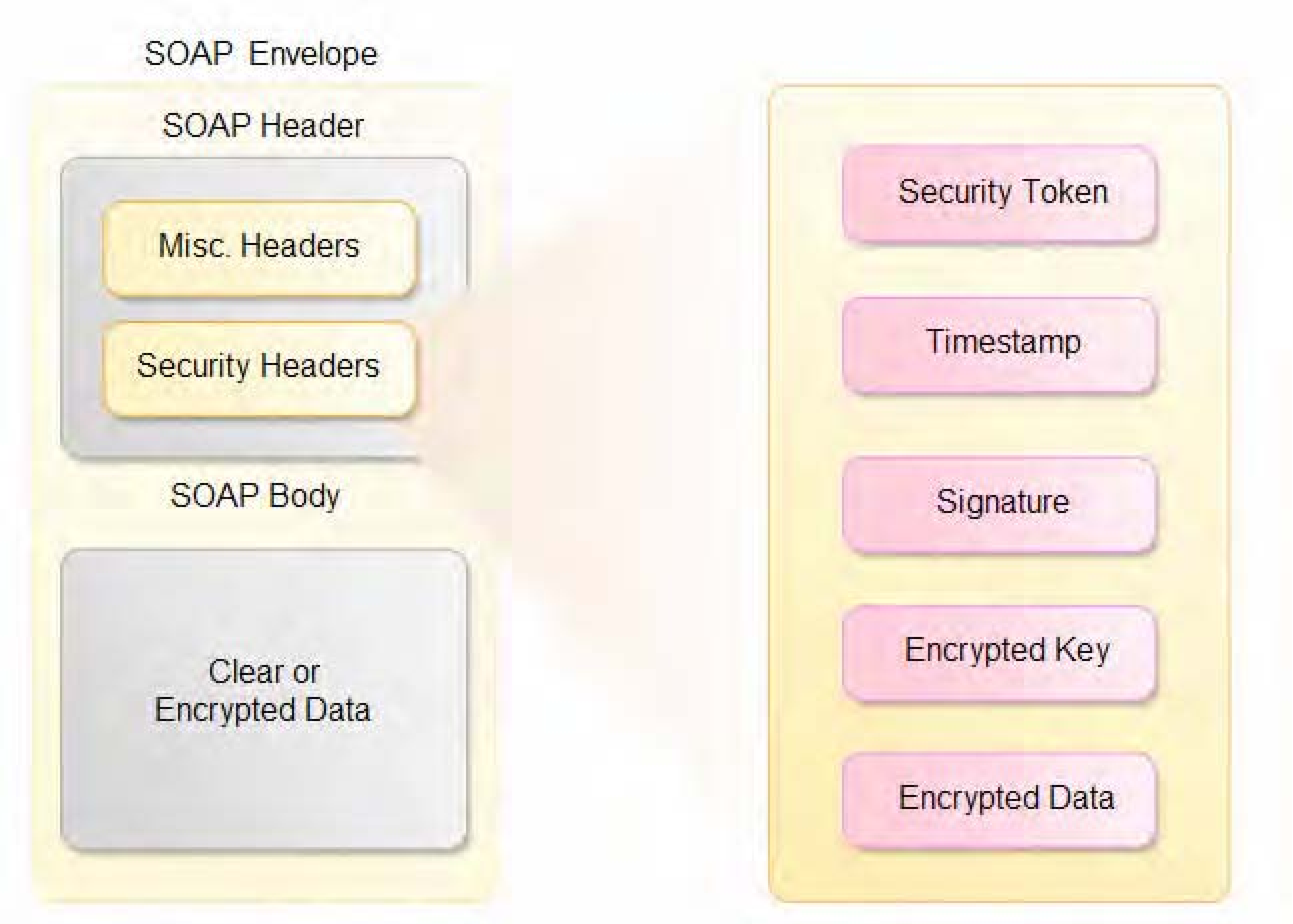
Agenda

- (Re)Introduction to Service Oriented Architecture (SOA)
- The importance of building a secure SOA
- Web services security standards
- Applying SOA security standards to your business

Web services security high level architecture


• Security Token Generation
• Digital Signature Generation
• Encrypt Message
• Decrypt Message
• Digital Signature Validation
• Security Token Validation and Setup Security Context
Client
AppServer
Request
Request
Security Handler
Security Handler
Response
Response
Service
SOAP Request +
[WS Security Headers
| Transport Headers]
Configuration Deployment Descriptor and Service Bindings
• Decrypt Message
• Digital Signature Validation
• Digital Signature Generation
• Encrypt Message
Configuration Deployment Descriptor and Service Bindings

SOAP message with Web Services Security



WS-Security Core Specification 1.1

- **Provides message level security which is used when building secure Web services**
- **Focused on message content protection and security token propagation**
- **Builds upon specific XML extensions and other supplemental specifications:**
  - XML Encryption
  - XML Signature
  - Username Token Profile
  - SAML Token Profile
  - X.509 Certificate Token Profile

Reference:
http://docs.oasis-open.org/wss/v1.1/wss-v1.1-spec-os-SOAPMessageSecurity.pdf

Defining the security constraints for a service

- **WS-Policy**
  - Provides a flexible and extensible grammar for expressing the capabilities, requirements, and general characteristics of entities in an XML Web services-based system
- **WS-SecurityPolicy**
  - Deals with defining "policy assertions" which are utilized by the WS-Security, WS-Trust and WS-SecureConversation specifications

Reference:
http://www.w3.org/Submission/WS-Policy/
http://docs.oasis-open.org/ws-sx/ws-securitypolicy/v1.2/ws-securitypolicy.html

Establishing and exchanging user identities

- **WS-Trust**
  - Uses the secure messaging mechanisms of WS-Security to define additional primitives and extensions for the issuance, exchange, and validation of security tokens
- **WS-Federation**
  - Describes how to use the existing Web services security building blocks to provide federation functionality, including *trust*, *single sign-on* (and *single sign-off*), and attribute management across a federation

Reference:
http://docs.oasis-open.org/ws-sx/ws-trust/200512/ws-trust-1.3-os.html
http://download.boulder.ibm.com/ibmdl/pub/software/dw/specs/ws-fed/WS-Federation-V1-1B.pdf?S_TACT=105AGX04&S_CMP=LP

Providing a context to multiple message flows

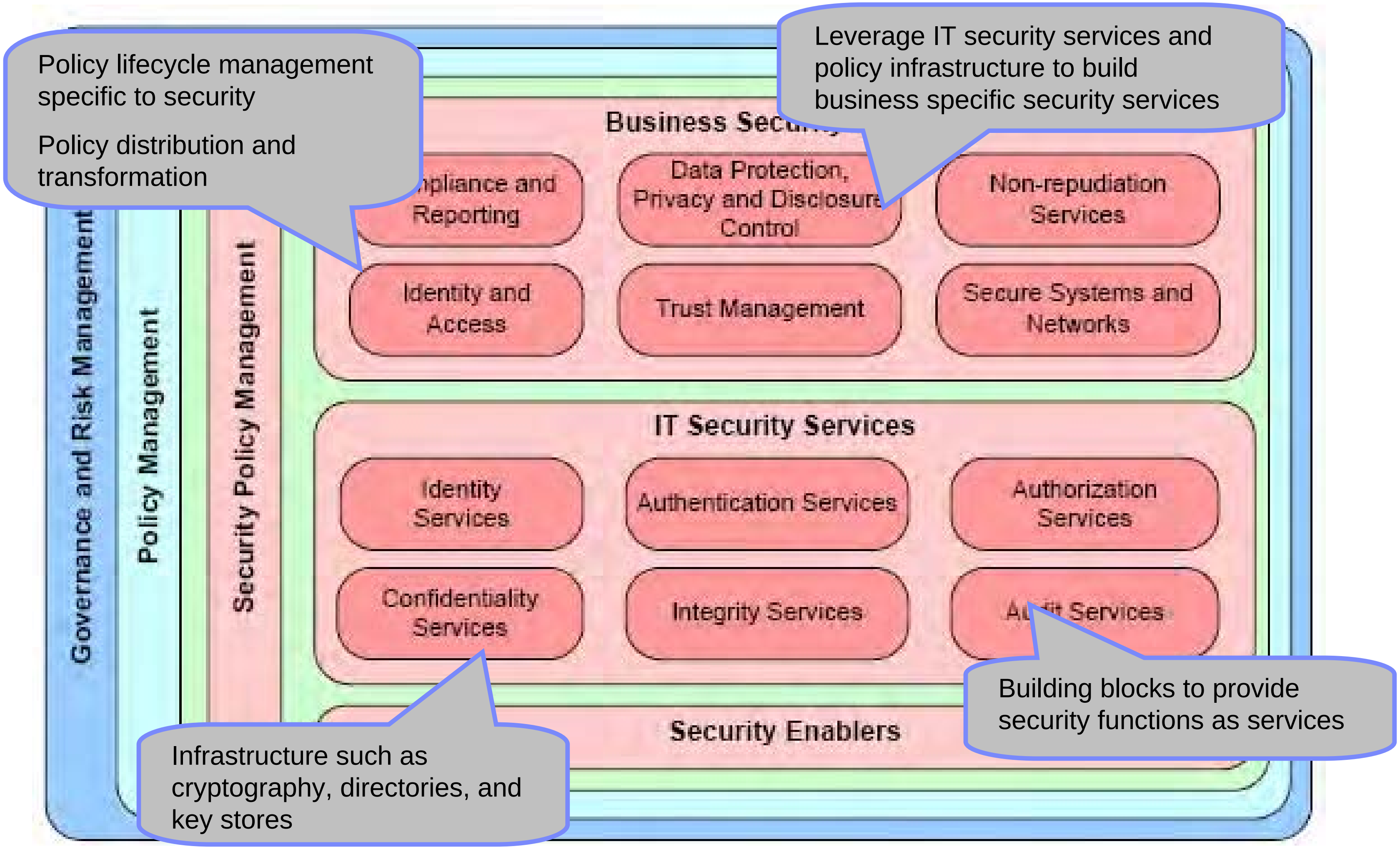
- **WS-SecureConversation**
  - Defines mechanisms for establishing and sharing security contexts, and deriving keys from security contexts, to enable a secure conversation

Reference:
http://docs.oasis-open.org/ws-sx/ws-secureconversation/200512/ws-secureconversation-1.3-os.html

Agenda

- **(Re)Introduction to Service Oriented Architecture (SOA)**
- **The importance of building a secure SOA**
- **Web services security standards**
- **Applying SOA security standards to your business**

IBM SOA Security Reference Model



Policy lifecycle management specific to security

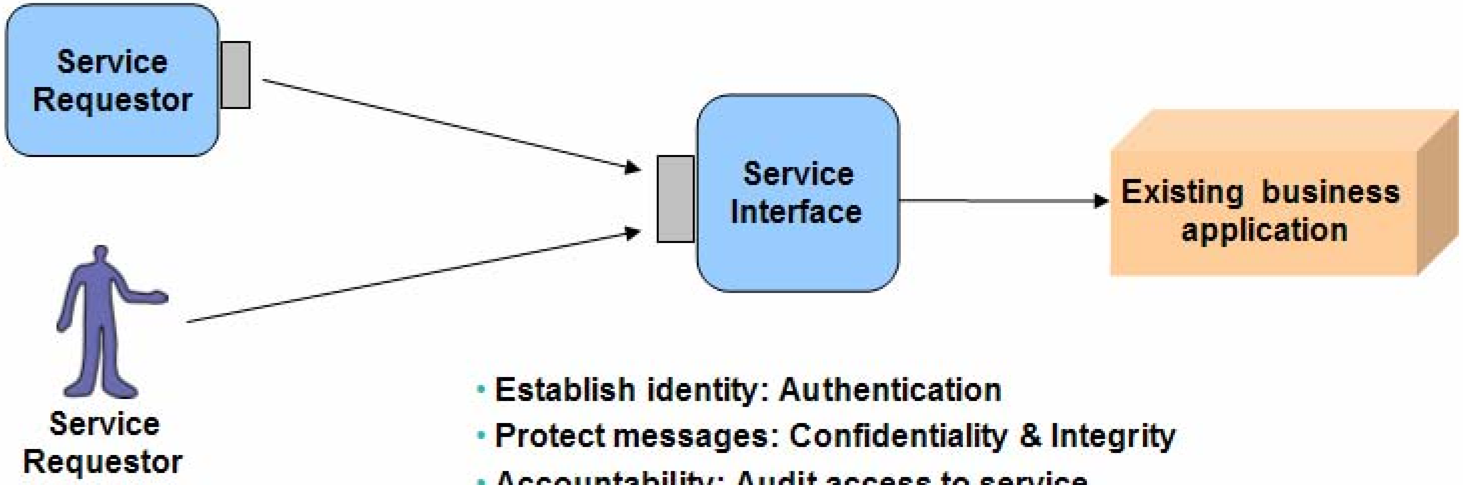
Policy distribution and transformation

Leverage IT security services and policy infrastructure to build business specific security services

Building blocks to provide security functions as services

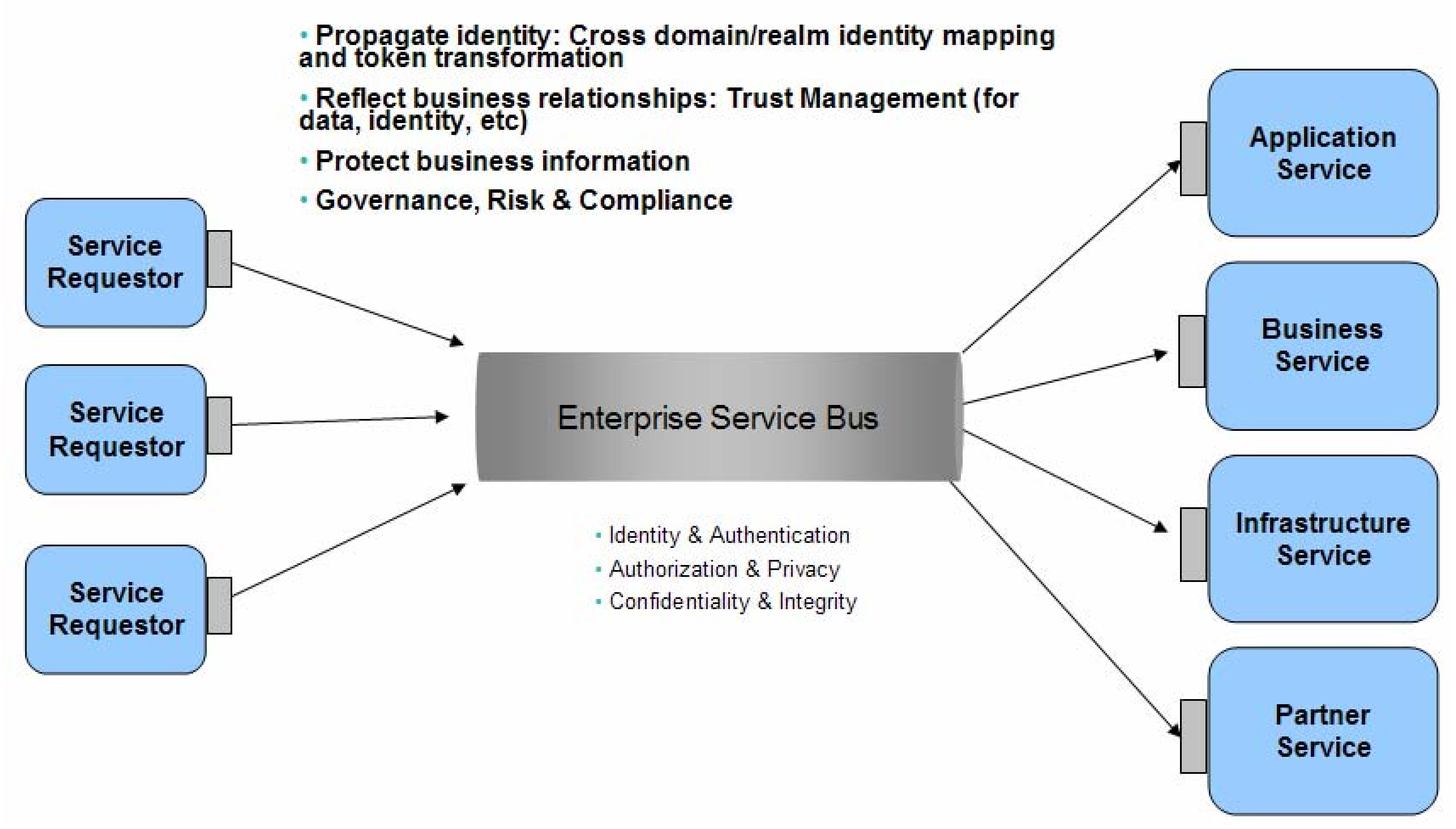
Infrastructure such as cryptography, directories, and key stores

Use Case 1 - Service creation



- Establish identity: Authentication
- Protect messages: Confidentiality & Integrity
- Accountability: Audit access to service
- User experience: SSO, Privacy

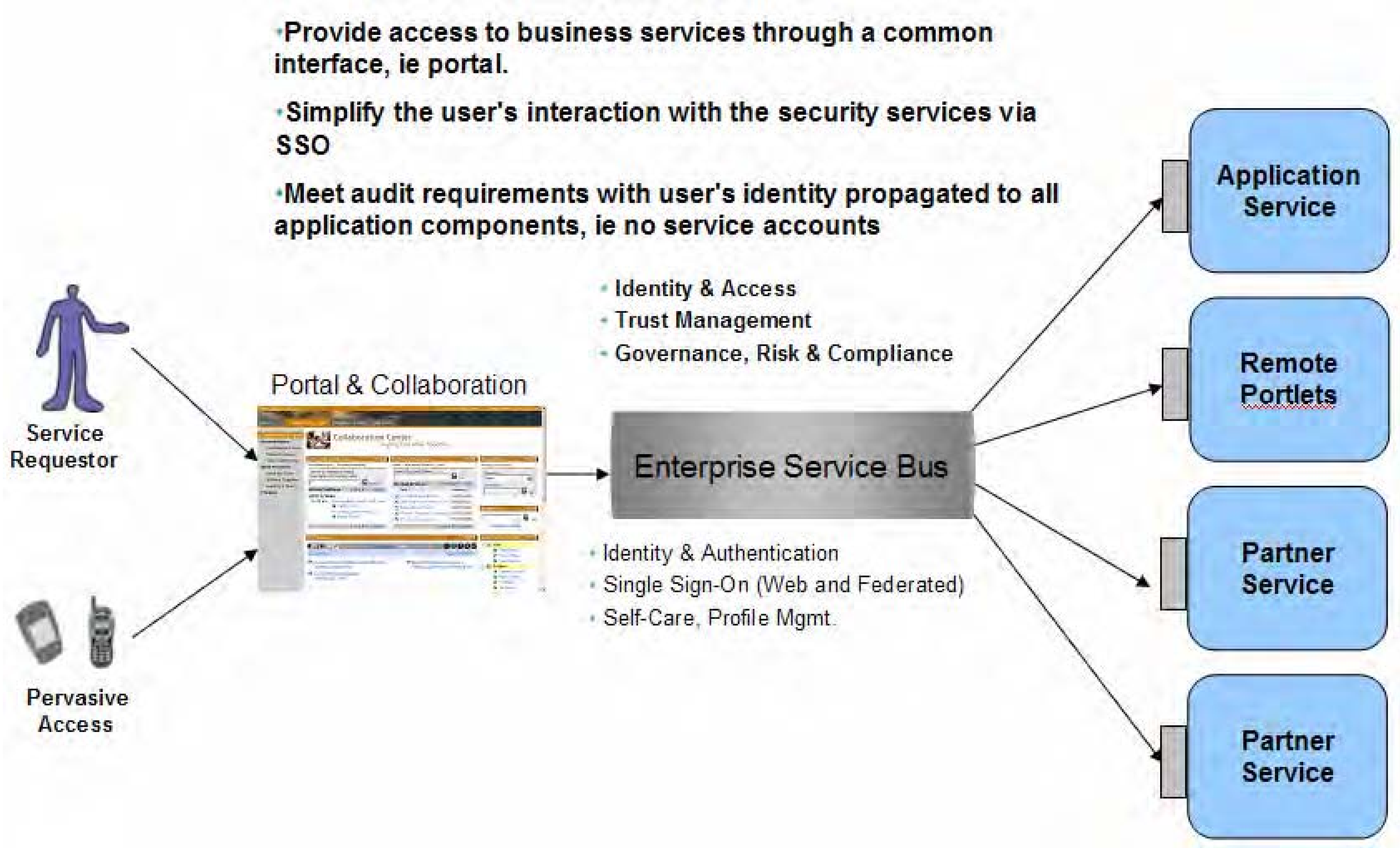
Use Case2 – Services integration



- Propagate identity: Cross domain/realm identity mapping and token transformation
- Reflect business relationships: Trust Management (for data, identity, etc)
- Protect business information
- Governance, Risk & Compliance

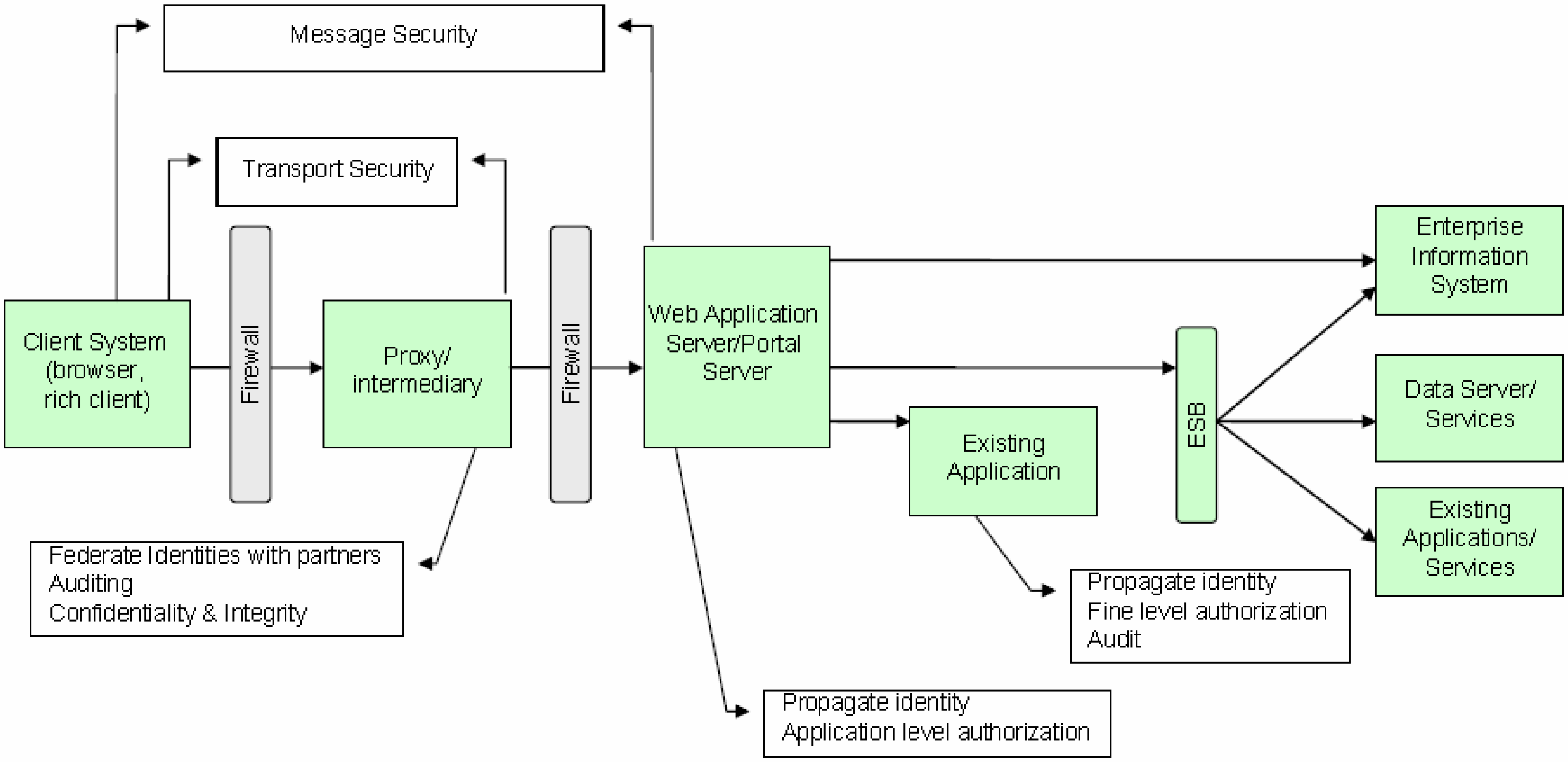
- Identity & Authentication
- Authorization & Privacy
- Confidentiality & Integrity

Use Case 3 – Service aggregation for collaboration



- Provide access to business services through a common interface, ie portal.
- Simplify the user's interaction with the security services via SSO
- Meet audit requirements with user's identity propagated to all application components, ie no service accounts

Security in a typical deployment architecture


Message Security
Transport Security
Client System (browser, rich client)
Firewall
Proxy/ intermediary
Firewall
Web Application Server/Portal Server
Enterprise Information System
ESB
Data Server/ Services
Existing Application
Existing Applications/ Services
Federate Identities with partners
Auditing
Confidentiality & Integrity
Propagate identity
Fine level authorization
Audit
Propagate identity
Application level authorization

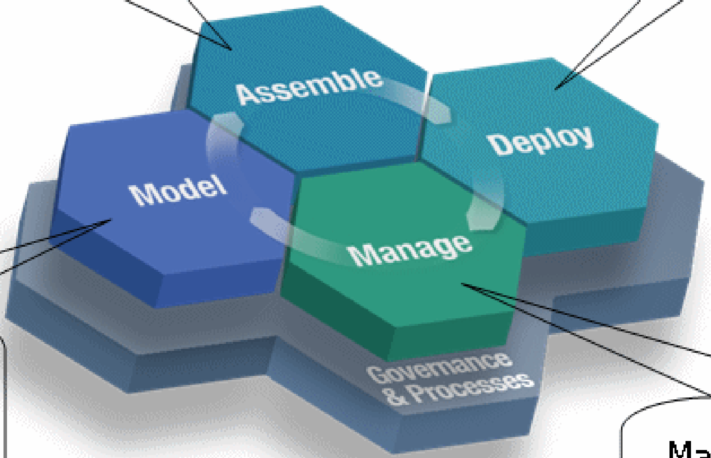
Security encompasses all stages of SOA life cycle

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



Define business and corporate security policies. Model security requirements and application security

Security policy officer
Security auditor
Business analyst

Manage application security
Manage identities
Monitor for compliance

IT administrator
Security administrator
Operator

Additional information

- ***Understanding SOA Security: Design and Implementation* – IBM Redbook**

- ***WS-I: Security Challenges, Threats, and Countermeasures Version 1.0***

  Reference:
  http://www.redbooks.ibm.com/abstracts/sg247310.html

- ***z/TPF Security Features for SOA***
  - Presentation in the **SOA Subcommittee** Tuesday morning

  Reference:
  http://www.ws-i.org/Profiles/BasicSecurity/SecurityChallenges-1.0.pdf

Trademarks

- IBM is a trademark of International Business Machines Corporation in the United States, other countries, or both.
- Other company, product, or service names may be trademarks or service marks of others.
- Notes
- Performance is in Internal Throughput Rate (ITR) ratio based on measurements and projections using standard IBM benchmarks in a controlled environment. The actual throughput that any user will experience will vary depending upon considerations such as the amount of multiprogramming in the user's job stream, the I/O configuration, the storage configuration, and the workload processed. Therefore, no assurance can be given that an individual user will achieve throughput improvements equivalent to the performance ratios stated here.
- All customer examples cited or described in this presentation are presented as illustrations of the manner in which some customers have used IBM products and the results they may have achieved. Actual environmental costs and performance characteristics will vary depending on individual customer configurations and conditions.
- This publication was produced in the United States. IBM may not offer the products, services or features discussed in this document in other countries, and the information may be subject to change without notice. Consult your local IBM business contact for information on the product or services available in your area.
- All statements regarding IBM's future direction and intent are subject to change or withdrawal without notice, and represent goals and objectives only.
- Information about non-IBM products is obtained from the manufacturers of those products or their published announcements. IBM has not tested those products and cannot confirm the performance, compatibility, or any other claims related to non-IBM products. Questions on the capabilities of non-IBM products should be addressed to the suppliers of those products.
- Prices subject to change without notice. Contact your IBM representative or Business Partner for the most current pricing in your geography.
- This presentation and the claims outlined in it were reviewed for compliance with US law. Adaptations of these claims for use in other geographies must be reviewed by the local country counsel for compliance with local laws.