



IBM WebSphere® Datapower Dispositivos SOA

Luis Héctor Sánchez Palacios
IT Specialist
Software Group
lhsanchz@mx1.ibm.com

Mayo de 2008



Agenda

- Antecedentes
 - Desarrollo
 - Desempeño
 - Operación
- Riesgos uso XML
- Dispositivo XML-aware
- Línea de dispositivos Datapower
- Características físicas
- Generación políticas de seguridad

Agenda

- Casos de uso
 - General
 - Caso de uso 1: Aceleración XML
 - Caso de uso 2: Protección vs amenazas XML , Gateway de Seguridad
 - Caso de uso 3: Habilitar Backend con XML
 - Caso de uso 4: ESB
- Anexos
 - WS-Security
 - Access Control

Desarrollo

- Tiempo dedicado a incluir
 - Cifrado y Descifrado
 - Firmas y Sellos digitales
 - Validación firmas y sellos digitales
 - Validación esquemas XML
 - Autenticación
- \$\$\$\$\$ Desarrollo de tales funciones y riesgos implicados

Riesgos uso XML

- XML Entity Expansion and Recursion Attacks
- XML Document Size Attacks
- XML Document Width Attacks
- XML Document Depth Attacks
- XML Wellformedness-based Parser Attacks
- Jumbo Payloads
- Recursive Elements
- MegaTags – aka Jumbo Tag Names
- Public Key DoS
- XML Flood
- Resource Hijack
- Dictionary Attack
- Message Tampering
- Data Tampering
- Message Snooping
- XPath Injection
- SQL injection
- WSDL Enumeration
- Routing Detour
- Schema Poisoning
- Malicious Morphing
- Malicious Include – also called XML External Entity (XXE) Attack
- Memory Space Breach
- XML Encapsulation
- XML Virus
- Falsified Message
- Replay Attack
- ...others

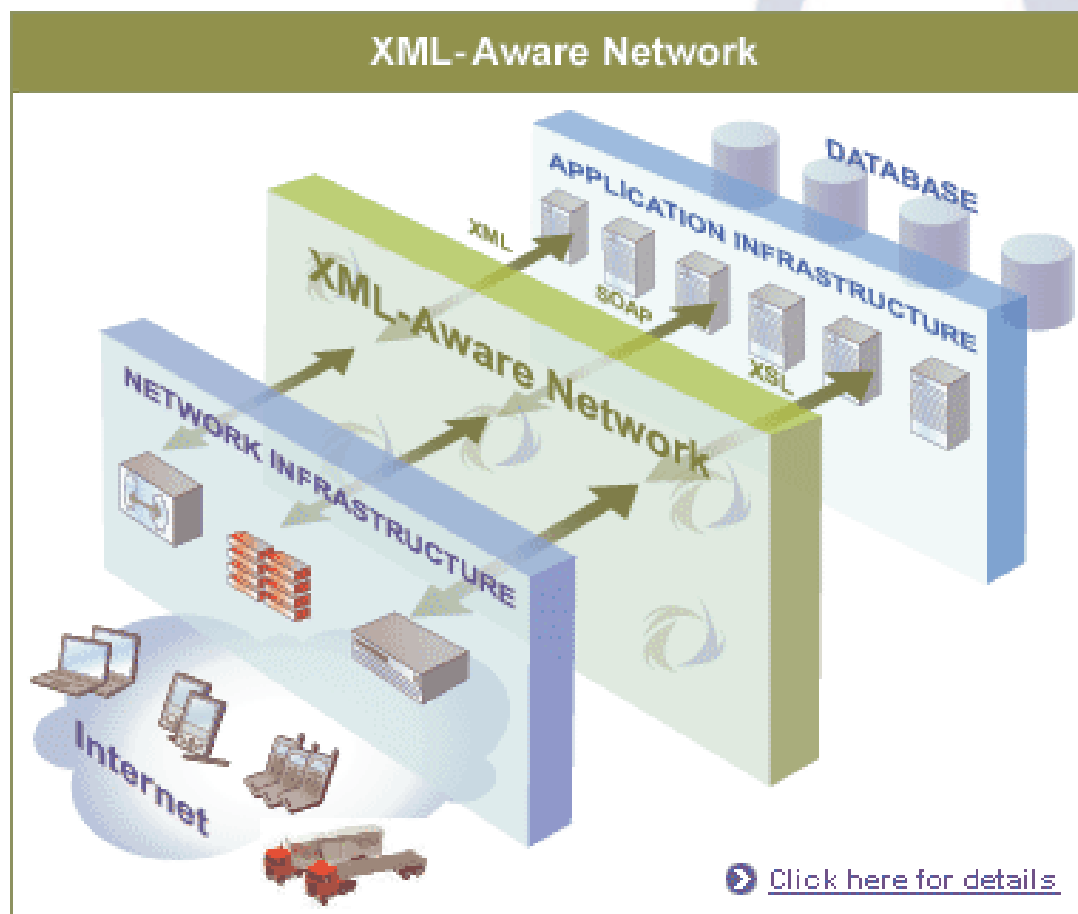
Desempeño

- SOA basado en XML
- XML -> mayor consumo de recursos (CPU y RAM)
 - Validación tramas XML
 - Transformación tramas XML
 - Manejo de los riesgos XML
 - Cifrado y Descifrado

Operación

- Generación y manejo
 - certificados
 - llaves primarias
- Auditorías
- Manejo de políticas seguridad

Dispositivo XML-aware

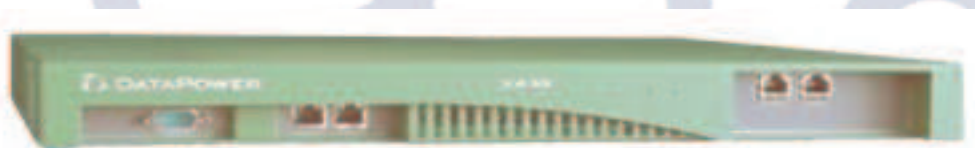


- Protección adicional a seguridad perimetral
- Introspección de transacciones
- Regula la cantidad de solicitudes
- Libera los recursos de los servidores

Linea de dispositivos Datapower

□ XA35

- Velocidad (XML)



□ XS40

- Velocidad (XML)
- Seguridad



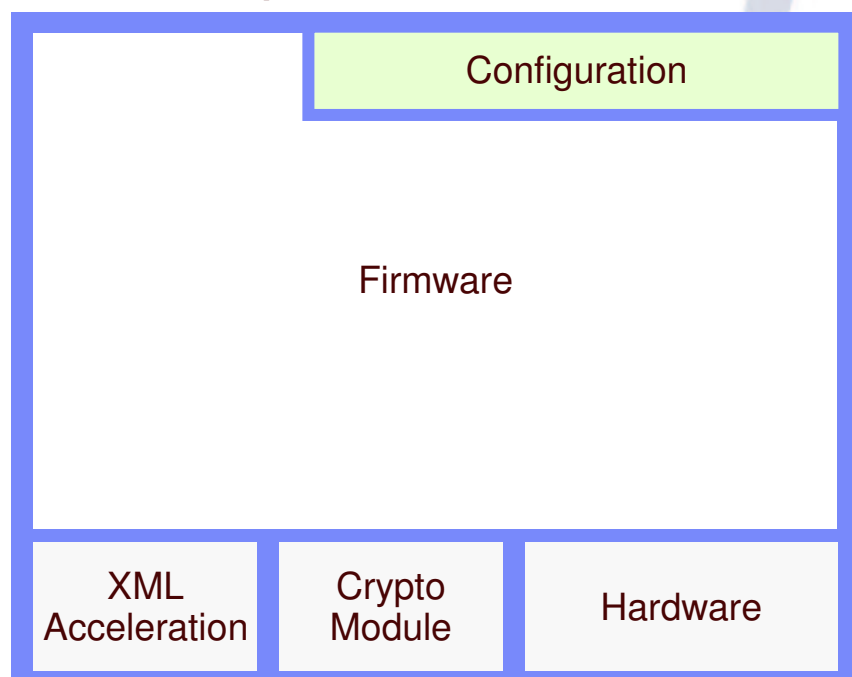
□ XI50

- Velocidad (XML, No XML)
- Seguridad
- Transformación
 - Transportes
 - Datos

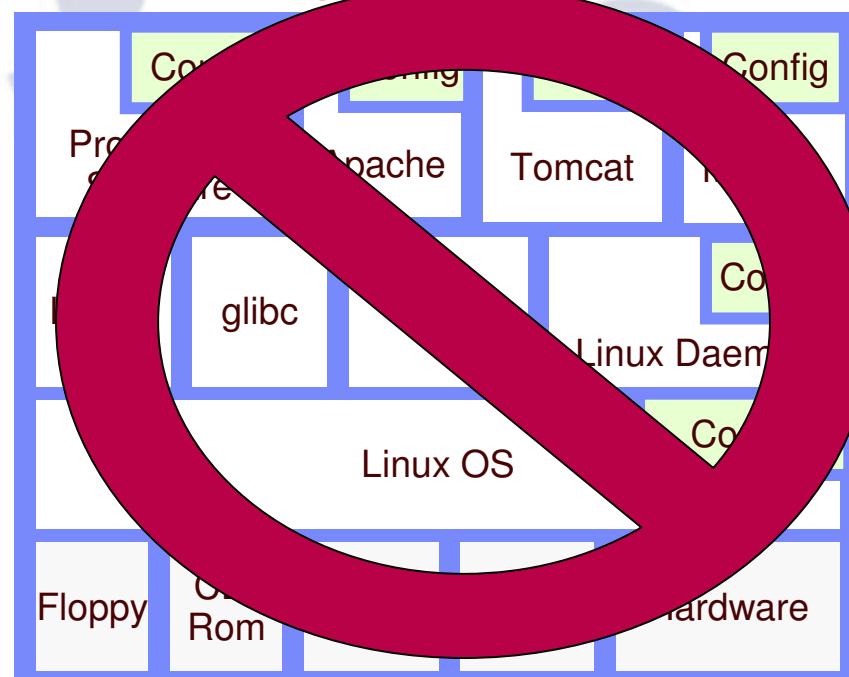


Características físicas

Dispositivo DataPower



Server Appliance



- No interfaces de entrada
- Sensores anti-tampering
- Estado sólido

Políticas de seguridad



- Multiples servicios

Políticas de seguridad

Select a Policy Name:

DigitalSig

Create rule: Click New, drag action icons onto line. Edit rule: Click on rule, double-click on action

Entry

Server to Client Both Directions Client to Server Error

Rule Actions:

Configured Rules

Reorder	Priority	Match Name	Direction	Actions
<input type="button" value="Up"/> <input type="button" value="Down"/>	1	Verify	Two Way	<input type="button" value="Filter"/> <input type="button" value="Sign"/> <input type="button" value="Verify"/>
<input type="button" value="Up"/> <input type="button" value="Down"/>	2	DigitalSigned	Two Way	<input type="button" value="Filter"/> <input type="button" value="Sign"/>
<input type="button" value="Up"/> <input type="button" value="Down"/>	3	<u>SignedElement</u>	Two Way	<input type="button" value="Filter"/> <input type="button" value="Sign"/>

Agenda

- Casos de uso
 - General
 - Caso de uso 1: Aceleración XML
 - Caso de uso 2: Protección contra amenazas XML, Gateway de Seguridad
 - Caso de uso 3: Habilitar Backend con XML
 - Caso de uso 4: ESB

Casos de Uso



Cliente de
Web Services



Data Power
Validación del esquema
Transformación del formato
Cifrado-Desecifrado
Firmado digital
Validación de firma
Autenticación
Autorización
Filtro de contenido
Ruteo basado en contenidos
Etc.

Aplicación
Validación del esquema
Transformación del formato

Aplicación
Reglas del Negocio
Autenticación
Autorización
Filtro de contenido
Ruteo basado en contenidos



Server
Services

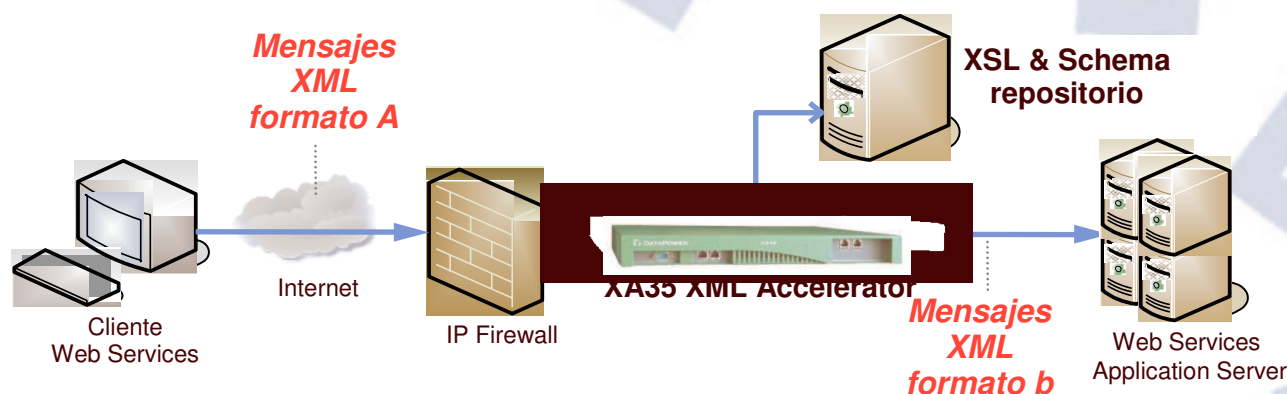


Manejo de
Identidades



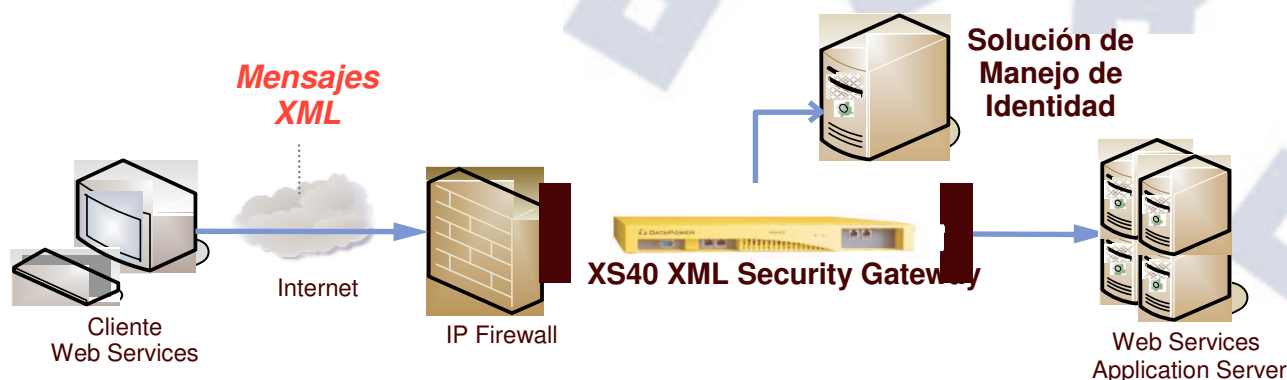
Repositorio
XML Schema

Caso de uso 1: Aceleración XML



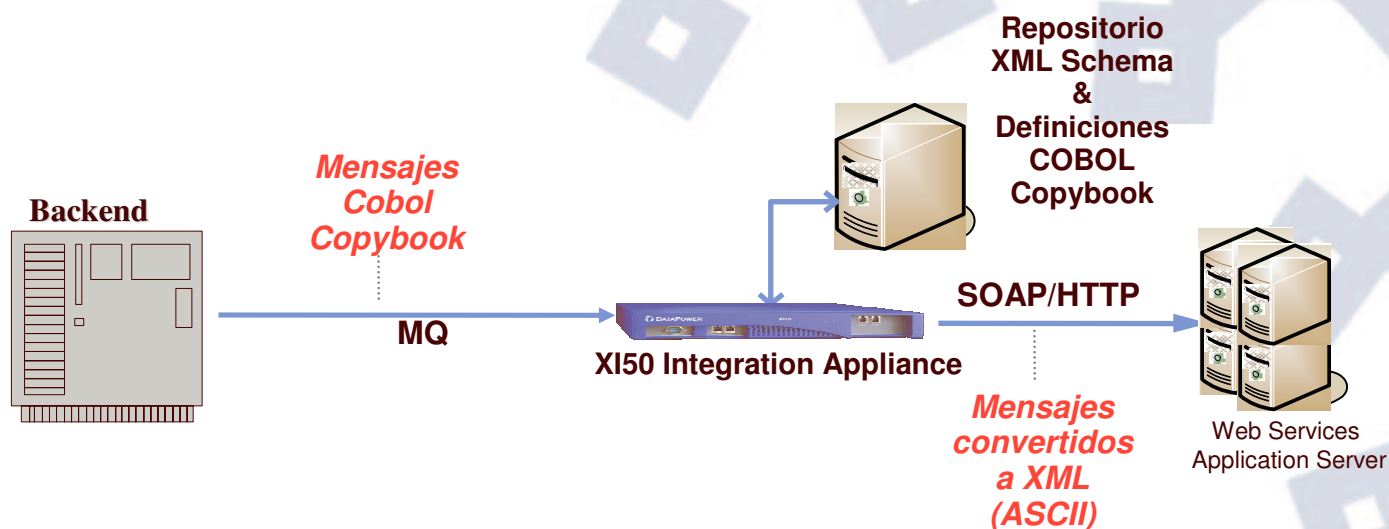
- XA35 coprocesador para validación de XML Schemas y transformación entre XMLs, mediante XSLT

Caso de uso 2: Protección contra amenazas XML



XS40 proporciona la primera línea de defensa de XML y hace cumplir la política de acceso almacenada en una solución de manejo de identidad (como Tivoli Access Manager, Netegrity, Oblix, LDAP, MSAD).

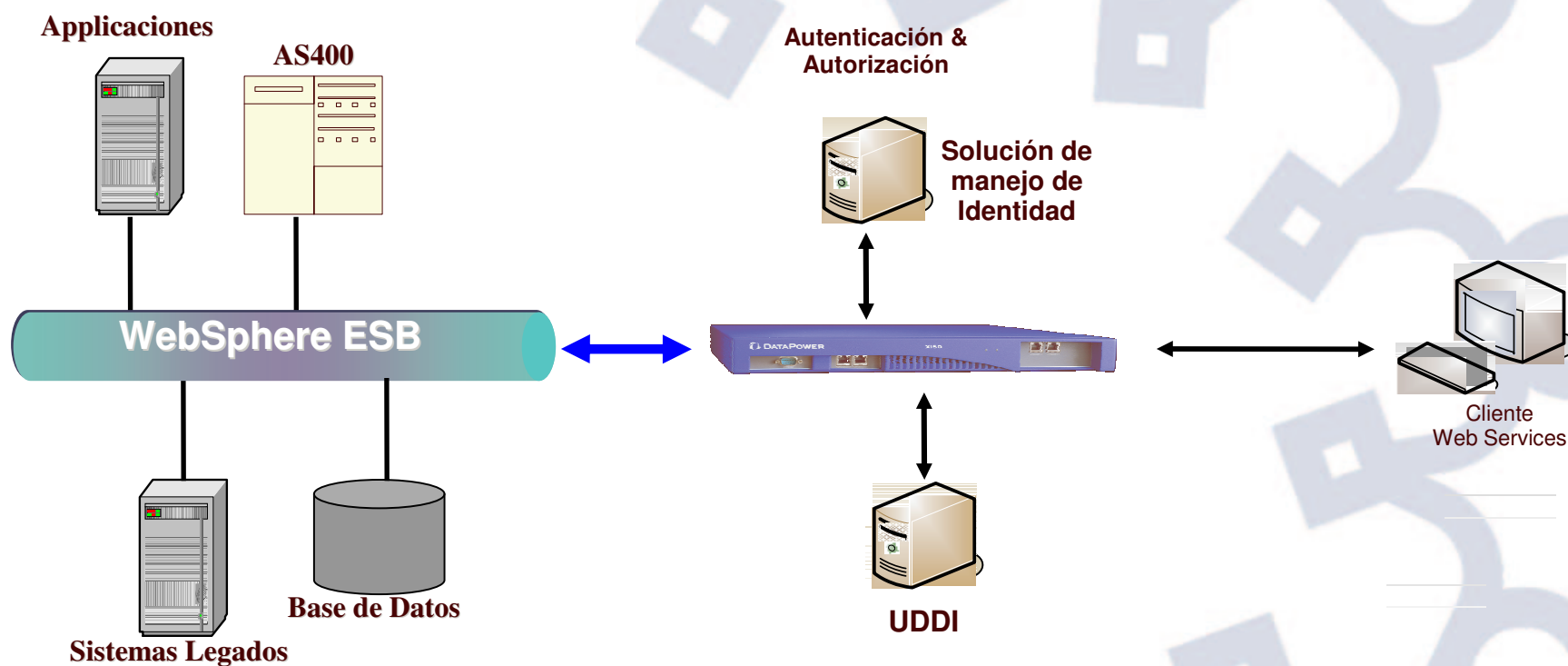
Caso de uso 3



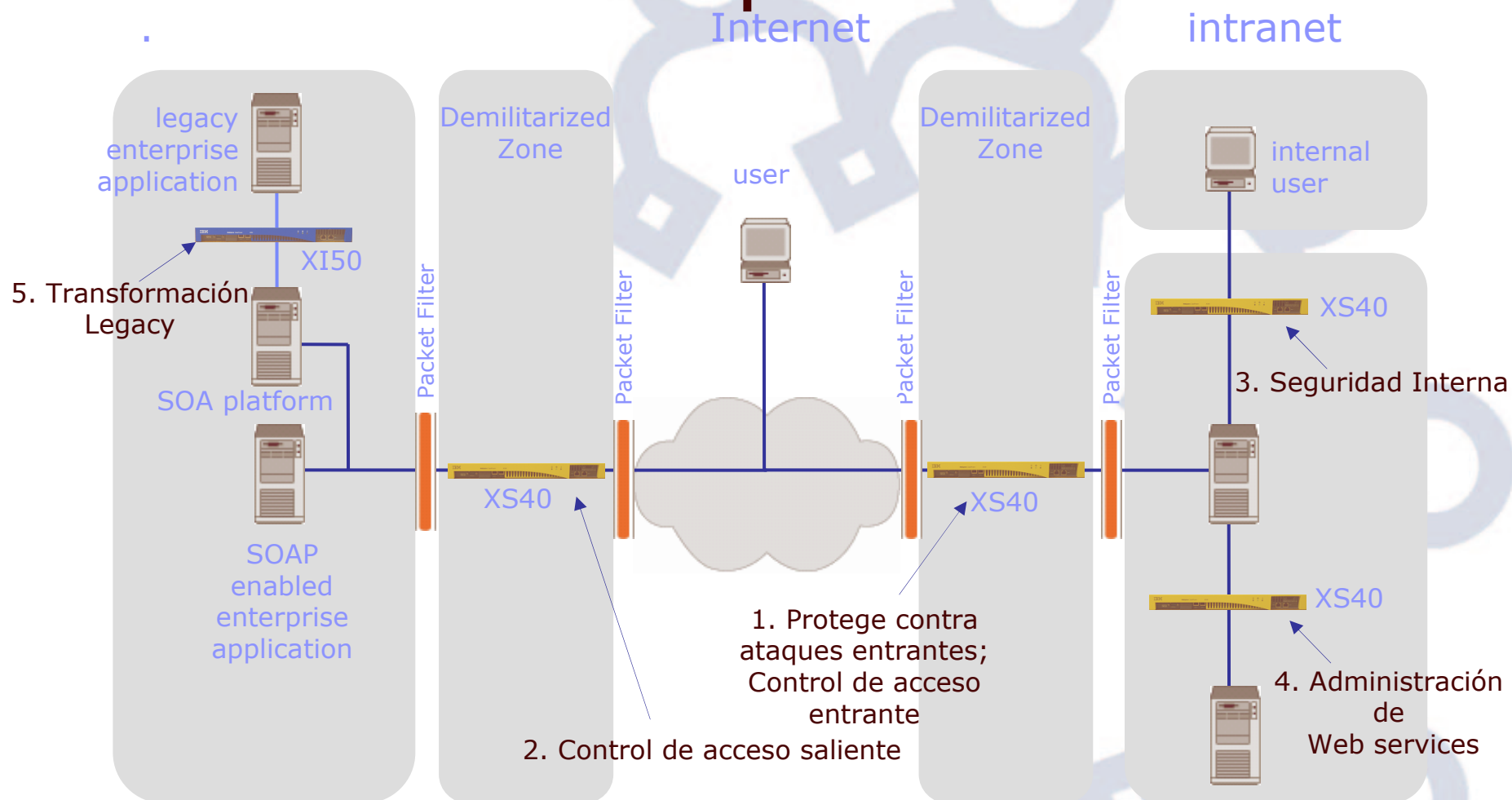
XI50 se conecta con el Mainframe vía MQ u otro mecanismo de conexión, convierte los datos del Backend a datos XML, los valida, y los envía a un destino protocolo web services (SOAP/HTTP).

Caso de uso 4

1



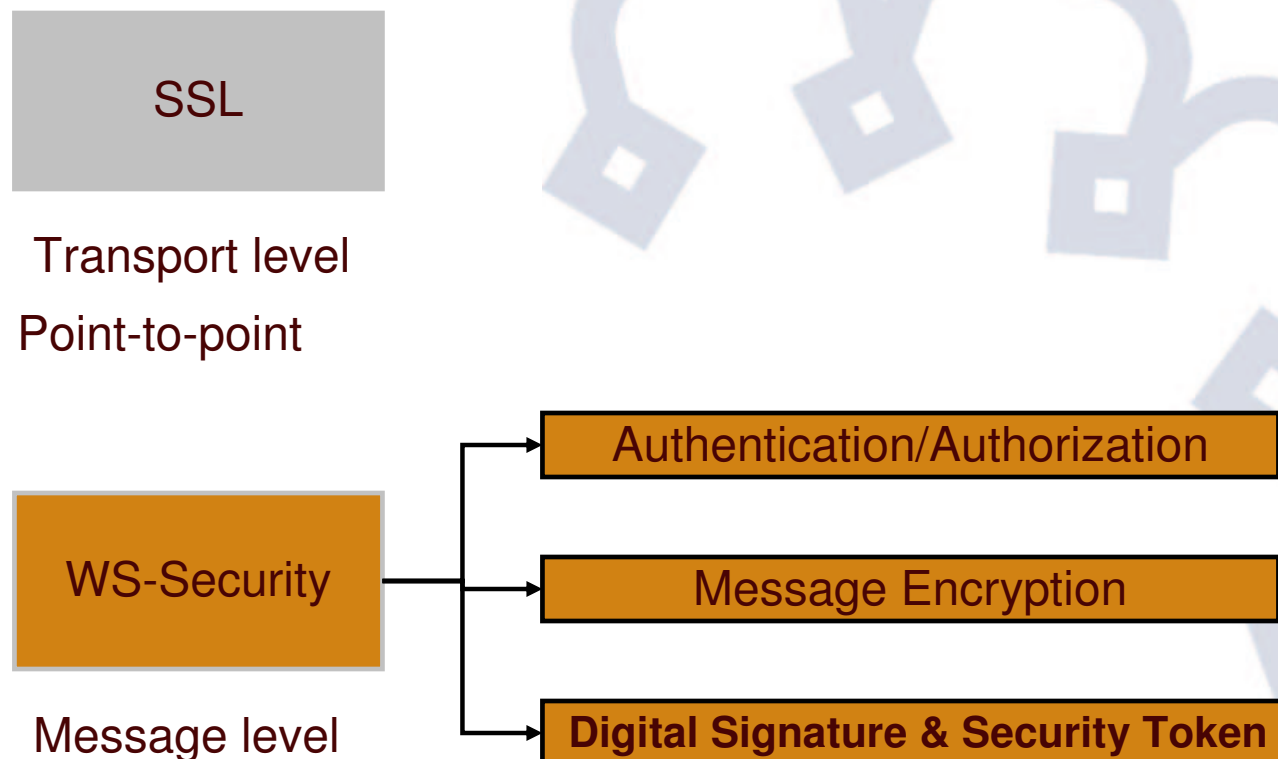
Escenarios de implantaciones



Anexos



Web Services Security



- Involves SOAP message modification
- Transport independent and can be sent via any protocol
- end-to-end security

Generate a Key

NETWORK

ADMINISTRATION

Main

- File Management
- System Control

Configuration

- Application Domain
- Include Configuration
- Export Configuration
- Import Configuration
- Import Package

Access

- New User Account
- Manage User Accounts
- Manage User Groups
- RBM Settings
- RADIUS Settings
- SNMP Settings
- IBM Tivoli Access Manager

Device

- System Settings
- Time Settings
- Failure Notification
- Throttle Settings
- Statistic Settings

Debug

- XML File Capture
- Browse Captured Files
- View List of Event Codes

Miscellaneous

- Configure Log Categories
- Manage Log Targets
- New Email Pager
- Crypto Tools

OBJECTS

Crypto Tools

Generate Key

LDAP (reverse) Order of RDNs on off

Country Name (C)

State or Province (ST)

Locality (L)

Organization (O)

Organizational Unit (OU)

Organizational Unit 2 (OU)

Organizational Unit 3 (OU)

Organizational Unit 4 (OU)

Common Name (CN) *

RSA Key Length

File Name

Validity Period days

Password

Password Alias

Private Key Exportable via hsmkwk on off

Export Private Key on off

Generate Self-Signed Certificate on off

Export Self-Signed Certificate on off

Generate Key and Certificate Objects on off

Object Name *

Generate Key on HSM on off

Using Existing Key Object

Generate Key

Confirm Action - Microsoft Internet Explorer

DATAPOWER

Generate a 1024 bit RSA key pair and a CSR ?

Confirm **Cancel**

Add Key



Keys and Certificates Management

Please click on one of the links below...

Basics used in encryption, decryption, signing, and credentials:

- [Keys](#)
- [Certificates](#)

Signature verification:

- [Validation Credentials](#)

SSL:

- [Crypto Profile](#) - for SSL proxy server and client profiles
- [Validation Credentials](#) - for validating actual client or server
- [Identification Credentials](#) - for identifying self

Cancel

XML Security

- **Sign, verify, encrypt & decrypt**
- **XML Encryption & XML Digital Signature at:**
 - Message-level
 - Part-of-message or field-level
 - Headers, as building block of other security specs
- **Field-level security configurable from the WebGUI**
- **Verify-all option (data-driven verification of all signatures)**
- **DataPower's own implementation, listed in W3C Interop matrix:**
 - <http://www.w3.org/Signature/2001/04/05-xmldsig-interop.html>
 - <http://www.w3.org/Encryption/2002/02-xenc-interop.html>
 - Agility for interoperability or customization
- **Secure Attachment Processing:**
 - Supports the full SOAP with Attachments specification (MIME/DIME)
 - WS-Security
- **Last-mile Security for SOA**

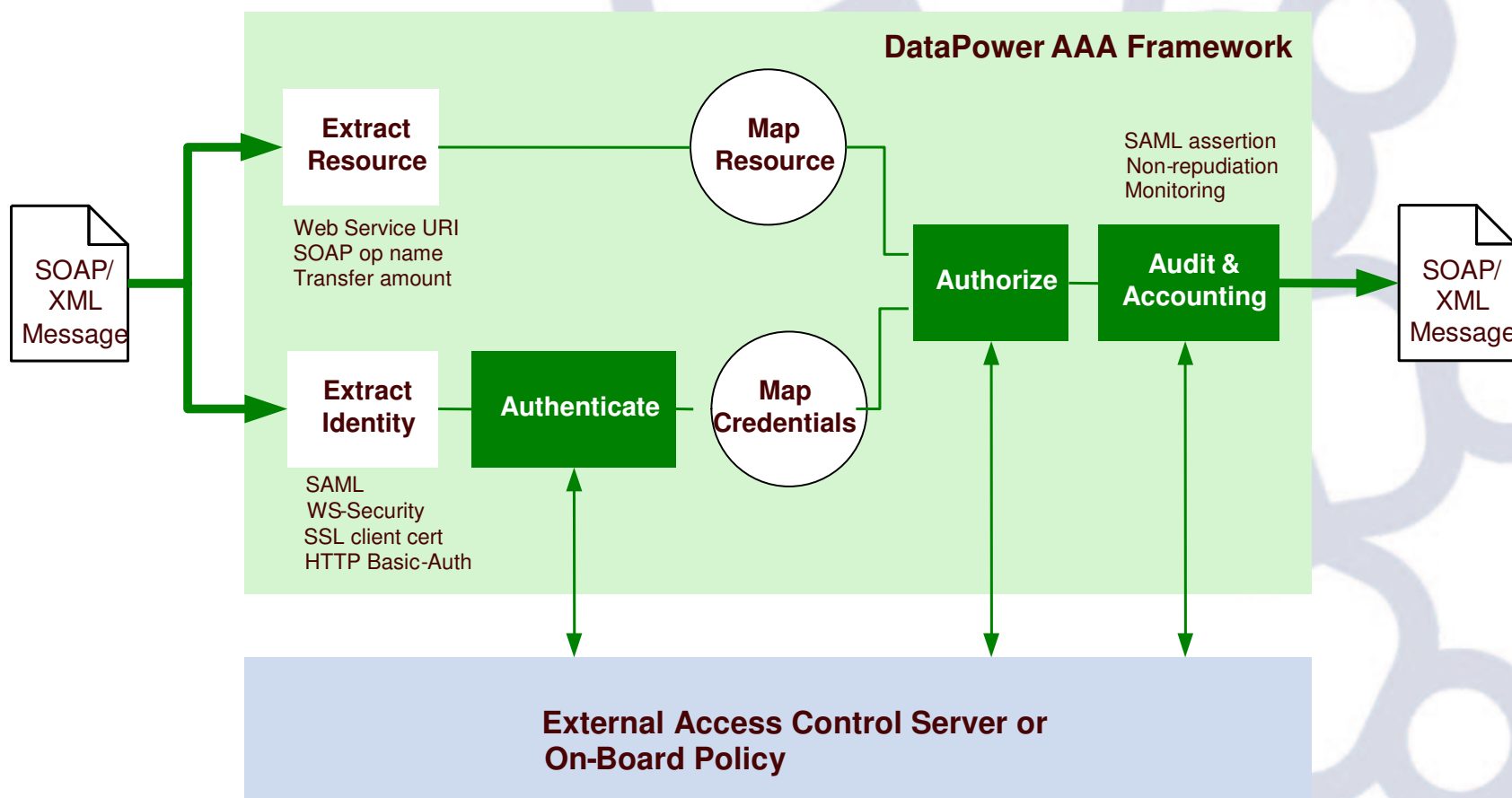
Access Control

Leading Standards and Third-party Integration Support

- **Access control policy:**
 - On-board: certs, XML file [can start simple]
 - Off-board: external access control servers
- **Standards-based integration:**
 - LDAP (for CRL, authentication, authorization)
 - RADIUS (authentication)
 - XKMS (for CRL, authentication)
 - SAML (consume, authentication, authorization, produce)
 - WS-Security, WS-Trust, WS-*
 - Outbound SOAP or HTTP call
- **Integration with access management solutions:**
 - Tivoli Access Manager
 - Tivoli Federated Identity Manager
 - RSA ClearTrust
 - Microsoft Active Directory
 - Sun Identity Server
 - Netegrity SiteMinder or TransactionMinder

Access Control

AAA Framework Diagram - Authenticate, Authorize, Audit



GRACIAS

