IBM Software Group

Security Services for SOA
U of T – Class ECE 1770

March 30, 2006

Jim Davey, CISSP
IBM Software IT Architect
davey@ca.ibm.com

James Andoniadis
IBM Tivoli Security IT Specialist
james.andoniadis@ca.ibm.com

Learning Objectives

- Provide an introduction to security technologies, standards, architectures, and requirements necessary for enabling secure, trusted, multi-party, business transactions
- Understand security concepts, frameworks, terminology and key industry trends to facilitate communications with security specialists in the design and deployment of secure IT systems

Agenda – Part 1

- Security Overview
- Security Standards
- Security in an SOA Environment
- Security Capabilities of the WBI Family
  - WebSphere Application Server
  - WebSphere Messaging
  - WBI – Connect (aka WebSphere Partner Gateway)
- Summary

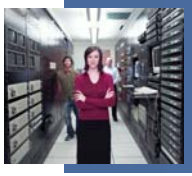
Agenda – Part 2

- Business and Enterprise Security Integration Context
- Identity And Access Management
- J2EE Security Model
- Federated Identity Management and Web Services Security
- Q & A

Security is an Enterprise Requirement that …

Affects Business Strategy

Impacts Business Processes and Operations



Helps Secure Business Applications

Needed to Secure the Infrastructure

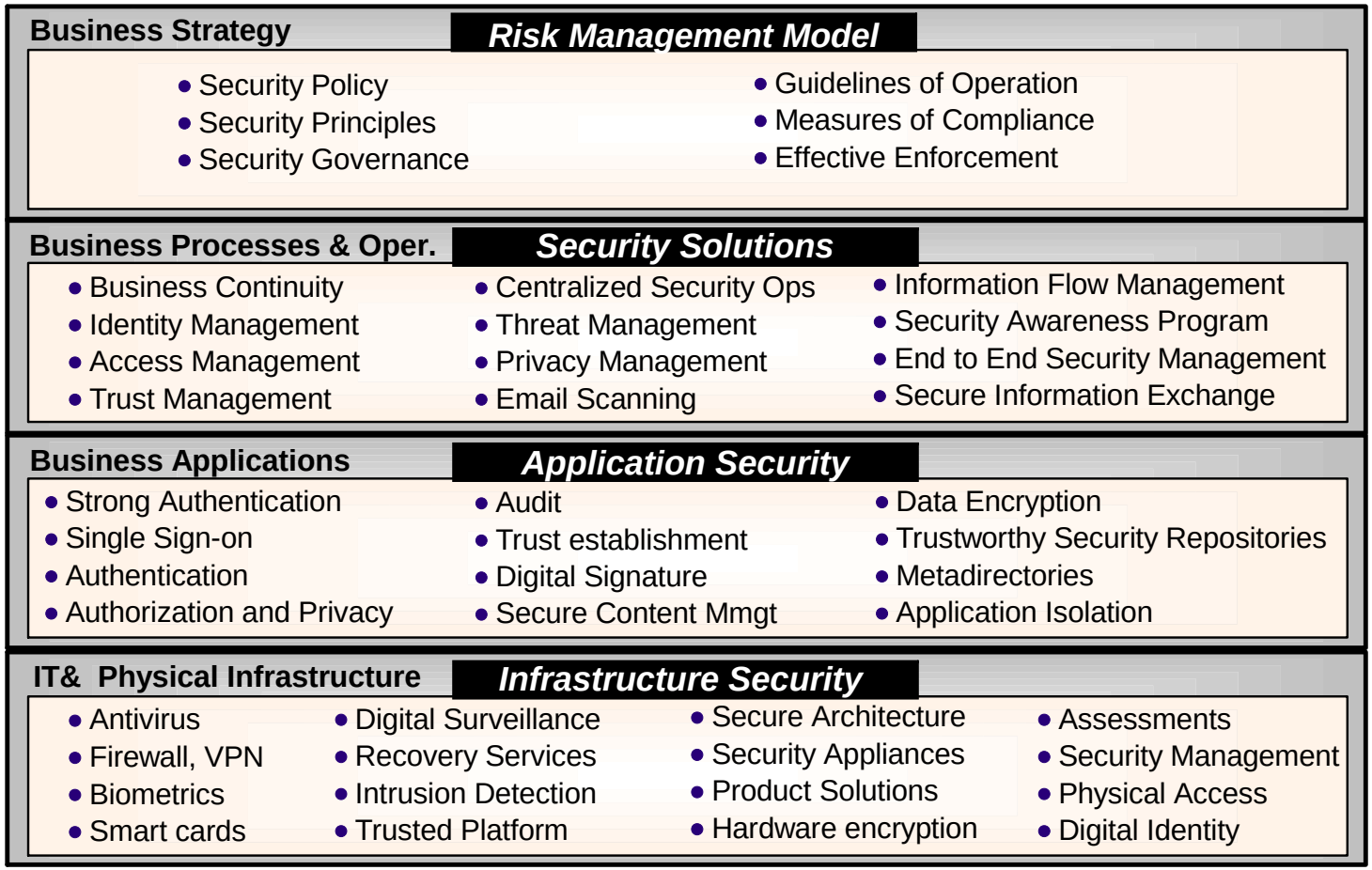
Enterprise Security View Point – How do I …

Business Strategy	• Protect data and strategic assets? • Build and protect trust with customers and partners? • Mitigate and manage the security risk? • Use security as e-business enabler?
Business Processes and Operation	• Ensure business continuity? • Reduce the cost of managing and administering security • Ensure the security controls remains appropriate over time? • Consistently enforce security and privacy policies • Ensure an end to end secure and trustworthy environment?
Business Applications	• Manage user identity across all enterprise? • Simplify and strengthen user authentication and authorization? • Quickly deploy security enhanced e-business initiatives? • Deploy solutions with appropriate security controls incl isolation? • Enforce accountability through audit?
Infrastructure	• Detect and manage intrusions? • Leverage new methods and technologies? • Manage the security infrastructure? • Verify and adhere to security and compliance policies?

.. to protect ..

Security: A Business Need

Security must be managed and integrated at the enterprise level.
It is about business, not technology

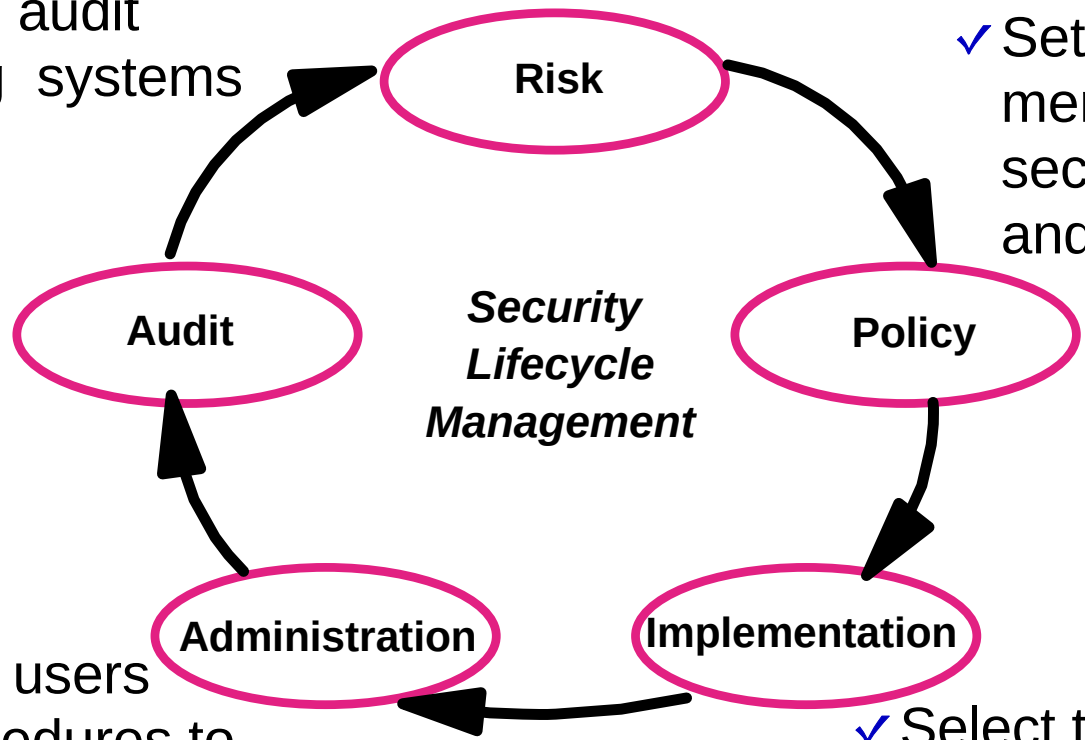


Security as a Business Process

- ✓ Identify assets
- ✓ Assign value
- ✓ Assess liabilities

- ✓ Identify owners
- ✓ Set require-ments for securing data and assets

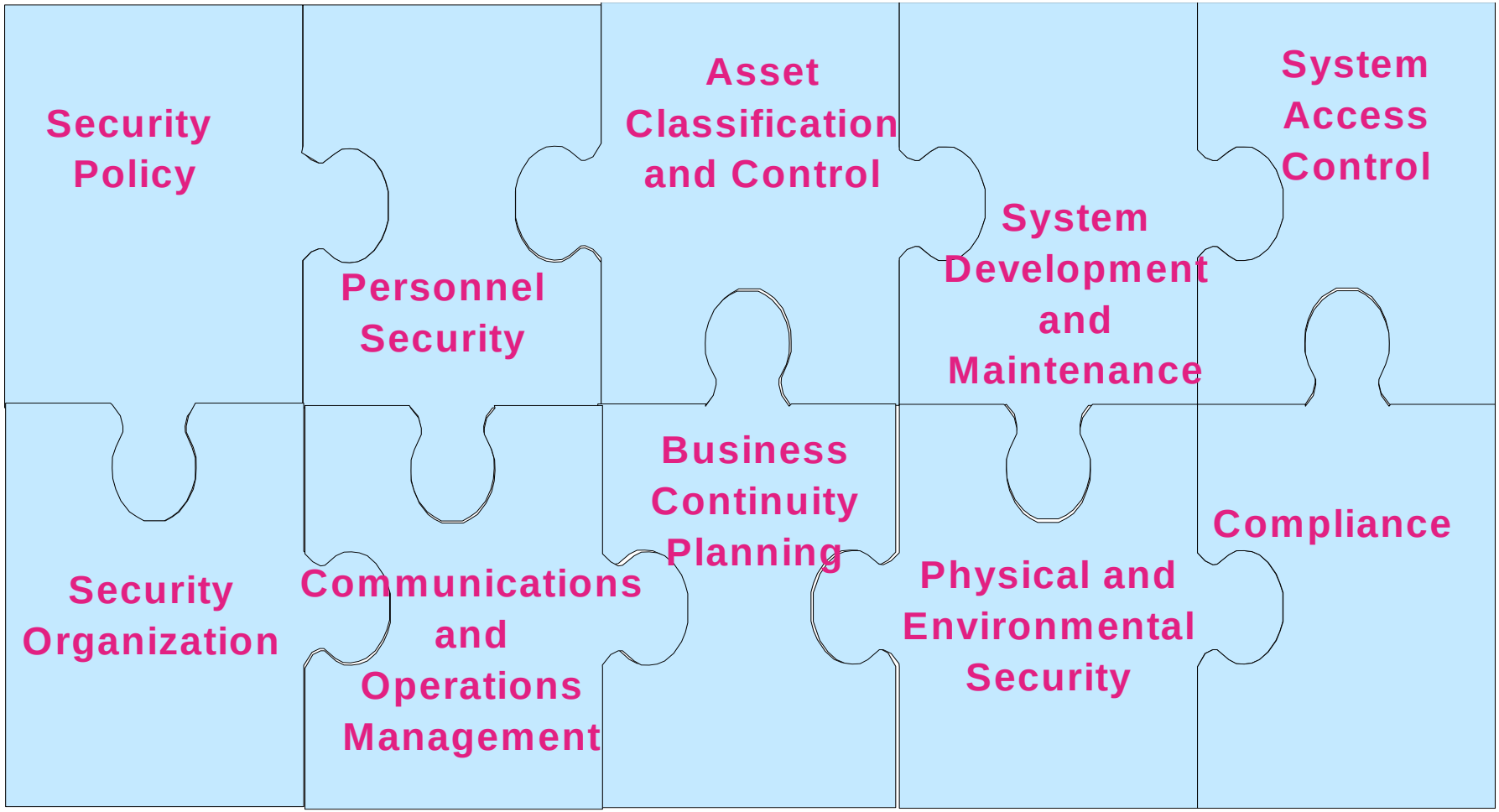
- ✓ Self-assessments
- ✓ Internal audit
- ✓ External audit
- ✓ Warning systems



- ✓ Educate users
- ✓ Set procedures to minimize risks

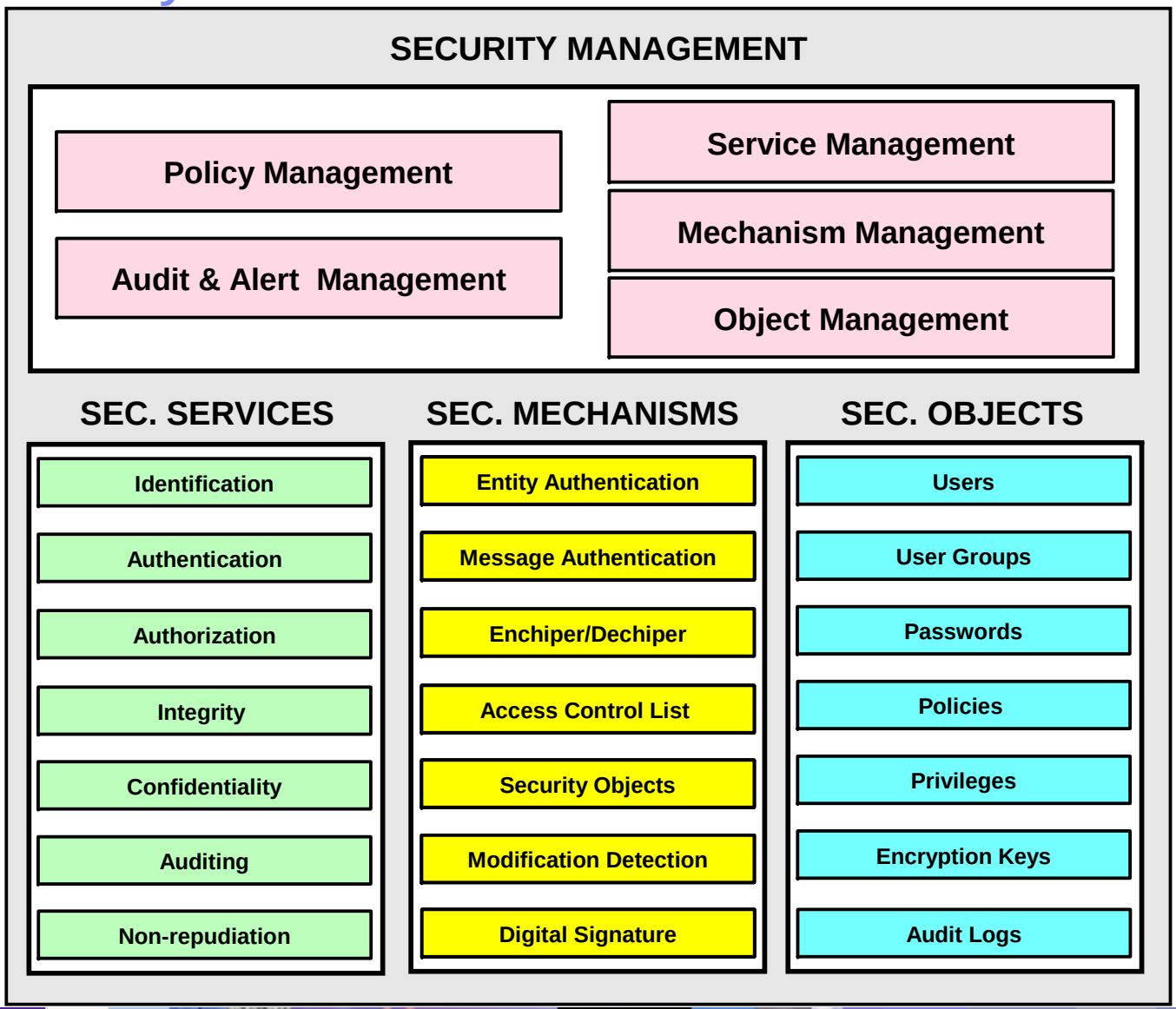
- ✓ Select technology
- ✓ Set management processes

British Standard 7799/ISO 17799: A Code of Practice for Information Security Management, is a compilation of more than 100 best security practices.



Security Standards

ISO Security Standard 7498-2



Security Services

- **Authentication**
  - User Identity validation
  - Username/Password, Token, X.509 Certificate
- **Authorization**
  - Authorization is the process of determining whether an identified entity has the authority to access a specific service in a secure domain (Policies/Roles/Groups)
  - Typical authorization engines protect larger collections: Queues not Messages, Files not Records or Tables not Rows
- **Accountability/Auditing**
  - Hold accountable for what an authorized principal does

Security Services

- **Data Integrity**

  Data integrity is a process, verifying that the content of a message has not been modified

  Primarily used with hashing and digital signatures

- **Confidentiality**

  Data confidentiality is to protect data against unauthorized disclosure

  Primarily used with key encryption

- **Privacy**

  The right of Individuals to determine for themselves when, how and to what extent information about them is communicated to others.

  Note: Privacy is what, how and when data is used that is similar to private property

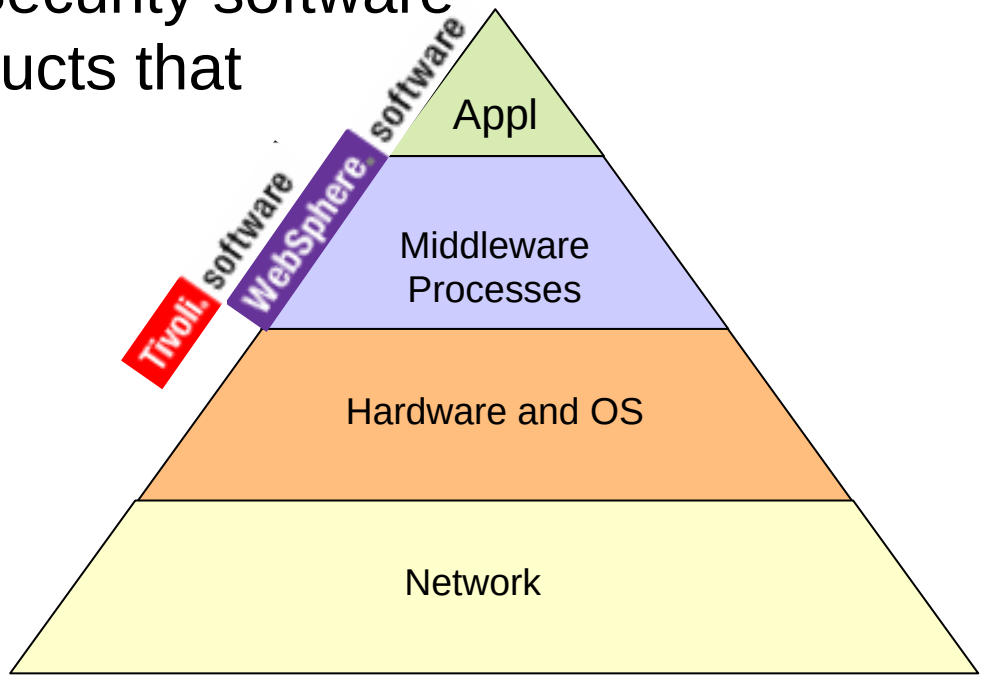
- **Non-repudiation**

  To ensure that a transferred message has been sent and received by the parties claiming to have sent and received the message. An irrefutable evidence has to be kept for future references.

Positioning IBM Middleware in the Security Services Pyramid

- Business Applications should utilize Security features from services provided by a layered **Security Services Pyramid**

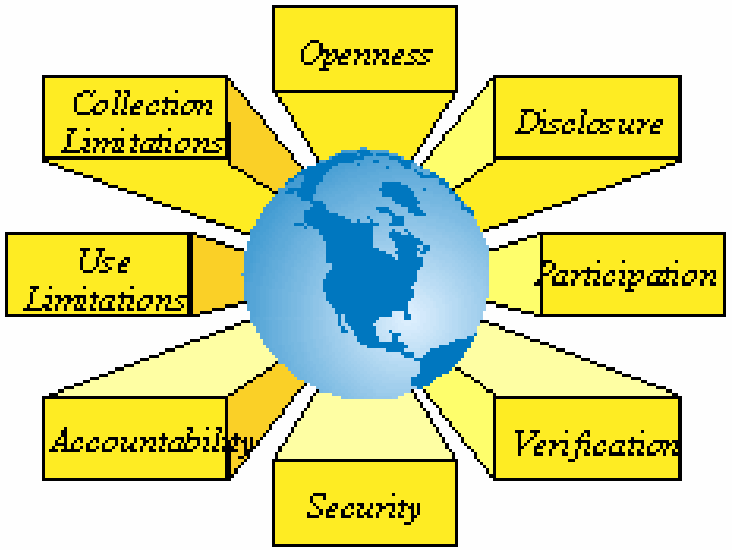
- **WebSphere** and **Tivoli** Security software are IBM Middleware products that leverage underlying services of Network, Hardware, and OS



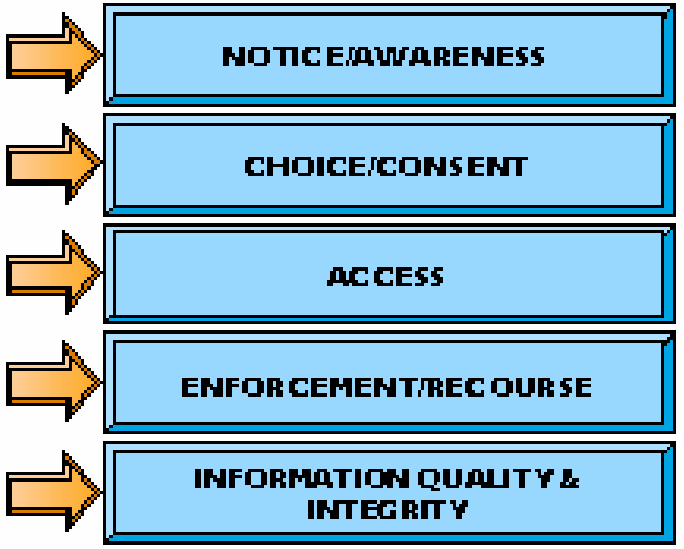
Privacy vs. Security

- The right of individuals to determine for themselves when, how and to what extent information about them is communicated to others.

Privacy Principles



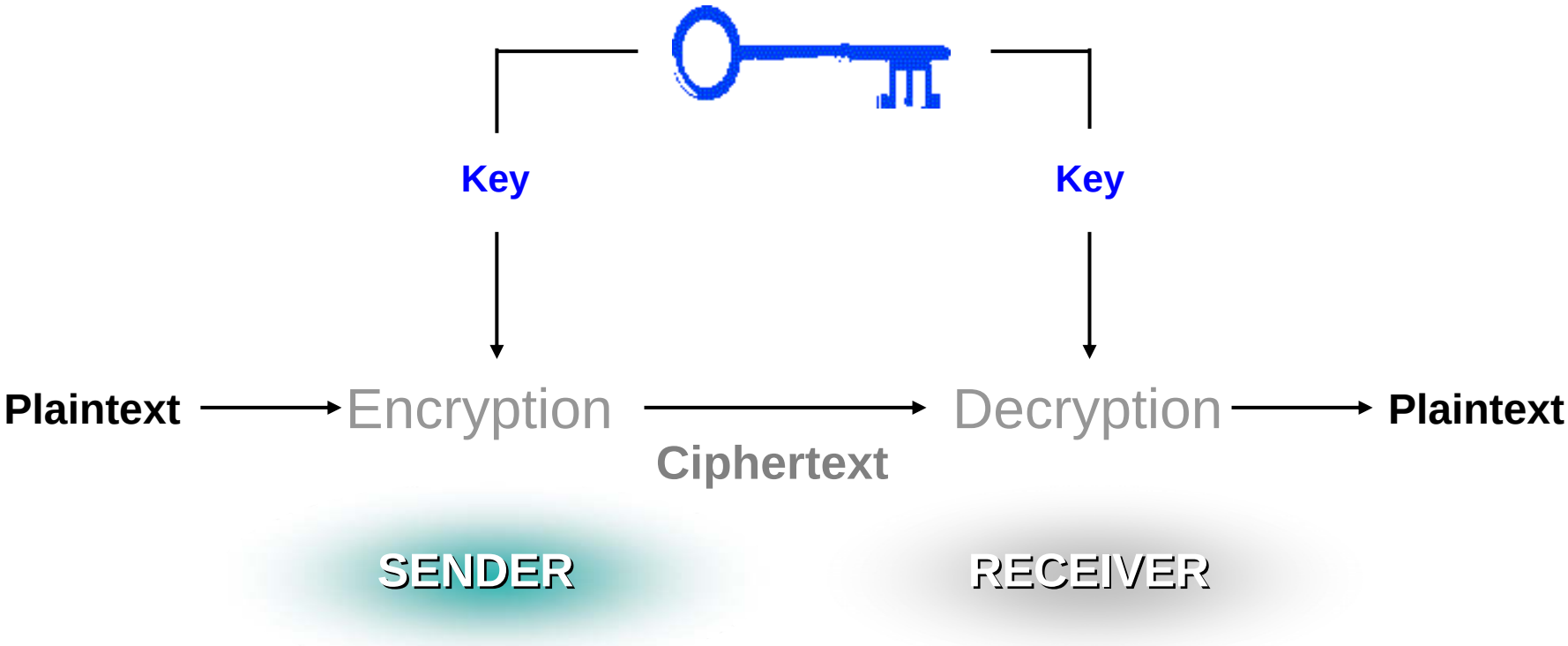
Protecting Privacy
via Fair Information Practices



- Privacy differs from Confidentiality, which is a security objective that refers to the protection of sensitive information from disclosure

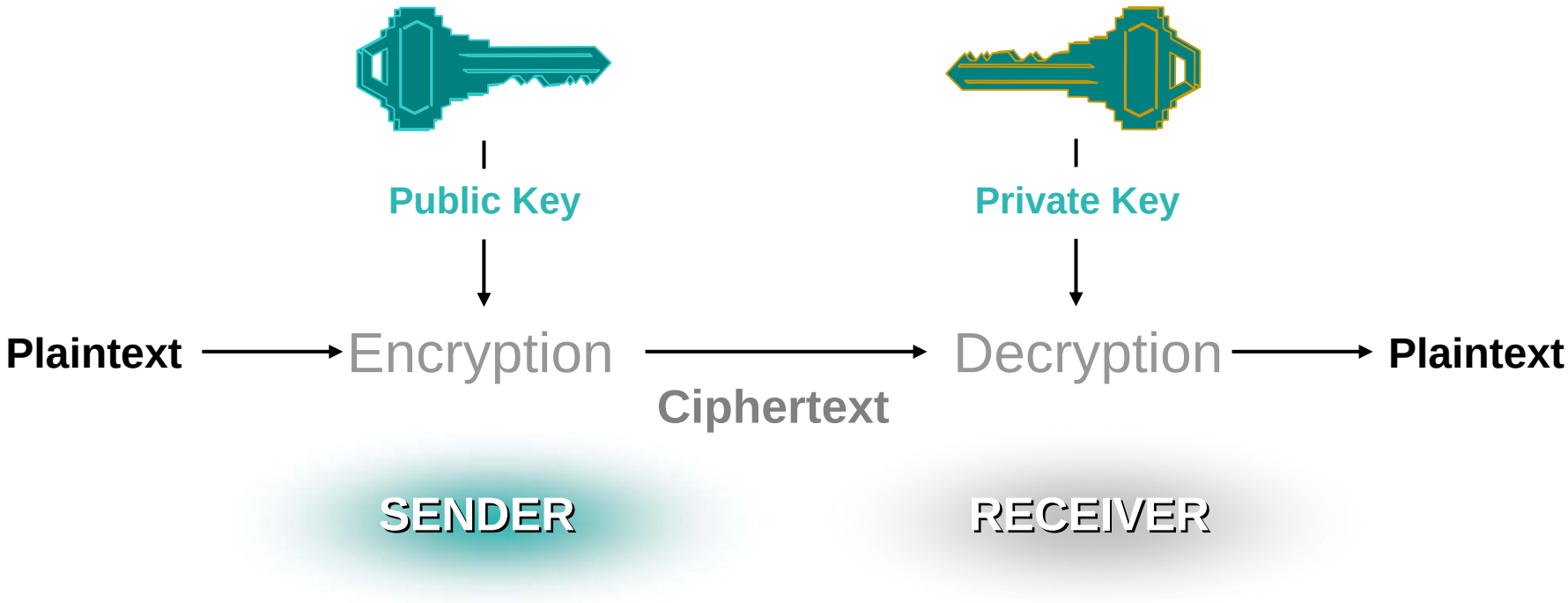
Basic Encryption

Symmetric Key Encryption (Secret Key)



Public Key Encryption

Asymmetric Key Encryption



Service Oriented Architecture

"A service-oriented architecture is essentially a collection of services. These services communicate with each other. The communication can involve either simple data passing or it could involve two or more services coordinating some activity. Some means of connecting services to each other is needed."

"A service in SOA is an exposed piece of functionality with three properties:

1. The interface contract to the service is platform-independent.
2. The service can be dynamically located and invoked.
3. The service is self-contained. That is, the service maintains its own state. "

SOA and Security

Service Oriented Architecture Paradigm changes the prospect of security

SOA:

- Provides cross enterprise interoperations
- Focuses on federated interoperability
- Allows execution of a sub-component
- Is for non-human facing invocation
- Enables dynamic service binding
- Goes beyond the Transport layer
  - Data integrity beyond transport
  - Data privacy beyond transport

Traditional security systems don't meet the SOA security requirements!

SOA and Security – What do we need?

"We need an architecture for interoperating across standalone security infrastructures."

- Service Oriented Security Architecture

  "…create a unified end-to-end chain of trust that spans independently secured networks."

The Intersection of Web Services and Security Management:

A Service-Oriented Security Architecture,

A META Group White Paper:
http://www3.ca.com/Files/IndustryAnalystReports/SOA.pdf

SOA – Then along came Web Services

- SOA evolves from the distributed objects thinking. RPC, Microsoft's Distributed Component Object Model (DCOM) and Object Management Group's (OMG) CORBA are among the early implementations of such concept -- remote access to loosely coupled service components . However, they are different.
- SOA exists long before WS. One can build an SOA without WS!
- Web Services is an implementation of such remote access concepts and is the first implementation of SOA through XML technology.

Secure, Reliable, Transacted Web Services

From joint IBM/MSFT WS Whitepaper at
http://msdn.microsoft.com/webservices/default.aspx?pull=/library/en-us/dnwebsrv/html/wsoverview.asp

Web Services Security

Learning how the industry fill the security gaps in Web Services helps us understand SOA Security better.

- SOAP over SSL such as HTTPS is not enough
- IBM, Microsoft, & Verisign proposed in April 2002 a WS-Security Language

  http://www-106.ibm.com/developerworks/webservices/ library/ws-secure/
- OASIS rectified the WS-Security proposal in April 2004

  It covers only the security in SOAP messaging, not all aspects of the security problems WS needs to solve

Web Services Security Building Blocks

- OASIS's security model is built on top of existing security protocols, API's and best practices for distributed, interoperable environments.
- Proxy model of security can be implemented in Web Service Gateway which intercepts all SOAP traffic and does security screening there
- A Web Services firewall which can offload security checking such as XML attack detection XML syntax checking from the Soap Server
- There are options to chose from for Identity Management such as Tivoli Federated Identity Management (FIM), Liberty Alliance's model and WS-Federation

Web Services and XML

Since Web Services are XML based, it carries over a few things from XML world in terms of security:

- XML Encryption

  Support encryption of an entire document or only selected portions. The smallest portion can be an element.

- XML Signature

  Recommends how to sign an XML data and how to present the resulting signature in XML.

  All or selected portion of an XML data can be signed.

- SAML (Security Assertion Markup Language)

  Defines a standard way to represent authentication, attribute, authorization information which can be understood by applications across enterprise boundary

- XACML (eXtensible Access Control Markup Language)

  General purpose access control language using SAML model as a base

Web Services and J2EE Security

There are a few things needed to support Web Services in J2EE in terms of security:

- JAAS (Java Authentication and Authorization Service)

  Is a set of APIs that enable services to authenticate and enforce access controls upon users. It implements a Java technology version of the standard Pluggable Authentication Module (PAM) framework, and supports user-based authorization.

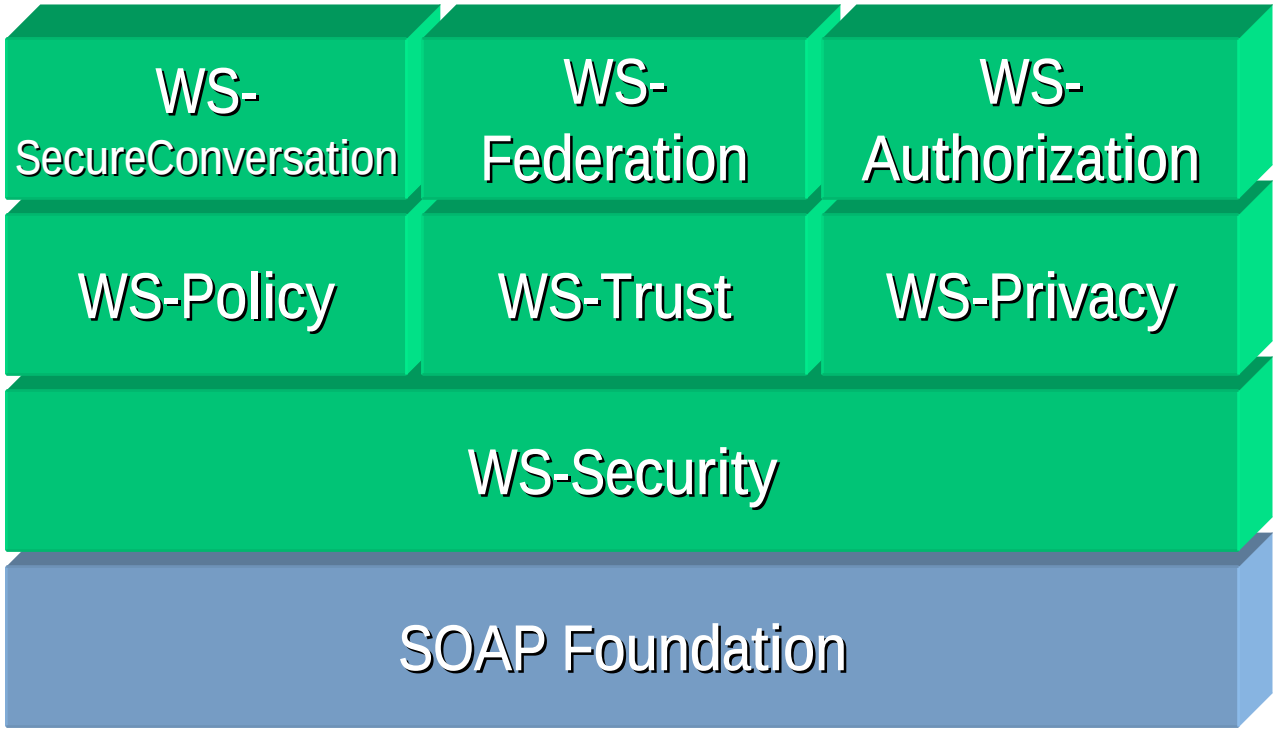
- JSSE (Java Secure Socket Extension)

  Provides SSL support for Java applications

- JCE (Java Cryptography Extension)

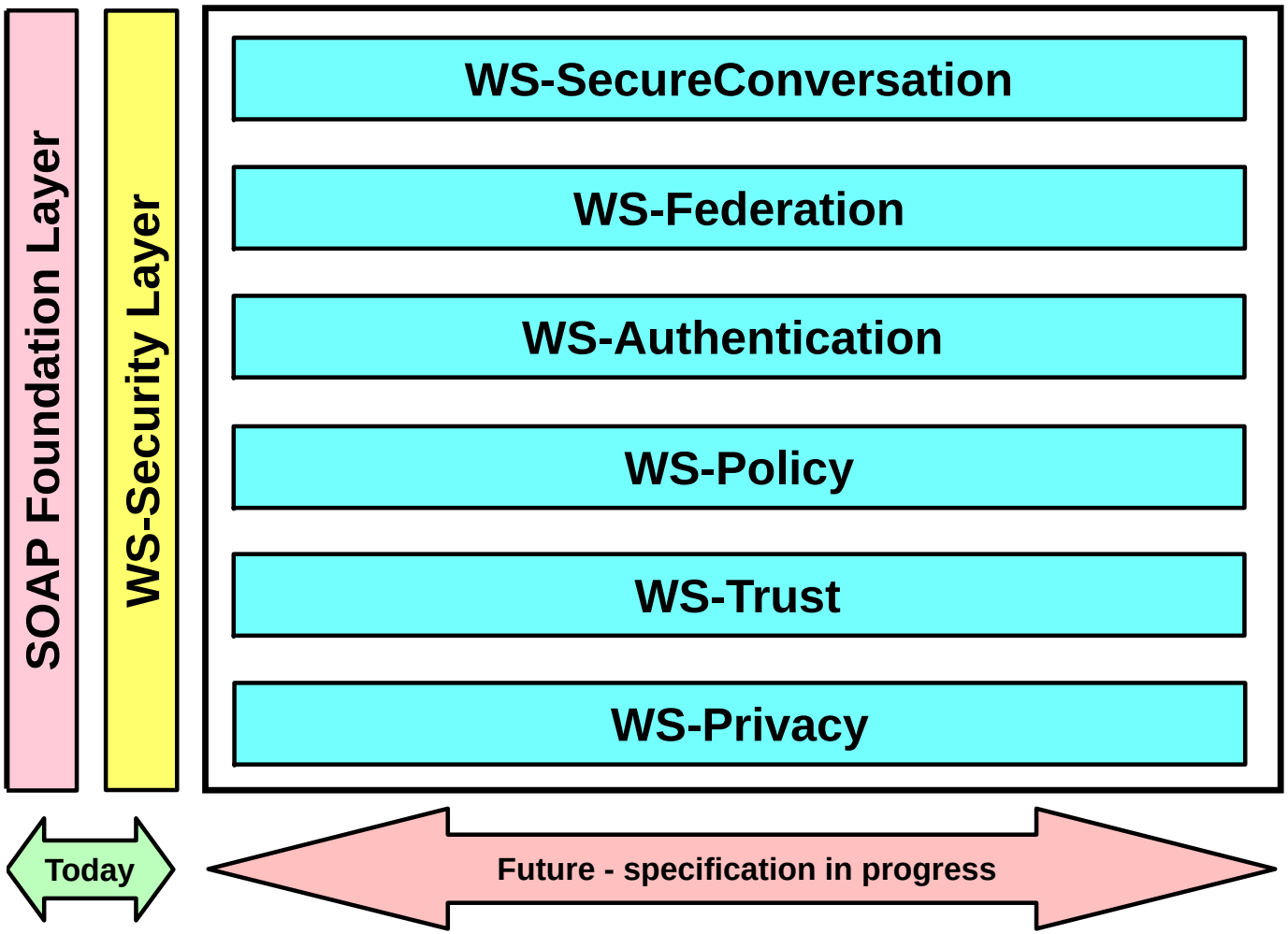
  Is a set of packages that provides a framework and implementations for encryption, key generation and key agreement, and Message Authentication Code (MAC) algorithms. Support for encryption includes symmetric, asymmetric, block, and stream ciphers. The software also supports secure streams and sealed objects.

Web Services Security Specifications



www.ibm.com/developerworks/library/ws-secmap

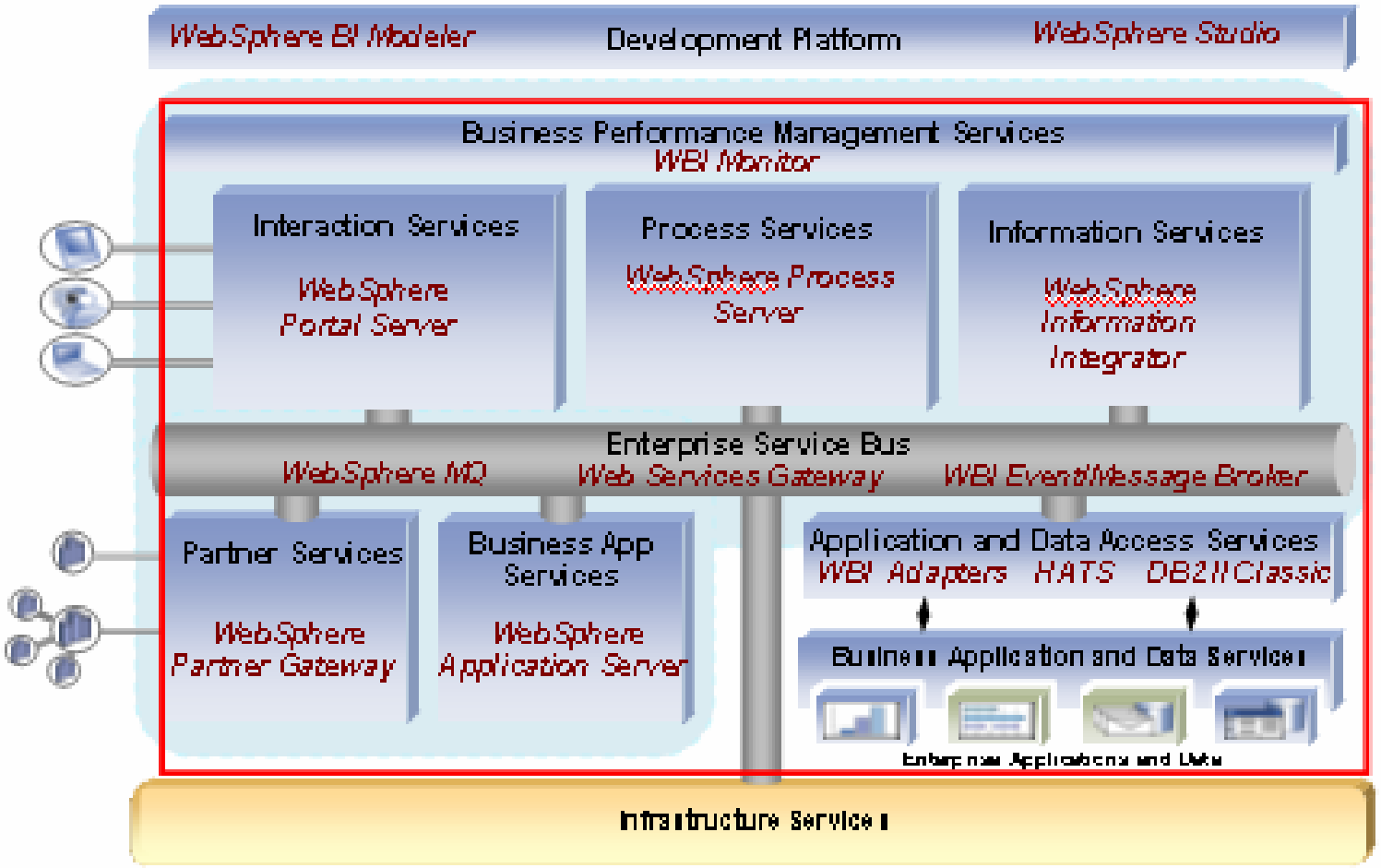
Web Services - Security standards



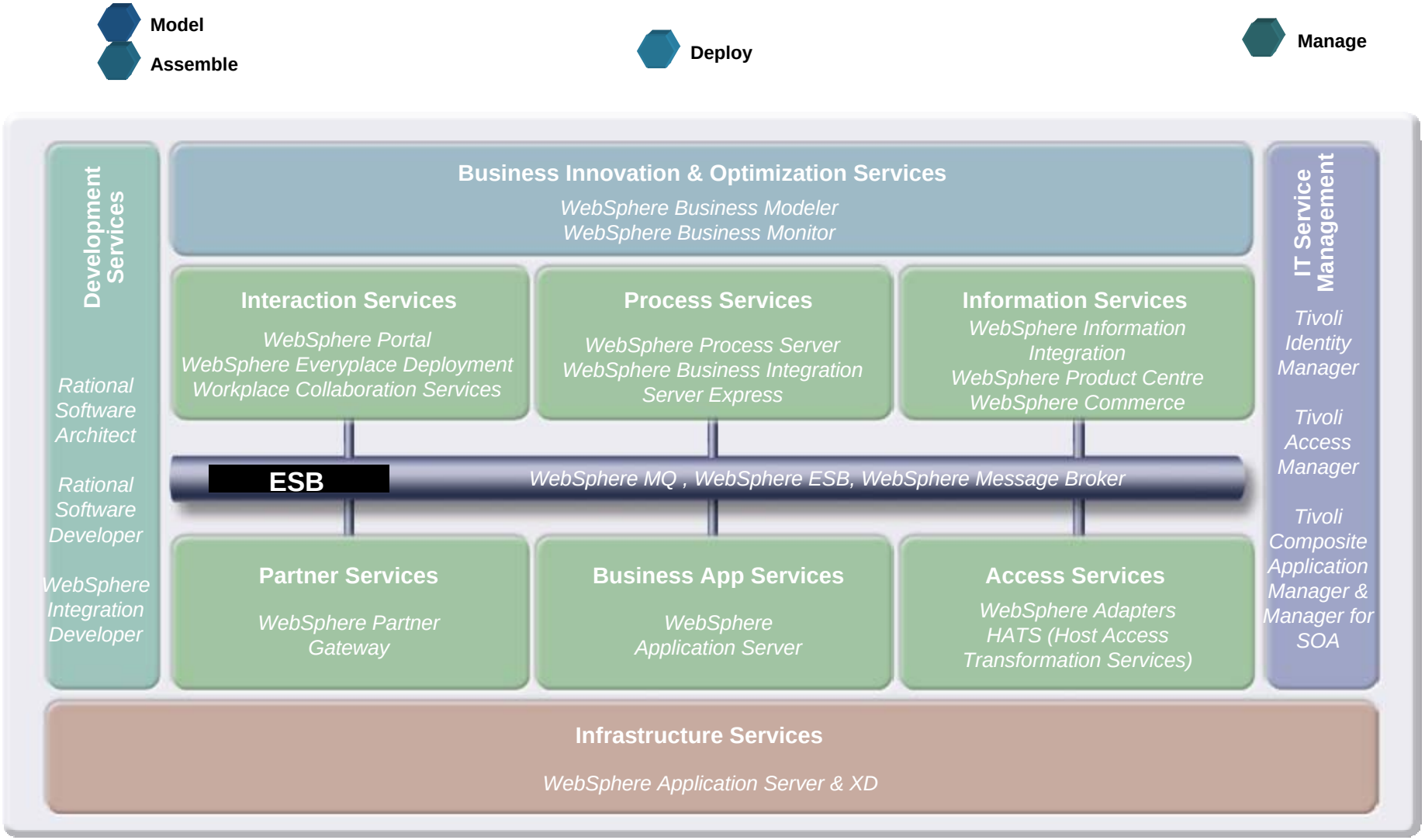
Security Features

Securing BI Reference Architecture

IBM Software Offerings



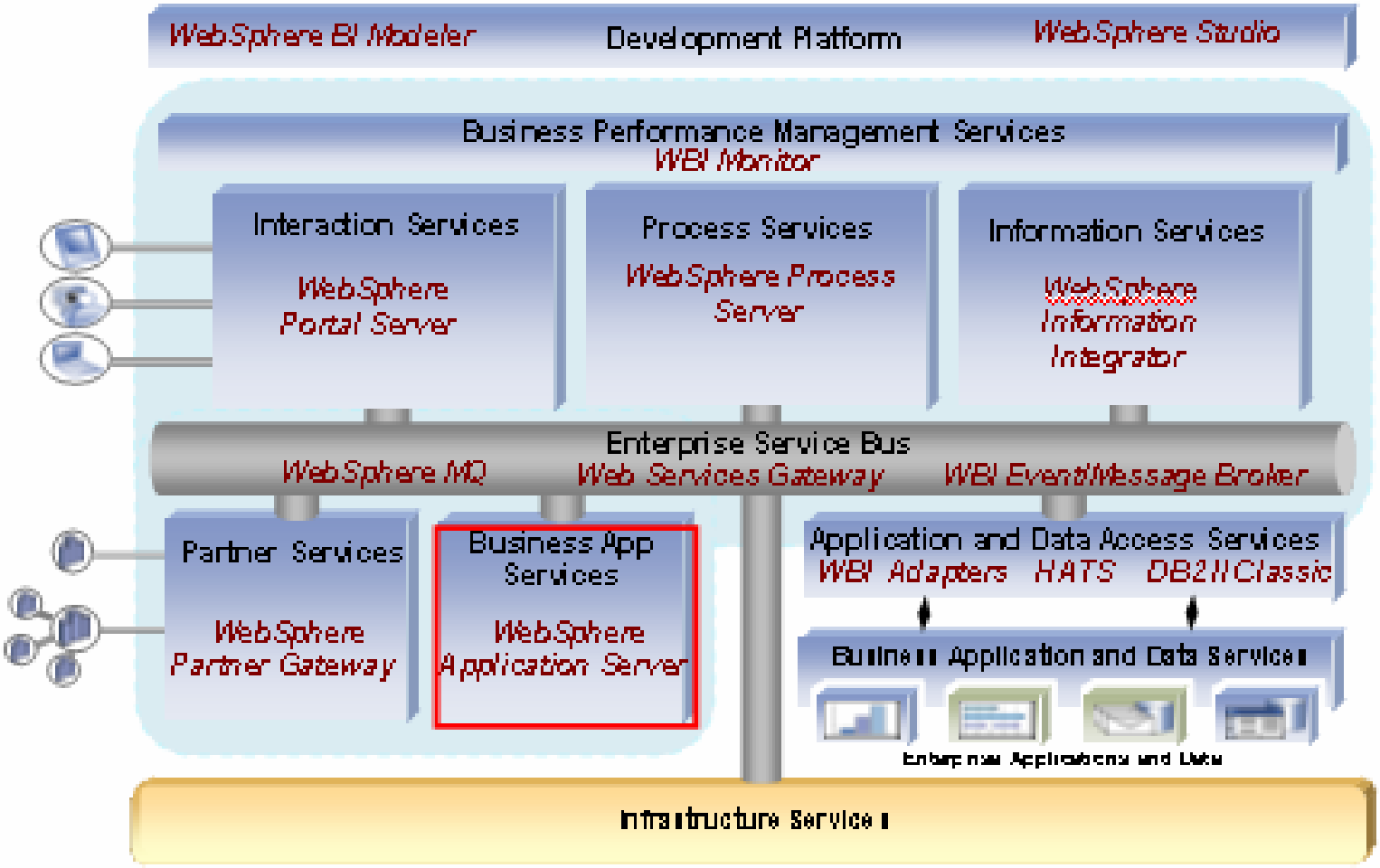
SOA Reference Architecture



Security Features

Securing BI Reference Architecture

IBM Software Offerings



Security Features

WebSphere Application Server Security

Key Components

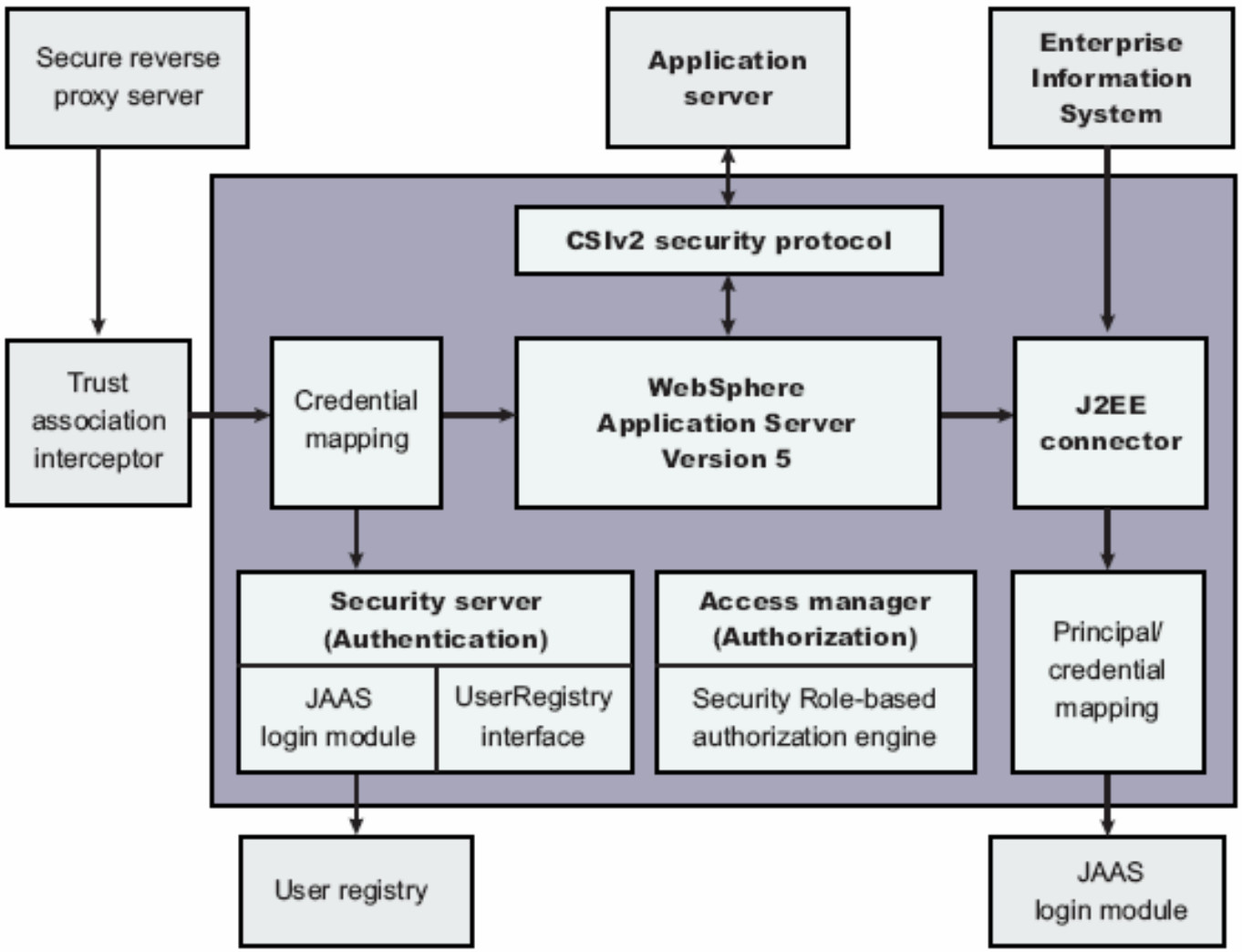
- Trust Association Interceptors (TAI)
- Credential Mapping
- Security Server - Authentication
- Access Manager - Authorization
- Common Secure Interoperability Protocol (CSIv2) – Java clients
- Policy files
- User Registry

Key Capabilities

- Plays an integral part of the multi-tier enterprise computing framework
- Provides pluggable User Registry, Authentication, and Authorization
- Supports SSO

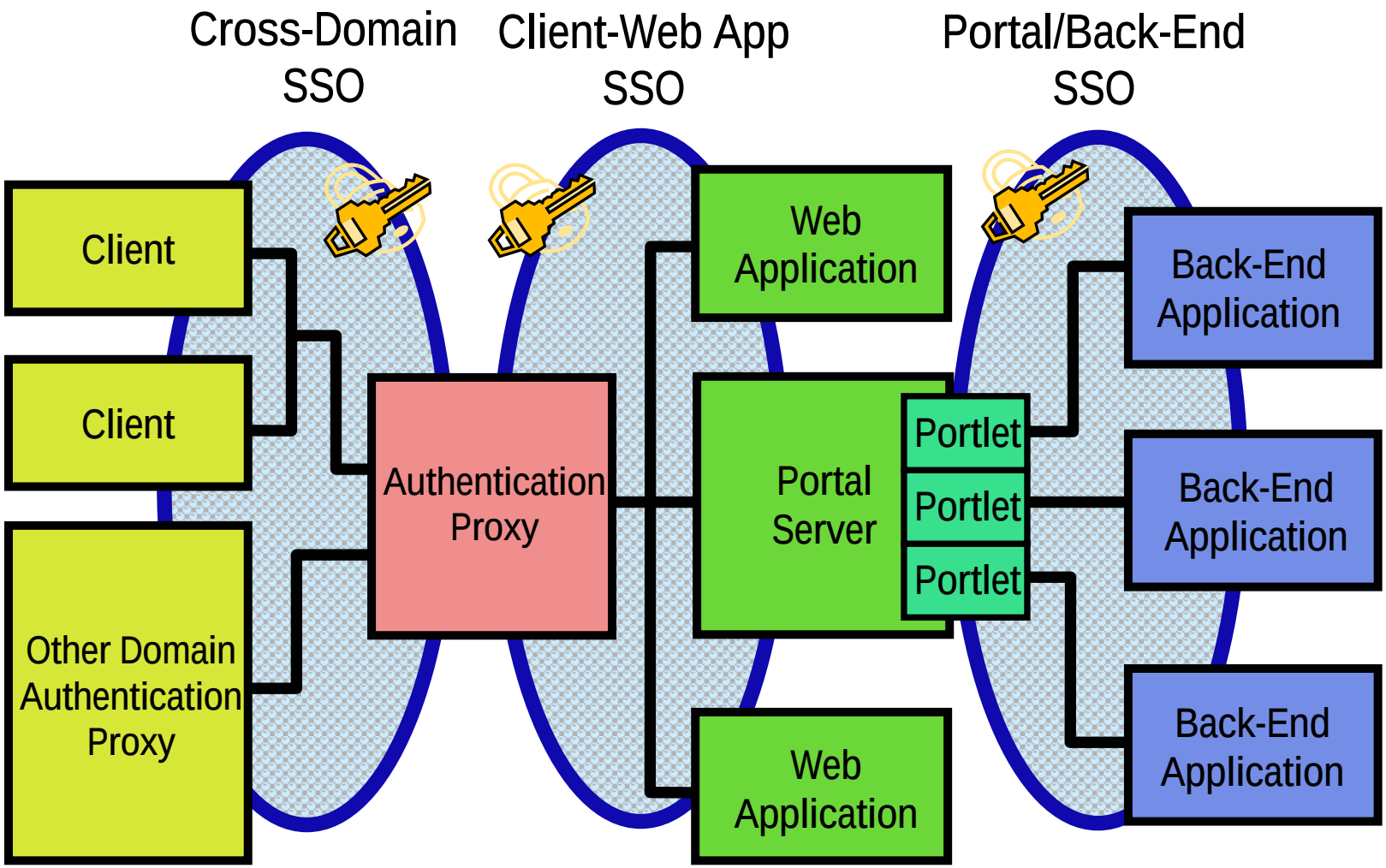
Security Features

WebSphere Application Server



Security Features

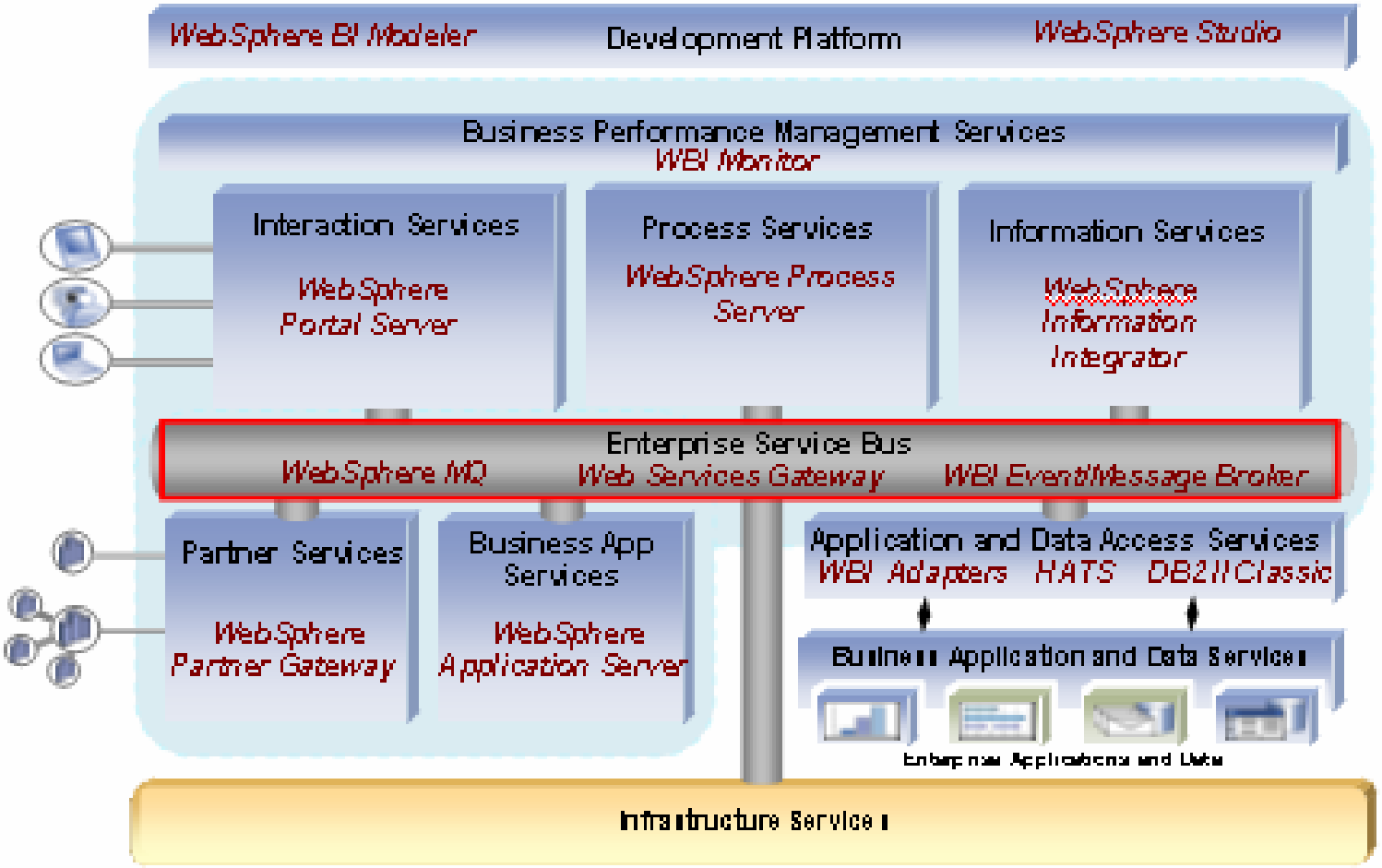
Multiple Realms of Single Sign-On



Security Features

Securing BI Reference Architecture

IBM Software Offerings



Security Features

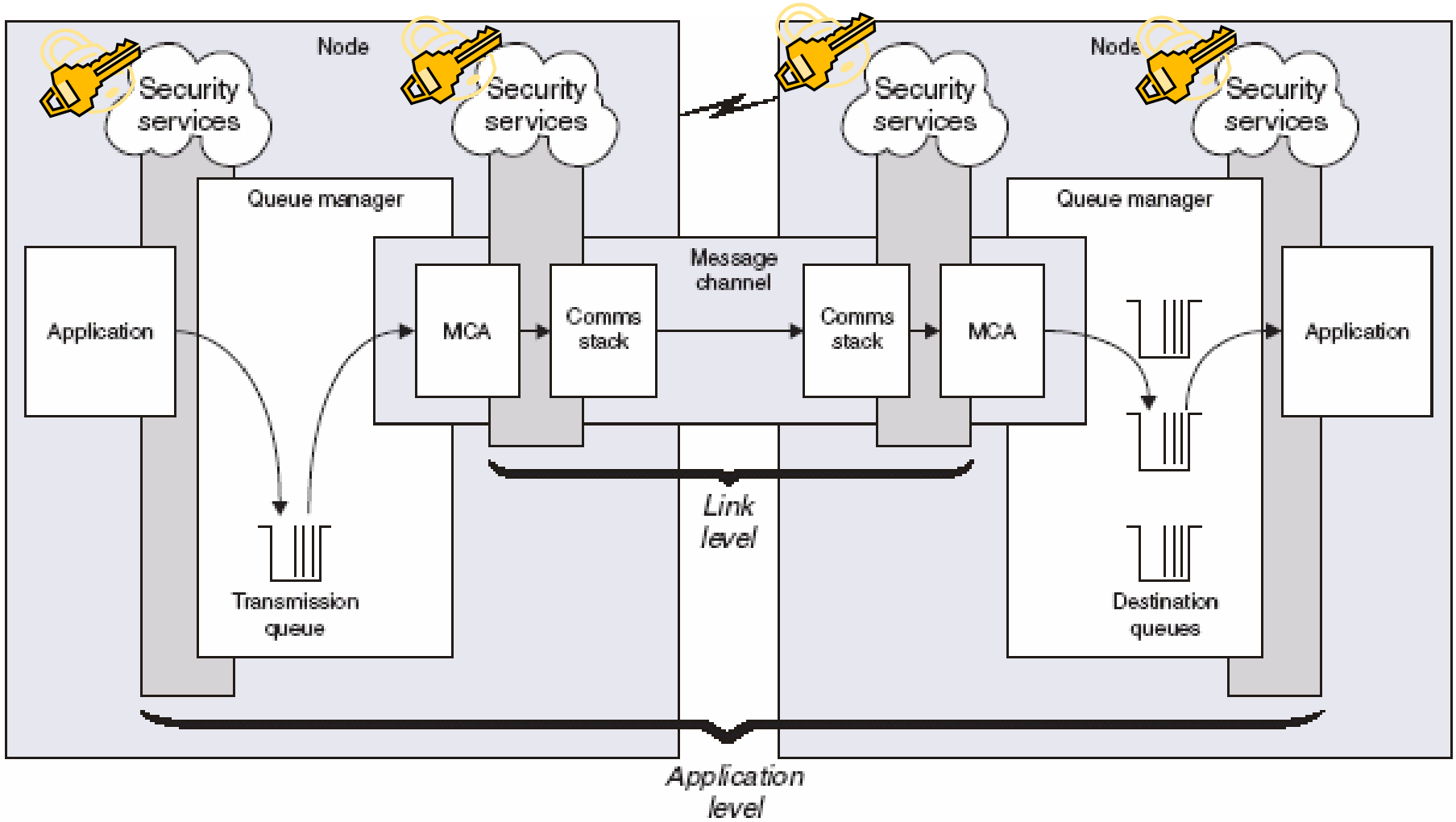
WebSphere MQ -- Security

- Key Components
  - Queue Manager
  - Queues
  - Channel
  - Messages

- Key Capabilities
  - Queue Authorization – Who can administer MQ Series
    - A special group, mqm, is created at product installation time
  - Provides Channel and API exits that is used to manage security
    - Message, Send, Receive and Security channel exits
    - API exits for data encryption
  - Supports SSL for Channel connectivity
    - Provides encryption and authentication for Queue managers and Clients
    - Supports both Message and MQI Channels

Security Features

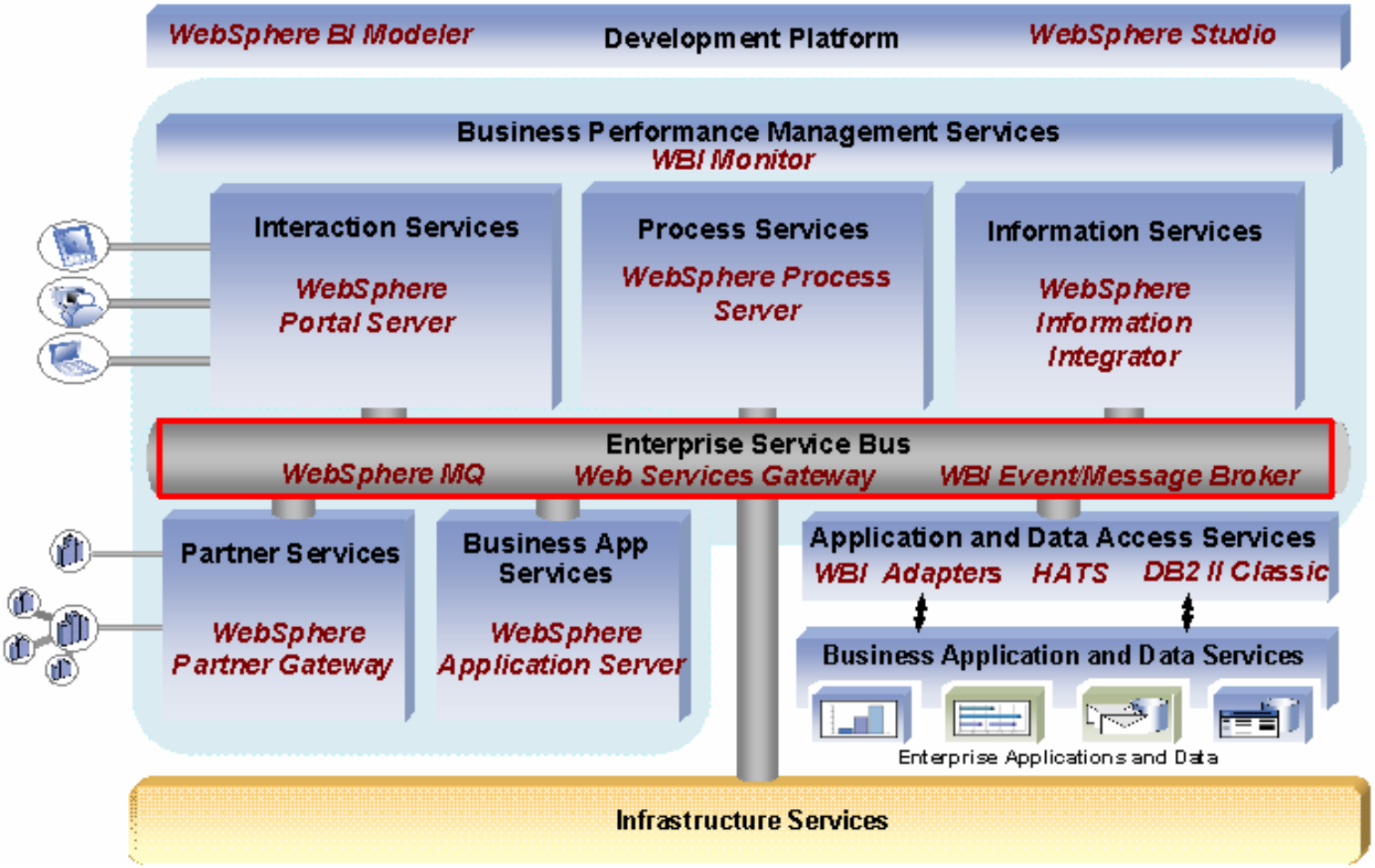
WebSphere MQ – Security Layers



Security Features

Securing BI Reference Architecture

IBM Software Offerings



Security Features

WebSphere Partner Gateway -- Security

Key Components

- User Id/Password
- Integrated certificate management via private secured keystore
- Support for authentication, authorization, encryption services, and audit/non-repudiation

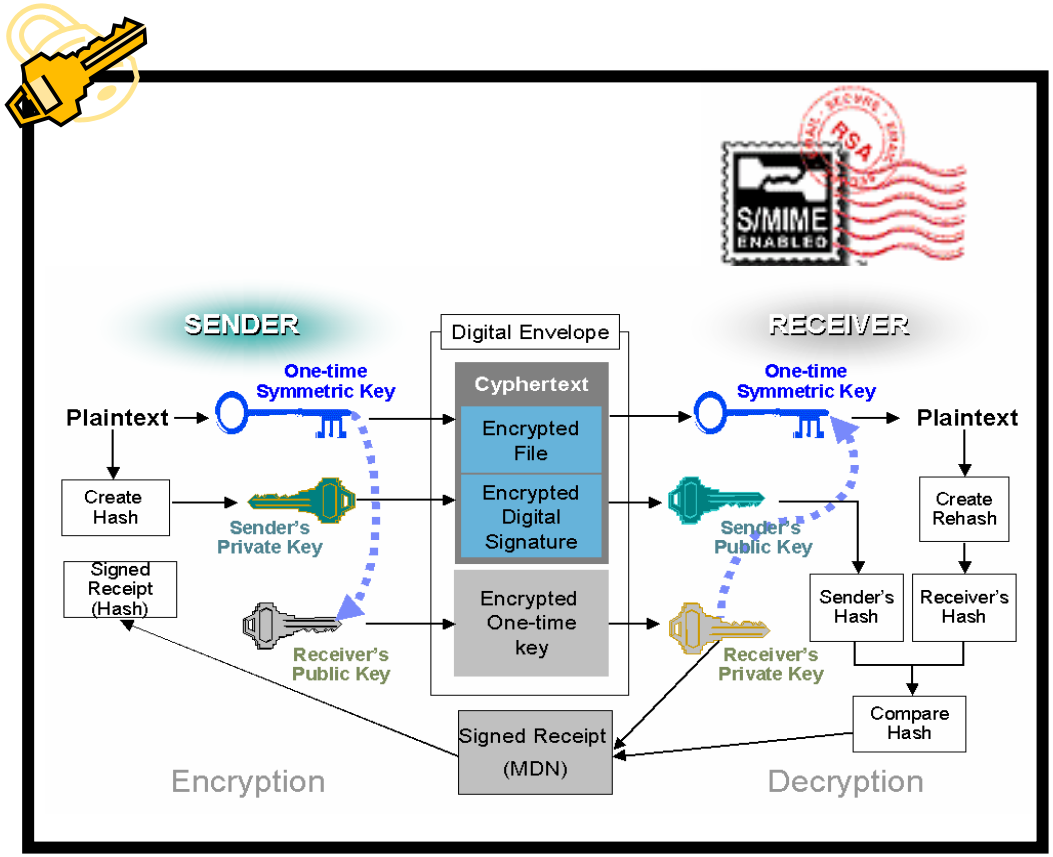
Key Capabilities

- Administration Security
  - Access control using permission model for administrators, operators users and groups enforcing access rights
  - Transport-layer security (SSL) for server and client-based authentication
  - Provides concurrent support of digital certificates from multiple certificate authorities
- Document Security (EDI-INT AS1, AS2, RosettaNet 1.1, 2.0)
  - S/MIME encryption
  - SSL – session based encryption
  - Supports encryption / decryption and digital signatures
  - Ability to secure and validate the authenticity of documents
  - Non-repudiation

Security Features

WPG Provides Secure Packaging

- **Base S/MIME packaging**
- **Provides standards based security**
  - Privacy/Confidentiality
  - Authentication
  - Integrity
- **EDI-INT adds:**
  - Non-Repudiation (Digital Receipt)
    - aka - Message Disposition Notification (MDN)
  - Tested for Interoperability
- **Uses Digital Certificates**

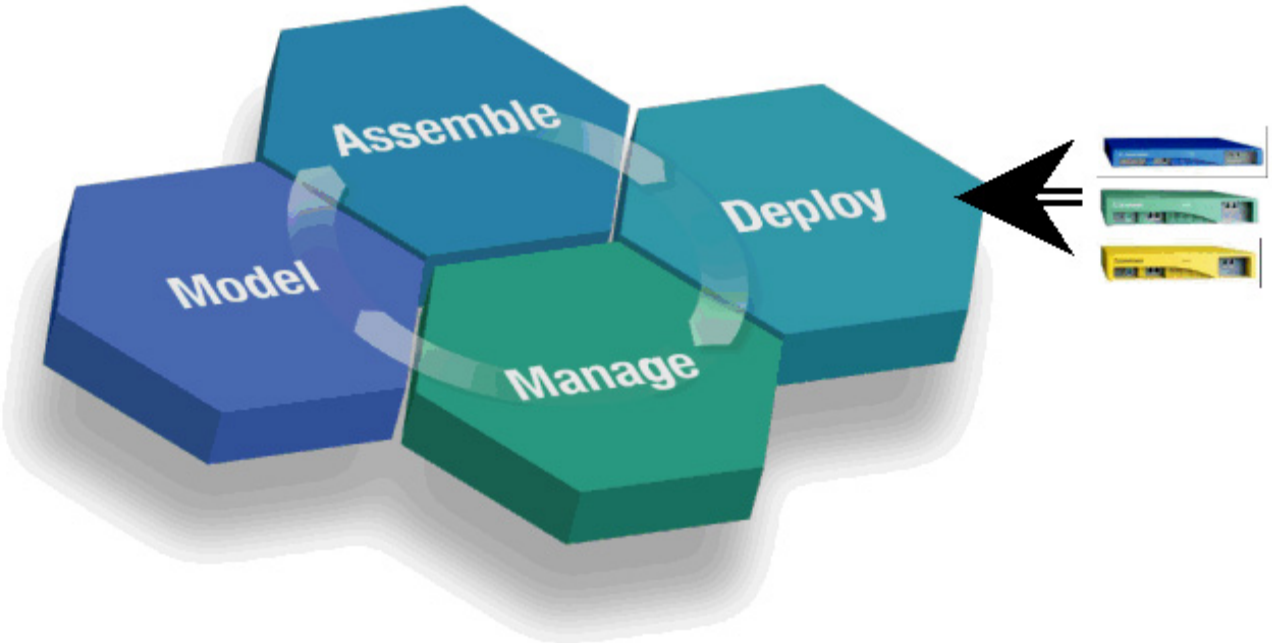


DataPower – Intelligent XML Aware Network Infrastructure

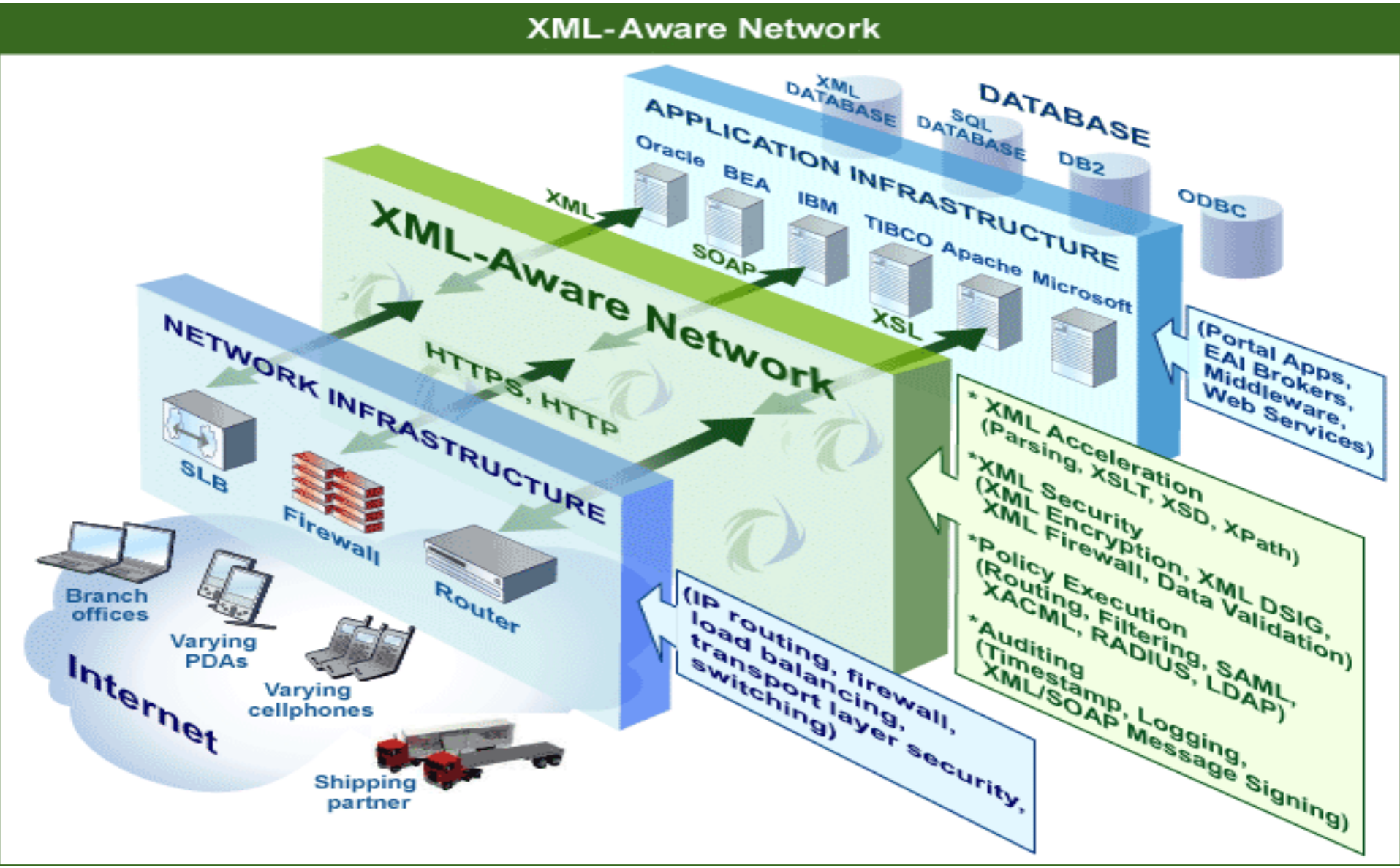
XA35 XML Accelerator

XS40 XML Security Gateway

XI50 XML Integration Appliance



DataPower – Intelligent XML Aware Network Infrastructure



Summary

Security Services in WebSphere BI Products

SECURITY SERVICE	WS ICS	WBI MB	WS MQWF	WS MQ	WPG	WBI Monitor	WPS	WAS
Authentication								
User ID / Password	●	●	●	●	●	●	●	●
Digital Certificate	★	●	◐	●	●		●	●
Authorization								
Access Control Lists	★	●	●	●	●	●	●	●
Roles / Groups	★	●	●	●	●	●	●	●
Audit								
Logs and Reports					●	●		
Confidentiality								
Session Based (SSL)	★	●	●	●	●		●	●
Message Based (Encryption)	★	◐		◐	●		◐	◐
Data Integrity								
Digital Signature	★	◐		◐	●		◐	◐
Non-repudiation								
Signed Receipt					●		◐	◐

Summary

Security has become the most widely discussed topic because we are entering a world of establishing highly interconnected networks that carry out critical transactions.

Connecting our local network to the Internet is a security-critical decision. The environment that machines must survive in has changed radically in recent years, and middleware security must anticipate those risks better than ever.

We can avoid the penetrate-and-patch approach to security only if we consider security to be a crucial and integral system property, not a simple feature or an afterthought.

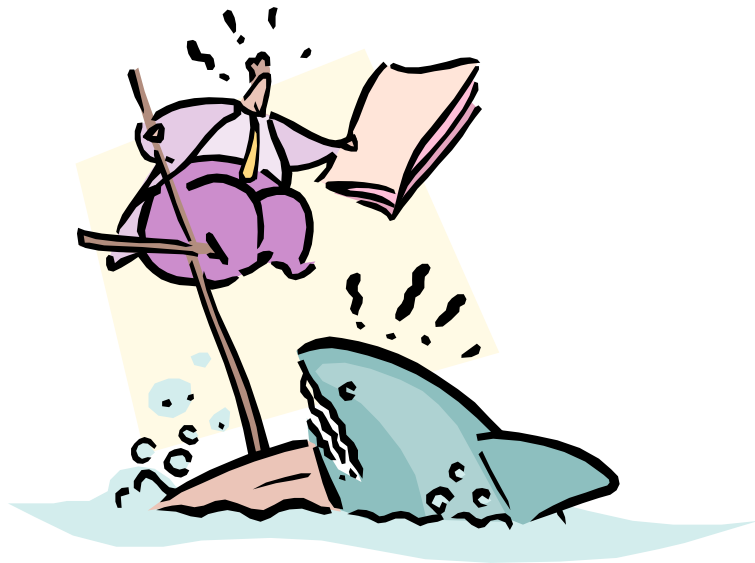
Optional Charts describing Security Skills, Career Roadmap, and Industry Credentials

Secure Thinking

- Thinking in “photo negative”
  - “Normal” architect: How will it work?
  - Security architect: How will it *fail*?
    - Murphy vs. Satan
- No such thing as absolute security
  - Typical: Is it secure?
  - Better: Is it secure *enough*?
    - Risk Mgmt vs. Risk Avoidance

Security Principles

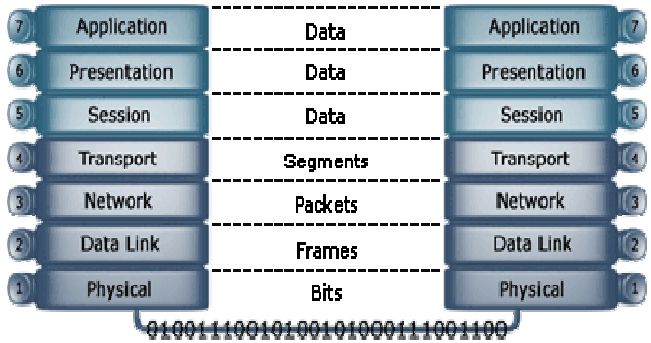
- Principle of Least Privilege
  - a.k.a. “less is more”
    - Avoiding “privilege creep”
    - Hardening
- Defense-in-depth
- Complexity is the enemy of security



Secured, but …

- Security affects system performance
- Security affects usability
- Security requires administration efforts
- Security protects the system against external users as well as internal users
- Security requires policies

Technical Development – Base Skills



- OSI Fundamentals
  Know and understand the impact of the 7 layers of the OSI model
  Respect the little known layers 8 and 9
- Operating Systems
  Extensive Linux, UNIX, and/or Microsoft experience
- Scripting/Programming
  Ability to work with PERL, VB, PGP, HTML, XML
- Networking
  A minimum understanding of basic network operations
  An extensive understanding of the TCP/IP protocol and TCP/UDP services

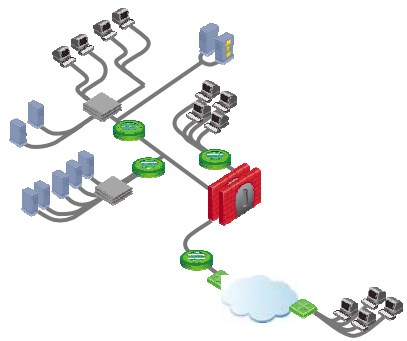
Technical Development - Functional

- Develop a primary technology focus but gain a detailed understanding and experience in a variety of technologies.

  Network, Desktop, Server, Identity Management, Messaging, Web Hosting, etc
- Gain Product Certifications where possible or work experience equivalent

  Checkpoint, Cisco, McAfee, WebSphere, Tivoli, IronMail, Exchange, etc
- Research common deployment and configuration models and learn based on experience and from others on the dos and don’ts.
- In a controlled environment learn how to break, exploit and twist a product.
- Get involved in new development and deployment opportunities where possible.
- DON’T FORGET TO USE THE INTERNET.

  Newsgroups, Forums, Vendor Sites, WhiteHat/BlackHat sites, etc



Certifications – Industry Standard Products

- Cisco
  - Cisco Certified Internetwork Expert (CCIE)
  - Cisco Certified Security Professional (CCSP)
  - Cisco Certified Network Professional (CCNP)
- Checkpoint
  - Check Point Certified Security Expert (CCSE)
  - Check Point Certified Security Expert Plus (CCSE+)
  - Check Point Certified Managed Security Expert (CCMSE)
- McAfee
  - IntruShield Certified Security Specialist (IN-CSS)
  - McAfee Intranet Defense: VirusScan Enterprise and ePolicy Orchestrator
- Symantec
  - Symantec Certified Security Engineer (SCSE)
- Microsoft
  - Microsoft Certified Systems Engineer (MCSE)
  - Microsoft Certified Solutions Developer (MCSD)
- RedHAT
  - RedHat Certified Engineer (RHCE)
  - RedHat Certified Architect (RHCA)
- Tivoli Suite
- WebSphere
- Enterasys
  - Enterasys Certified Internetworking Engineer (ECIE)
  - Enterasys Security Systems Engineer (ESSE)

Certifications - Compliance

isestorm

- BS7799 Lead Auditor

  Provide practical help and information to those who are working towards compliance and certification according to the BS 7799 process.
- Certified Information Systems Auditor (CISA)

  Globally accepted standard of achievement in the IS audit, control and security field
- Certified Information Security Manager (CISM)

  Ability to provide effective security management and consulting. It is business-oriented and focuses on information risk management while addressing management, design and technical security issues at a conceptual level

Certification – Intelligence/Technical

- Certified Information System Security Professional (CISSP)

  An aid to evaluating personnel performing information security functions

  Focus on areas like; Access Control Systems, Cryptography, and Security Management Practices
- GIAC Certified Intrusion Analyst (GCIA)

  Global Information Assurance Certification (GIAC)

  Provides assurance that a certified individual holds the appropriate level of knowledge and skill necessary for a practitioner in key areas of information security
- Systems Security Certified Practitioner (SSCP)

  Focuses on practices, roles and responsibilities as defined by experts from major IS industries. (Access Controls, Administration, Audit and Monitoring, Risk, Response and Recovery, Cryptography, Data Communications, Malicious Code/Malware)
- OSSTMM Professional Security Tester (OPST)

  The applied skills requirement for the appropriate and proper use of security and network knowledge and tools to complete valid, measurable security tests and audits efficiently
- OSSTMM Professional Security Analyst (OPSA)

  A functional, security certification for auditors, managers, and analysts. While it imparts the wisdom of the OSSTMM, it ensures sensible knowledge on how to plan, execute, security in a practical and efficient way

  Open Source Security Testing Methodology Manual (OSSTMM)

  A peer-reviewed methodology for performing security tests and metrics. (information and data controls, security awareness levels, fraud and social engineering control levels, computer and telecommunications networks, wireless devices, mobile devices, physical security access controls, security processes, and physical locations such as buildings, perimeters, and military bases)

Industry Security Standards

Sarbanes-Oxley
Public Company Accounting Reform and Investor Protection Act

NIST

Common Criteria

- Common Criteria (ISO15408)

  It states requirements for security functions and for assurance measures.

  Evaluation Assurance Level ‘x’ (EALx) is a commonly known designation under CC.
- BS7799 / ISO17799

  BS7799 defines the specification for an Information Security Management System (ISMS). The scope of any ISMS includes people, processes, IT systems and policies

  ISO 17799 is an international standard that sets out the requirements of good practice for Information Security Management
- Health Insurance Portability an Accountability Act of 1996 (HIPAA)

  Protection of confidentiality and security of health data through setting and enforcing standards.
- Federal Information Processing Standards (FIPS)

  FIPS Publications are issued by NIST as technical guidelines for US government procurement of computer systems and services.
- Technical Security Standard for Information Technology (TSSIT)

  The purpose of TSSIT is to set out the detailed administrative, technical and procedural safeguards required in an IT environment in order to implement the requirements of the Canadian "Security" volume, Treasury Board Manual.
- Control Objectives for Information and related Technology (COBIT)

  COBIT lists a series of auditable control objectives that, if implemented thoroughly, will help ensure that an organization's information systems are managed efficiently and effectively in achieving the organization's objectives. Included within the control objectives are a series of security controls that will help ensure the confidentiality, integrity, and availability of the information system

References and Links

- Training and Certifications

  CISSP CBK Review Seminar: IS401CE

  GIAC Certified Intrusion Analyst (GCIA)

  Systems Security Certified Practitioner (SSCP)

  OSSTMM Professional Security Tester (OPST): icestore Course List

  OSSTMM Professional Security Analyst (OPSA): icestore Course List

  BS7799 Lead Auditor: icestore Course List

  Certified Information Systems Auditor (CISA)

  Certified Information Security Manager (CISM)

  OSI Fundamentals: OSI001E

  Cisco Certification: IBM Course List

  Checkpoint Certification: IBM Course List

- Standards and Regulations

  Common Criteria (ISO15408)

  BS7799 / ISO17799: Available upon request.

  Health Insurance Portability an Accountability Act of 1996 (HIPAA)

  National Institute of Standards & Technology (NIST)

  Federal Information Processing Standards (FIPS)

  Technical Security Standard for Information Technology (TSSIT): Available upon request.

  Control Objectives for Information and related Technology (COBIT)

  The Personal Information Protection and Electronic Documents Act (PIPEDA)

  Sarbanes-Oxley

Acronyms

- **LDAP** – Lightweight Directory Access Protocol uses to as a directory to provide access to resources and know for its inherent security capabilities that allow
- **EDI-INT** – Electronic Data Interchange Internet Integration known as EDI over the Internet provides a standard way to communicate secured transactions to extended trading partners for reliable exchange of documents.
  - **AS1** - Applicability Statement describing how current Internet standards can be used to achieve this functionality for MIME and SMTP. Security supported is object signature and object based encryption only.
  - **AS2** - Applicability Statement describing how current Internet standards can be used to achieve this functionality for Process-to-Process (real-time) EDI based on MIME and HTTP. Security supported is object signature, and both session and object encryption.
  - **AS3** - Applicability Statement describing how current Internet standards can be used to achieve the transfer of EDI or XML data over internet in a secure manner based on FTP. Security supported is object signature, and both session and object encryption.
- **S/MIME –** Secure/Multipurpose Internet Mail Extension (RFC 1521) is a lightweight protocol
- **SOAP** – Simple Object Access Protocol is a lightweight protocol for exchange of information in a decentralized, distributed environment. It is an XML based protocol that consists of three parts: an envelope that defines a framework for describing what is in a message and how to process it, a set of encoding rules for expressing instances of application-defined data types, and a convention for representing remote procedure calls and responses.
- **WS-Security** – WebServices Security describes enhancements to SOAP messaging to provide quality of protection through message integrity, message confidentiality, and single message authentication. These mechanisms can be used to accommodate a wide variety of security models and encryption technologies.