
IBM
IBM SOA*
Summit
*Informations valorisées et SOA,
le couple gagnant.

IBM SOA Summit

IBM

Sécuriser les architectures SOA
TA102

Eric Trojman

Senior I/T Architect IBM certified - Enterprise & Security

Agenda

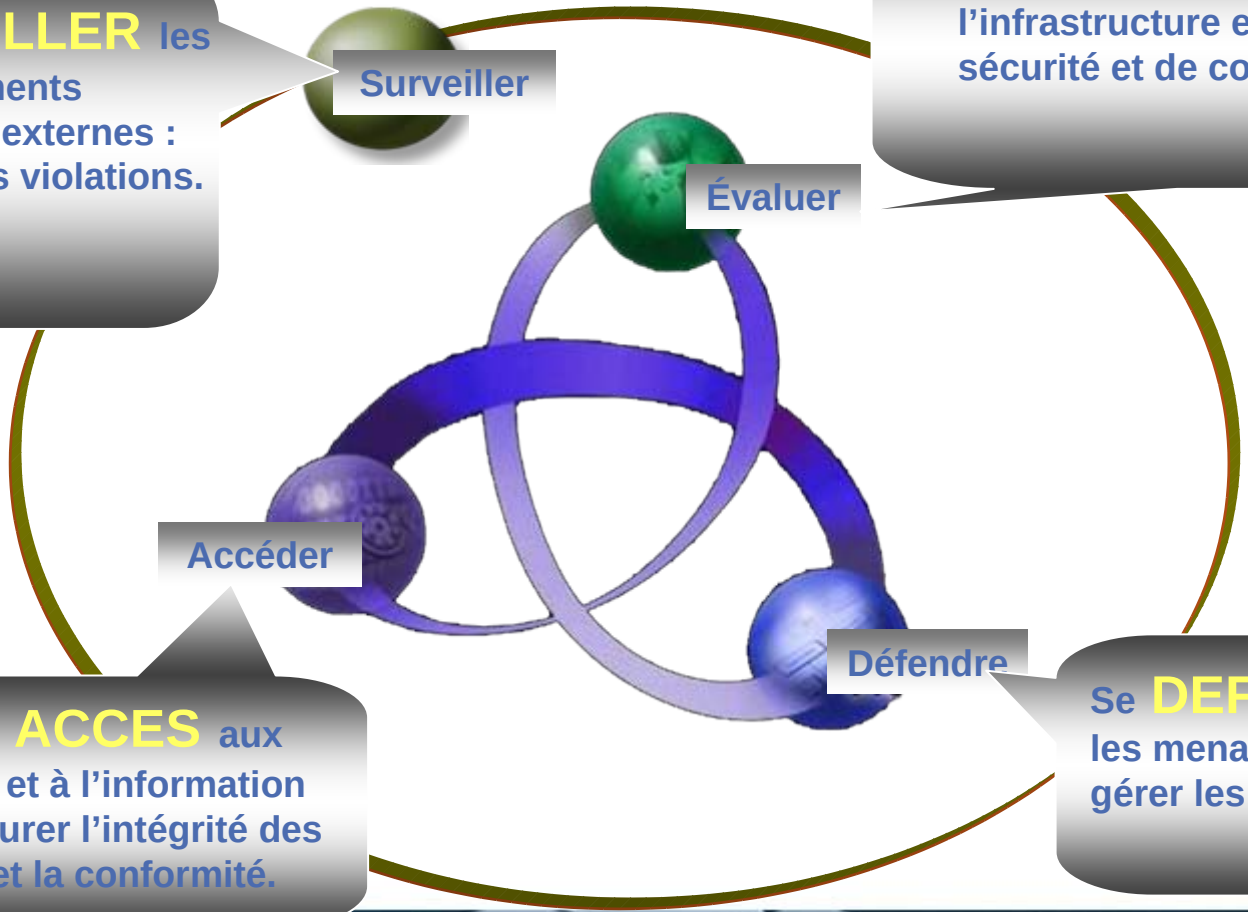
- **L’approche sécurité dans un projet SOA**
- **Inquiétudes sur la sécurité XML. Pourquoi s’en préoccuper ?**
- **Aspects opérationnels des Architectures Orientées Services**
- **Questions & réponses**

L’approche sécurité dans un projet SOA

Stratégie IBM en matière de sécurité

SURVEILLER les comportements internes et externes : détecter les violations.

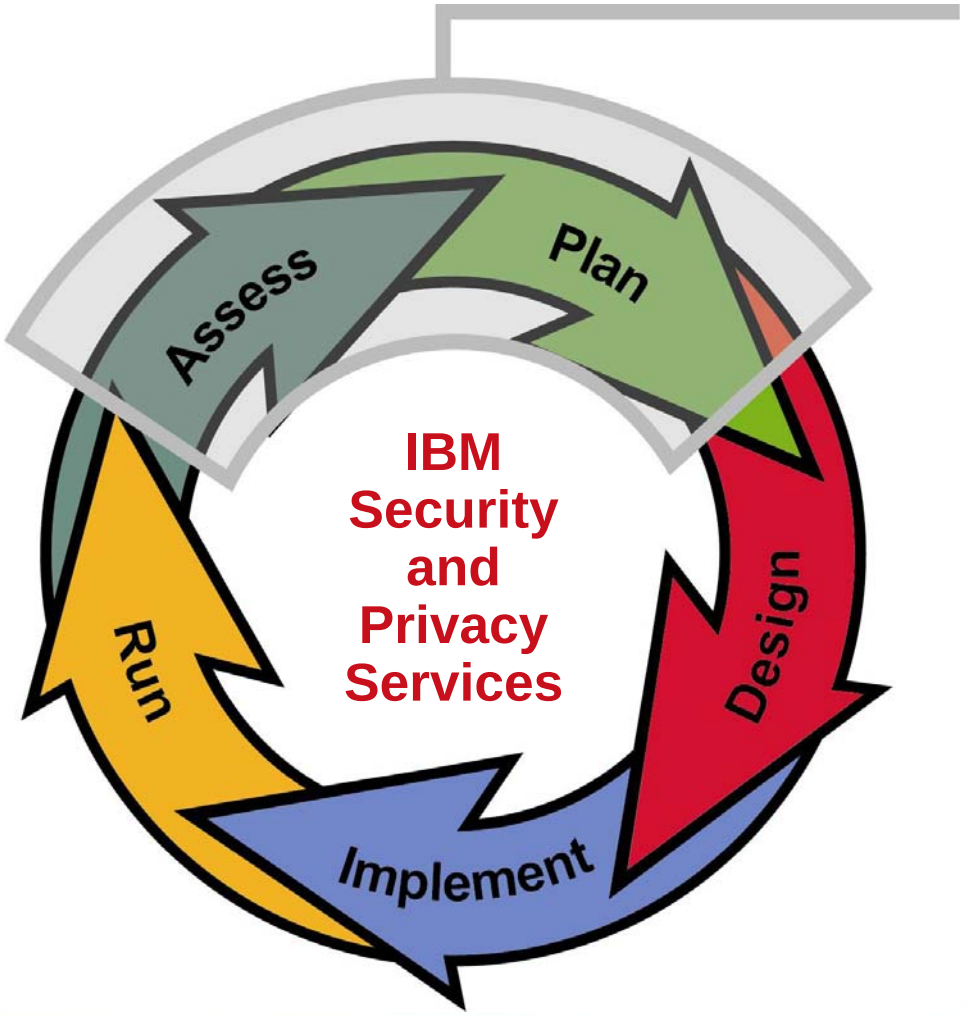
EVALUER le statut de l'infrastructure en matière de sécurité et de conformité.



Gérer les **ACCES** aux systèmes et à l'information afin d'assurer l'intégrité des données et la conformité.

Se **DEFENDRE** contre les menaces de sécurité et gérer les risques.

A reference model for enterprise security program



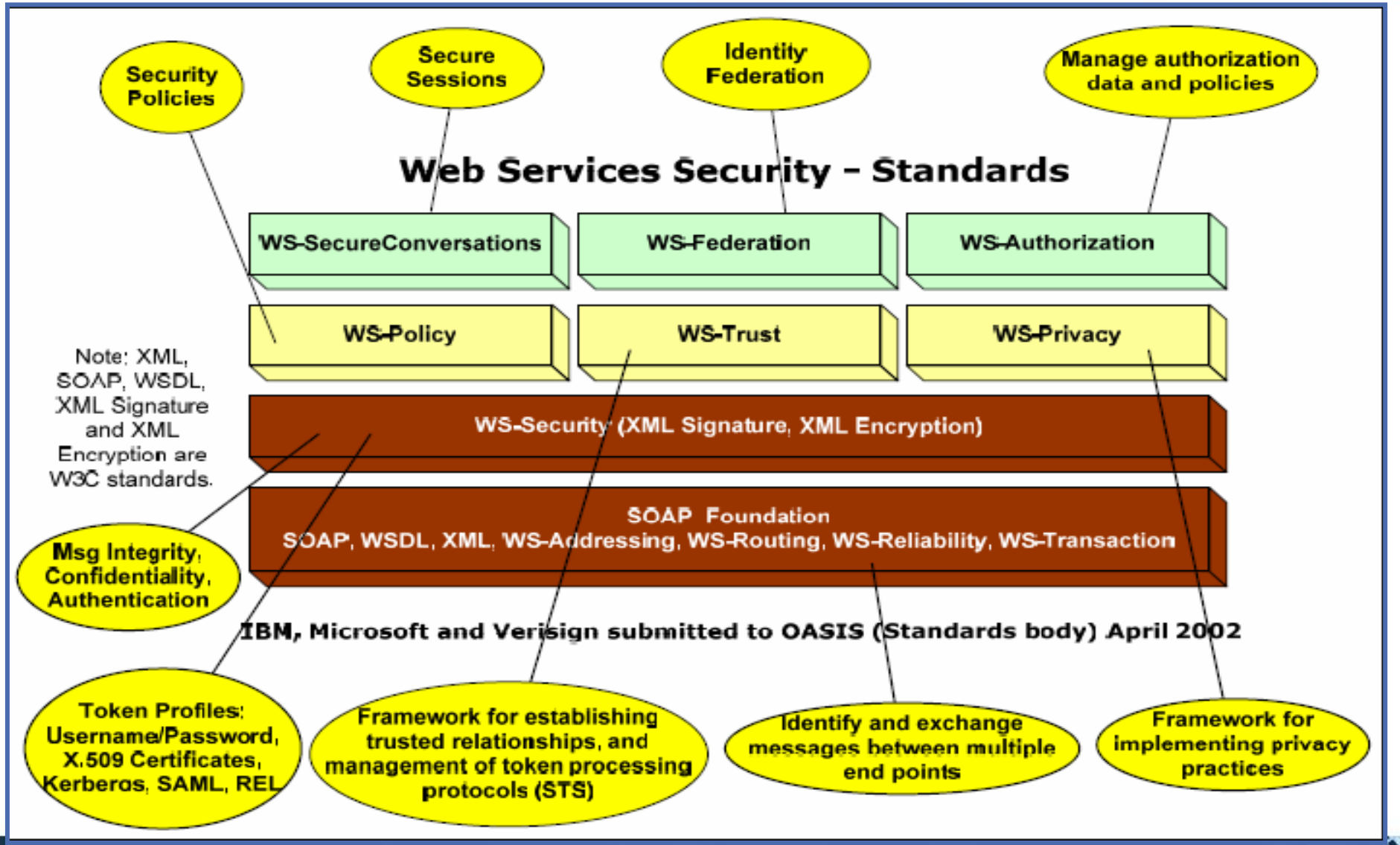
The IBM Information Security Framework is usually applied during the assess and plan phases

An integrated and comprehensive approach to enterprise security, based on best practices, that allows clients to evaluate their security posture and efficiently drive an organization-wide security program that supports their business growth objectives

Fonctions Sécurité SOA
Spécifications de la PSSI

- ***Authentification*** **: vérification de l'identité des** utilisateurs et des services **habilités avant toute interaction entre le système et les utilisateurs.**
- ***Habilitation/Contrôle d'accès*** **: contrôle de l'accès des** utilisateurs et des services **aux informations et aux services.**
- ***Intégrité des informations*** **: protection contre toute modification non autorisée d'information, technique de** scellement**.**
- ***Confidentialité*** **: prévention de toute divulgation non autorisée d'informations sensibles, chiffrement des données** lors des échanges et du stockage **avant et après traitement.**
- ***Disponibilité*** **: assurance que l'accès aux informations est maintenu.**
- ***Audit*** **: enregistrement et** corrélation des activités **permettant la reconstitution des transactions ou des processus.**
- ***Traçabilité****:* **Moyens techniques répondant au besoin d'audit.** authentification de l'origine et du destinataire **des transactions**
- ***Non Répudiation*** **:** Signature **de l'information ou de l'opération comprenant la «** Date Certaine **» .**
- ***Intégrité de l'environnement*** **: protection de l'environnement technique contenant ou gérant les informations.(**Protection aussi physique et opérationnelle **en adéquation avec la sécurité logique.**

Web Services Interoperability (WS-I.org)
Spécification des exigences sécurité dans les contrats



Inquiétudes sur la sécurité XML
Pourquoi s'en préoccuper?

Types d’attaques XML

- Four broad classifications –
  - **XML Denial of Service (xDOS)** – Slowing down or disabling a Web Service so that valid service requests are hampered or denied
  - **Unauthorized Access** – Gaining unauthorized access to a Web Service or its data
  - **Data Integrity/Confidentiality** - Attacks that strike at data integrity of Web Service responses, requests or underlying databases
  - **System Compromise** – Corrupting the Web Service itself or the servers that host it
- These can be facilitated by tricky/complex XML, virus-laden XML/SOAP attachments, etc
- We will cover each class of attack in the following slides

Attaques xDoS à message unique

- **Jumbo Payloads** – Sending a very large XML message to exhaust memory & CPU on the target system
- **Recursive Elements** – XML messages that can be used to force recursive entity expansion or other repeated processing to exhaust server resources
- **MegaTags** – Otherwise valid XML messages with excessively long element names, may lead to buffer overruns
- **Coercive Parsing** – XML messages specially constructed to be difficult to parse to consume the resources of the machine
- **Public Key DoS** – Utilizing the asymmetric nature of public key operations to force resource exhaustion on the recipient by transmitting a message with a large number of long-key-length, computationally expensive digital signatures

Attaques xDoS à messages multiples

- **XML Flood** – Sending thousands of otherwise benign messages per second to tie up a Web Service. This attack can be combined with Replay Attack to bypass authentication and Single Message xDOS to increase its impact.

- **Resource Hijack** – Sending messages that lock or reserve resources on the target server as part of a never-completed transaction. For example, messages that intentionally force lock contention on resources or similar situations.

Attaques sur accès non autorisé

- **Dictionary Attack** –Guessing the password of a valid user using a brute force search through dictionary words.
- **Falsified Message** – Faking that a message is from a valid user, such as by using Man in the Middle to gain a valid message and modifying it to send a different message.
- **Replay Attack** – Re-sending a previously valid message for malicious effect, possibly where only parts of the message (such as the security token) are replayed

Attaques sur l'intégrité et la confidentialité des données

- **Message Tampering** – Modifying parts of a request or response in flight, most dangerous when undetected; less commonly known as "Message Alteration".
- **Data Tampering** – Exploiting weakness in the access control mechanism that permits the attacker to make unauthorized calls to the Web Service to alter data.
- **Message Snooping** – A direct attack on data privacy by examining all or part of the content of a message. This can happen to messages being transmitted in the clear, transmitted encrypted but stored in the clear, or decryption of messages due to stolen key or cryptoanalysis.
- **XPath/XSLT Injection** – Injection of expressions into the application logic. Newer modifications include Blind XPath Injection, which reduces the knowledge required to mount the attack.
- **SQL Injection** – Modifying SQL in XML to obtain additional data than what the service was designed to return.
- **WSDL Enumeration** – Examining the services listed in WSDL to guess and gain access to unlisted services.
- **Routing Detour** – Using SOAP routing header to access to internal Web services

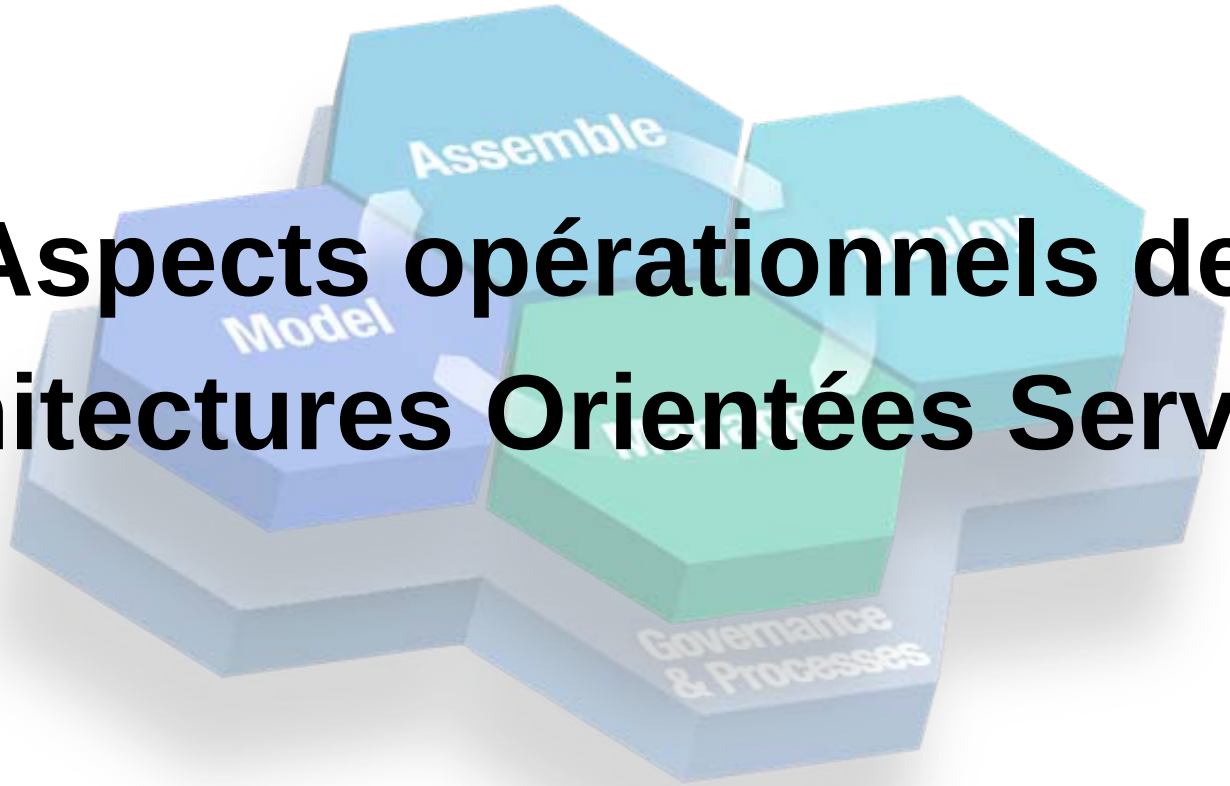
Attaques par mise en péril du Système

- **Malicious Include** – Causing a Web service to include invalid external data in output or return privileged files from the server file system. For example, using embedded "file:" URLs to return Unix password files or other privileged data to the attacker.
- **Memory Space Breach** – Accomplished via Stack Overflow, Buffer Overrun or Heap Error, allows execution of arbitrary code supplied by the attacker with permissions of host process.
- **XML Encapsulation** – Embedding system command in the XML payload, such as through the CDATA tag.
- **XML Virus (X-Virus)** - Using SOAP with attachments or other attachment mechanisms to transmit malicious executables such as viruses or worms.

Résumé sur la sécurité XML SOA

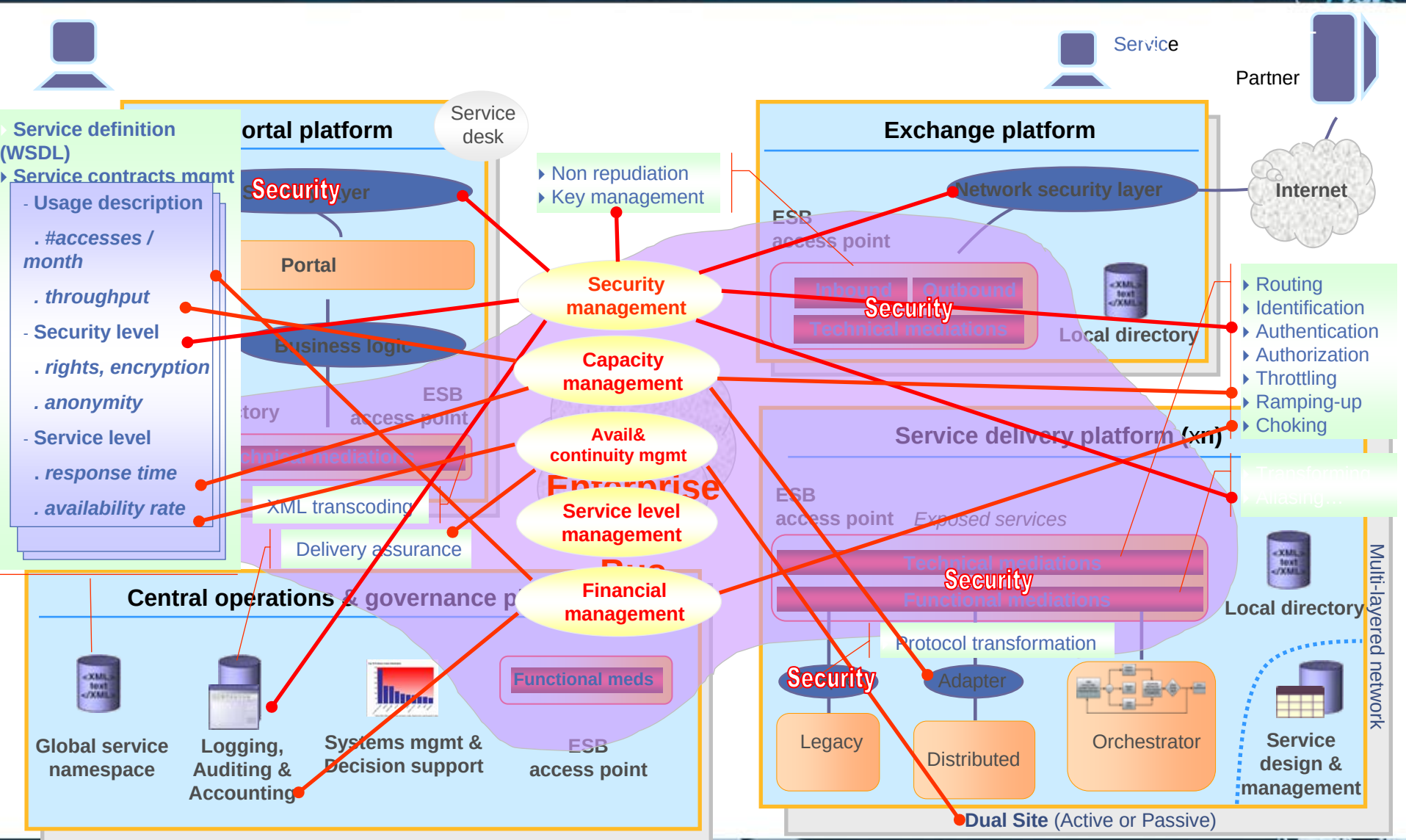
Summary and Conclusion

- To truly harden a system using Web Services, several important security steps need to be performed. These (recommended by Gartner and others) include:
  - Inspecting messages for well-formedness
  - Validating schema
  - Verifying digital signatures
  - Signing messages
  - Implementing service virtualization to mask internal resources via XML transformation and routing
  - Encrypting data at the field level
- In addition, there are other types of monitoring for the types of attacks mentioned above that are needed, as well as configurations to ensure compliance with service-level agreements (SLMs)
  - These intensive actions can be performed by Datapower at the front-end at a significant savings in back-end resource consumption and configuration



Aspects opérationnels des Architectures Orientées Services

Traitement de la sécurité en milieu SOA



Configuration management | Change management | Release management | Incident & problem management

La sécurité par les appliances DataPower

Parse | Schema Validate | XPath Filter | XML Decrypt | Signature Verify | Parse | Schema Validate | XML Transform | XML Sign | XML Encrypt

XML Accelerator
- Offload XML processing
- No more hand-optimizing XML

XA35

- Proxy Web Services Applications
- XML/SOAP Validation and Transformation
- HTML – XML Transformation
- Some XML Threat Protection (XML Parser Limits)
- Logging, including Off-Device Message Logging
- SSL Termination/Initiation
- XML CoProcessor Mode – Java API to Device
- SNMP Management Integration
- Remote Device Management Integration

XML Security Gateway
- Enhanced security capabilities
- Agility – future-proof
- Easy deployment

XS40

XA35 Plus:
- Content Encryption/Decryption
- XML Sign/Verify
- Authentication, Authorization, Auditing
- Dynamic Routing
- Filtering
- Fetch External Content
- Content Extraction
- Attachment Processing
- Full XML Threat Protection
- Web Application Firewall
- WSDL-based Configuration
- Direct Database Access
- MultiProtocol Gateway
- Service Level Monitoring
- WSDM Integration

Integration appliance
- XML to any conversion at wire speed
- Groundbreaking DOP architecture
- Integrated message-level security

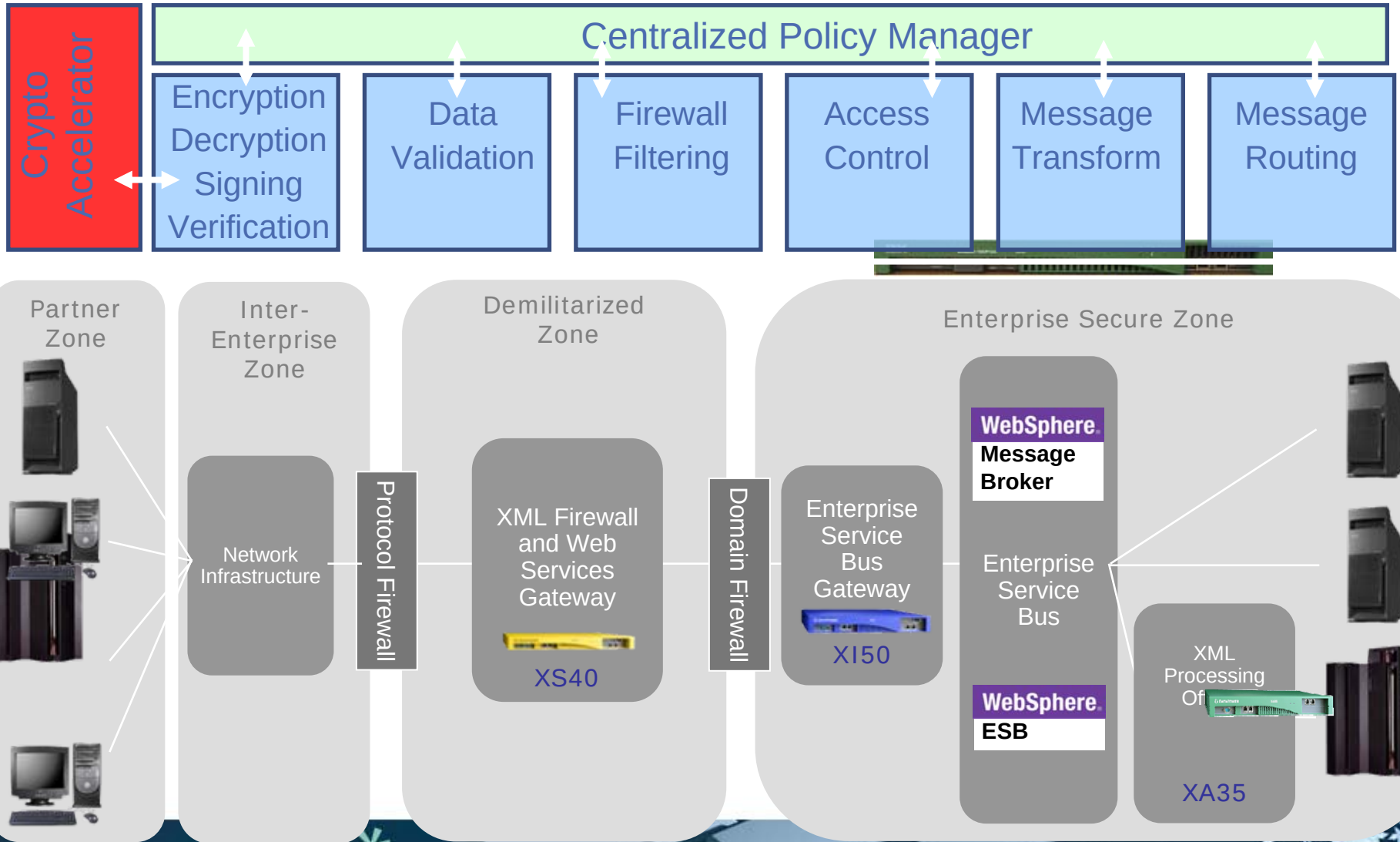
XI50

XS40 Plus:
- MQ Support
- Binary – XML Transformations (DataGlue)
- Tivoli Access Manager support

XML-aware subsystems
- First to break XML gigabit barrier
- Highly embedded OEM

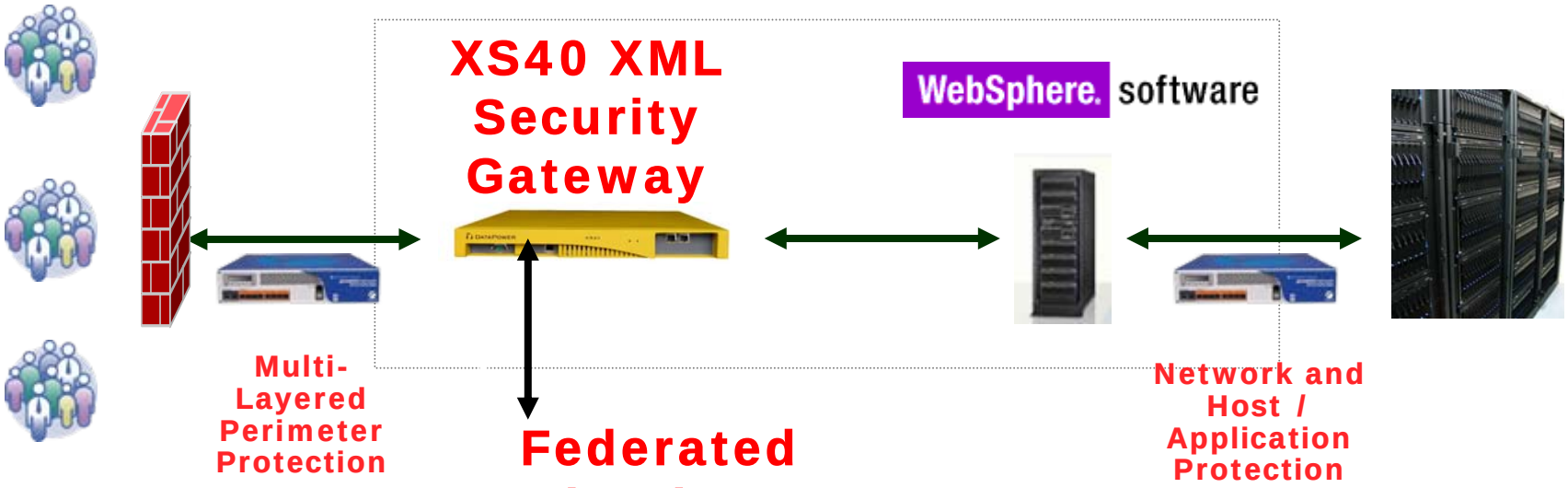
WebSphere software

Where to use WebSphere DataPower?



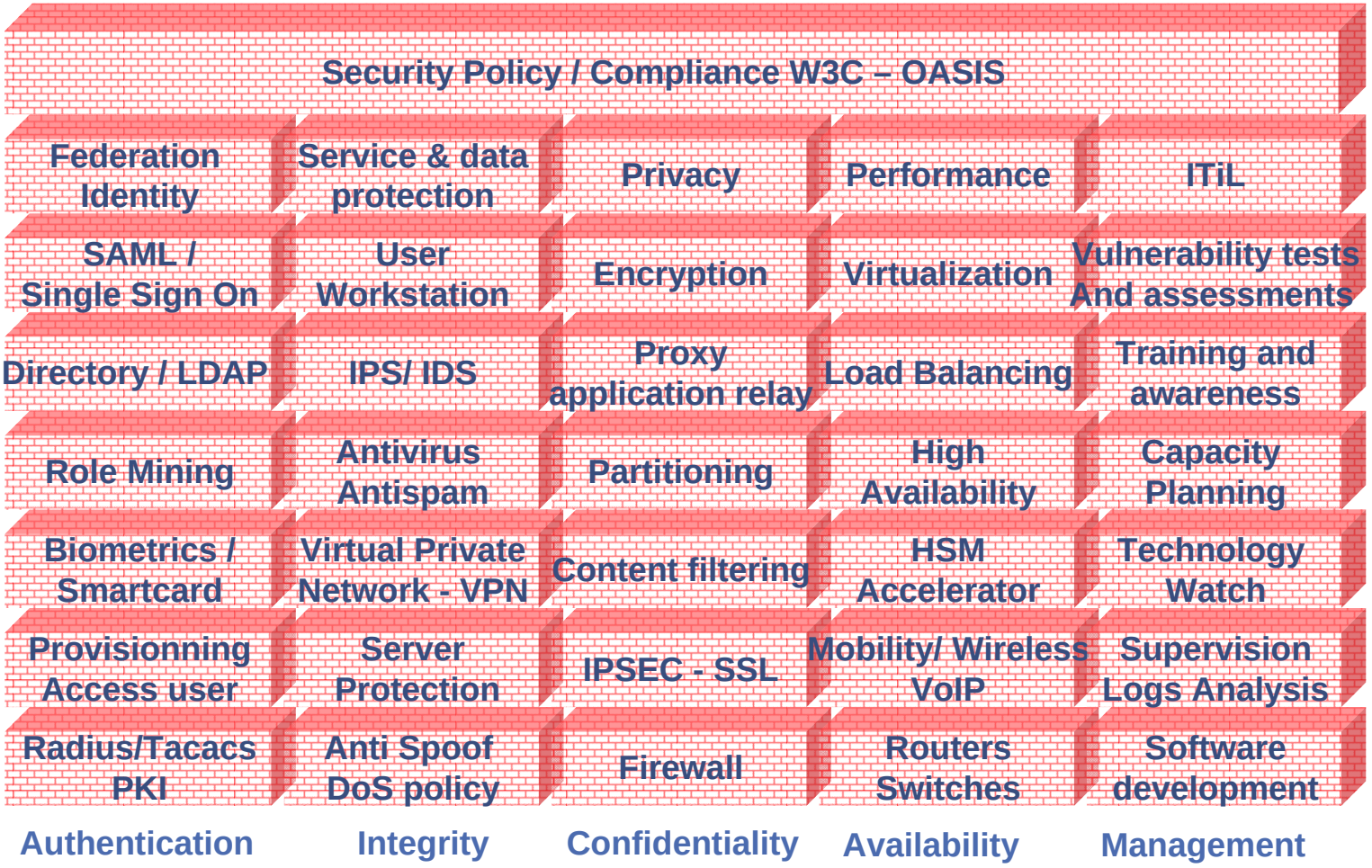
Secure Infrastructure with Tivoli - ISS & DataPower

First line of defense to securely implement external web services. Secure once for many applications and aggregate user interactions



Helps protect SOA implementations addressing XML threats with fine-grain access control. Integrates with security access and policy systems for enterprise SOA deployments and centralized security policy management

Conclusion: synthèse sécurité SOA



धन्यवाद

Hindi

תודה רבה

Hebrew

Grazie

Italian

Спасибо

Russian

Gracias

Spanish

شكراً

Arabic

Merci

French

Obrigado

Portuguese

多謝

Traditional Chinese

Thank You

English

Danke

German

ขอบคุณ

Thai

감사합니다

Korean

多谢

Simplified Chinese

ありがとうございました

Japanese

நன்றி

Tamil