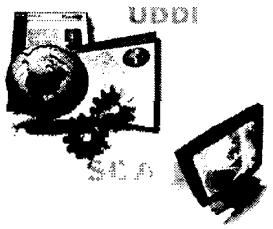
Adaptive Schemes of Web Services Security Technologies for E-Business

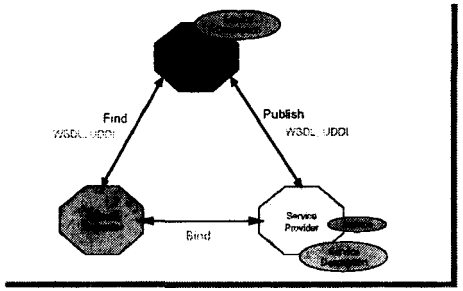


DongJoon Kim
(djkim@ec.cse.cau.ac.kr
)

Table of contents

Introduction

- **Web Services**
  - A Web service is a software system designed to support interoperable machine-to-machine interaction over a network. (W3C)



Introduction

- **Needs for web services security**
  - Based on message exchange on the internet
  - The increase of importance for security as characteristics of web services(integration, communication, etc.)
  - Interruption to web services spread
- **Web services security**
  - Transport-level security
    - ☞ http, https, ftp ...
  - Message-level security
    - ☞ soap, xml ...

Security requirements for web services

- **Confidentiality**
  - guarantees that data is protected against unauthorized attempts to read it
  - Two broad approaches
    - to use a private connection between the two parties(either a dedicated line or a virtual private network(VPN))
    - to use encryption when data is being sent over an untrusted network such as the internet
- **Authentication**
  - guarantees that access to web services and data is restricted to only those who can provide the appropriate proof of identity
  - prove the identity through a credential such as a password or a certificate

Security requirements for web services

- **Integrity**
  - means that the message is not modified in transit
  - does not mean that information cannot be tampered with
  - if information is tampered with, this tampering can be detected
- **Authorization**
  - is the process to verify what resources an authenticated entity has access to
  - Authentication – "who you are"
    Authorization – "what you are allowed to do"
  - If web services have different security infrastructures, they will transfer both identity and authorization information each other.

Security requirements for web services

- **Non-repudiation**
  - is an attribute of communications that seeks to prevent future false denial of involvement by either party
  - Non-repudiation with proof of origin provides the recipient of data with evidence that proves the origin of data
  - Non-repudiation with proof of receipt provides the originator of data with evidence that proves the data was received as addressed
  - Detailed logging of any changes to customer information requested will be the most effective method in case any questions should arise.
- **Key management**
  - allows a simple client to obtain key information
  - involves the generation, certification, distribution and revocation of keys

Standards for web services security

- **HTTP Basic Authentication**
  - Authorization – Basic *credential*
  - Challenge-Response Authentication
  - Digest Authentication
- **HTTPS**
  - HTTP over SSL
  - SSL(Secure Sockets Layer) : a mechanism by which two endpoints exchange data in an encrypted format
  - HTTPS does not provide end-to-end security.
- **HTTP Basic Authentication + HTTPS**

Standards for web services security

- **XML Signature**
  - o is a digital signature expressed in XML
  - o developed by the W3C and IETF
  - o provides integrity, non-repudiation and authentication
  - o type
    - ☞ Enveloped XML Signature : the signature is contained within the signed document itself
    - ☞ Enveloping XML Signature : the signed data is contained within the XML signature structure itself
    - ☞ Detached XML Signature : the signature is separate from the signed entities or entities
  - o allows multiple documents to be signed
  - o W3C Recommendation

Standards for web services security

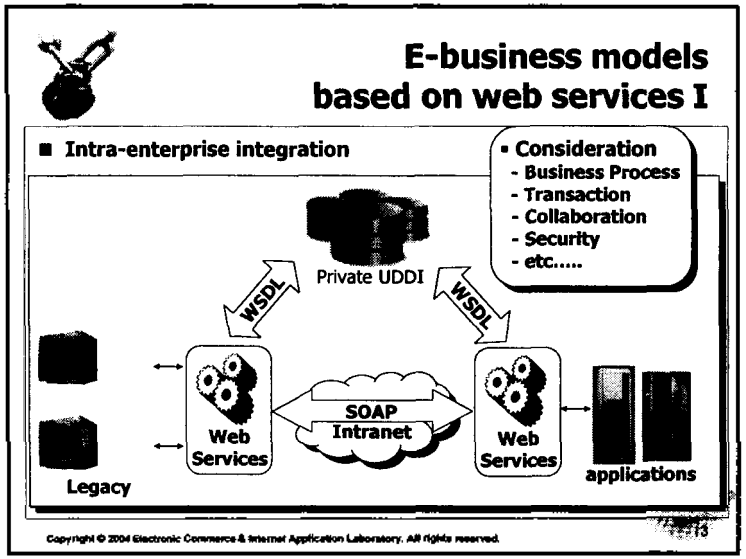
- **XML Encryption**
  - o is a process for encrypting data and representing the result using the syntax of XML
    - ☞ Encrypted data can be expressed using XML.
    - ☞ Portions of an XML document can be selectively encrypted.
  - o The advantages compared with SSL
    - ☞ can support end-to-end security
    - ☞ can support partial encryption, but SSL can't
  - o W3C Recommendation
- **XKMS(XML Key Management Specification)**
  - o is a Web Services that provides an interface to a PKI
  - o X-KISS & X-KRSS
  - o W3C Working Draft

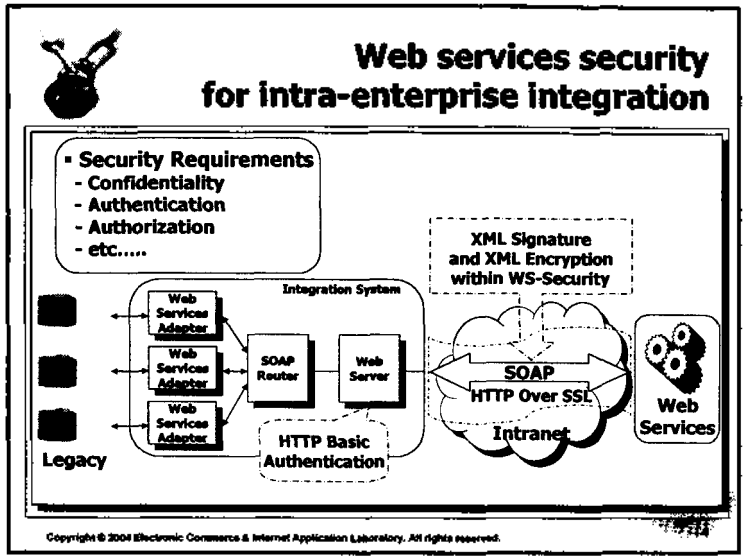
Standards for web services security

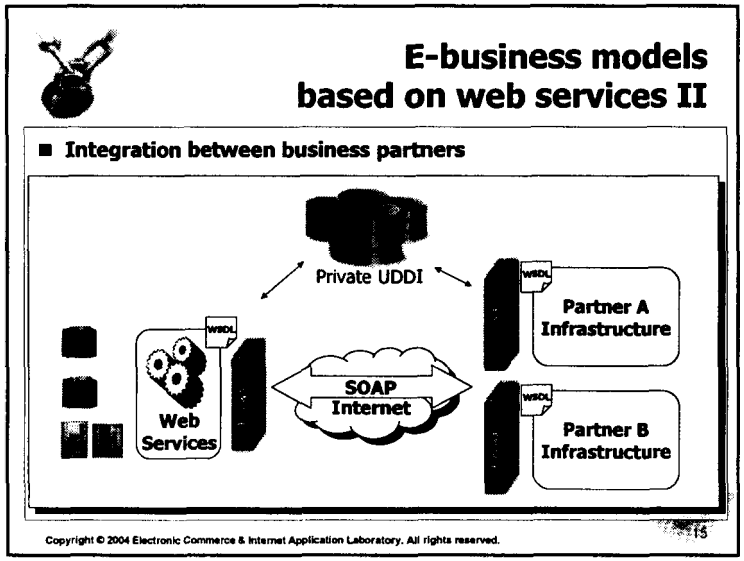
- **SAML (Security Assertion Markup Language)**
  - o is an XML-based security standard for exchanging information
  - o is useful for transporting authentication and authorization credentials across different security domains
  - o uses token-authentication methods
  - o the possibility of Single Sing-On
  - o SAML 1.1 : OASIS Standard
- **XACML (eXtensible Access Control Markup Language)**
  - o is an XML-based security standard for expressing rules and policies for controlling access to information
  - o is also used for the authorization request/response
  - o XACML 1.0 : OASIS Standard

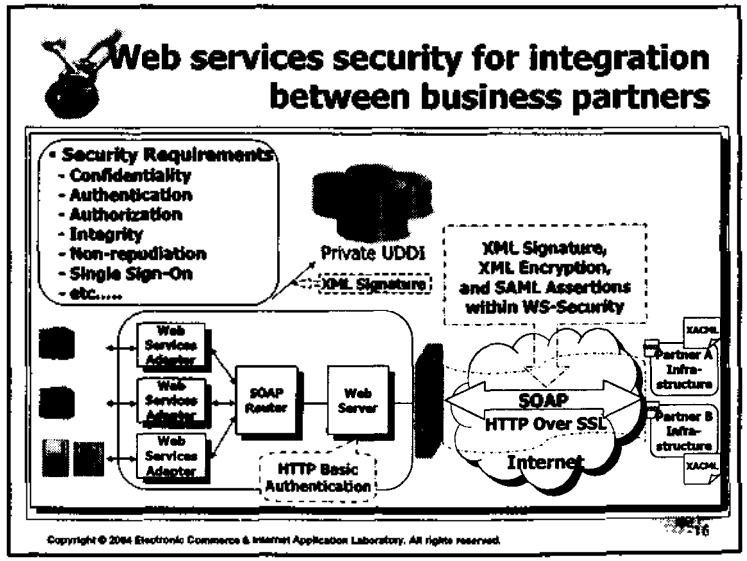
Standards for web services security

- **WS-Security**
  - o how security tokens are contained in SOAP message
  - o how XML Security specifications are used to encrypt and sign security tokens
  - o The main mechanisms
    - ☞ security token propagation
      - ➢ supports mechanism for attaching many different types of security tokens
    - ☞ message integrity
    - ☞ message confidentiality
    - ☞ end-to-end security
  - o developed by the Microsoft, IBM and VeriSign
  - o submitted to the OASIS for standardization in June 2002
    - ☞ Web Services Security: SOAP Message Security
    - ☞ Web Services Security: Username Token Profile
    - ☞ Web Services Security: X.509 Token Profile


E-business models based on web services I
Intra-enterprise integration
Consideration
- Business Process
- Transaction
- Collaboration
- Security
- etc.....
Private UDDI
WSDL
WSDL
Web Services
SOAP
Intranet
Web Services
Legacy
applications
Copyright © 2004 Electronic Commerce & Internet Application Laboratory. All rights reserved.
13

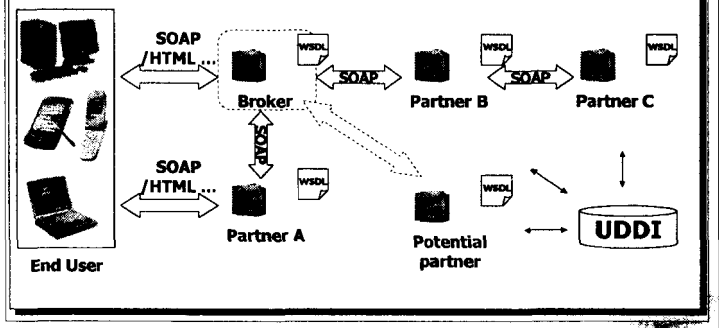

Web services security for intra-enterprise integration
Security Requirements
- Confidentiality
- Authentication
- Authorization
- etc.....
XML Signature and XML Encryption within WS-Security
Integration System
Web Services Adapter
Web Services Adapter
Web Services Adapter
SOAP Router
Web Server
SOAP
HTTP Over SSL
Intranet
Web Services
HTTP Basic Authentication
Legacy
Copyright © 2004 Electronic Commerce & Internet Application Laboratory. All rights reserved.
14


E-business models based on web services II
Integration between business partners
Private UDDI
WSDL
Partner A Infrastructure
WSDL
Web Services
SOAP
Internet
WSDL
Partner B Infrastructure
Copyright © 2004 Electronic Commerce & Internet Application Laboratory. All rights reserved.
15


Web services security for integration between business partners
Security Requirements
- Confidentiality
- Authentication
- Authorization
- Integrity
- Non-repudiation
- Single Sign-On
- etc.....
Private UDDI
XML Signature
XML Signature, XML Encryption, and SAML Assertions within WS-Security
Web Services Adapter
Web Services Adapter
Web Services Adapter
SOAP Router
Web Server
SOAP
HTTP Over SSL
Internet
XACML
Partner A Infra-structure
Partner B Infra-structure
XACML
HTTP Basic Authentication
Copyright © 2004 Electronic Commerce & Internet Application Laboratory. All rights reserved.
16

E-business models based on web services III

- Dynamic business



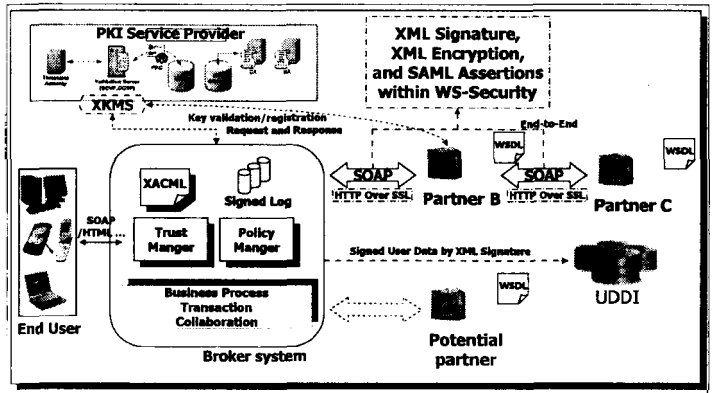
17

Web services security for dynamic business

- **Security Requirements**
  - Confidentiality
  - Authentication
  - Authorization
  - Integrity
  - Non-Repudiation
  - Single Sign-On
  - End-to-End Security
  - Key Management
  - Trust Management
  - Policy Management
  - Etc...
- **Security Technologies**
  - HTTP Basic Authentication
  - HTTP Over SSL
  - XML Signature
  - XML Encryption
  - SAML & XACML
  - XKMS
  - WS-Security
  - WS-Trust
  - WS-Policy
  - Etc...

18

Web services security for dynamic business



19

Security requirements supported by web services security technologies

	XML Signature	XML Encryption	WS-Security	XKMS	SAML	XACML	HTTPS	HTTP Basic Auth.
Confidentiality		✓	✓				✓	
Integrity	✓		✓				✓	
Authentication	✓		✓		✓			✓
Authorization			✓		✓	✓		✓
Non-Repudiation	✓		✓					
Key Management				✓				

20