IBM SOA ARCHITECT SUMMIT
LE 22 MAI 2008

Gestion de la sécurité SOA

Mokdad SALHI
Architecte certifié IBM - SOA Leader
msalhi@fr.ibm.com

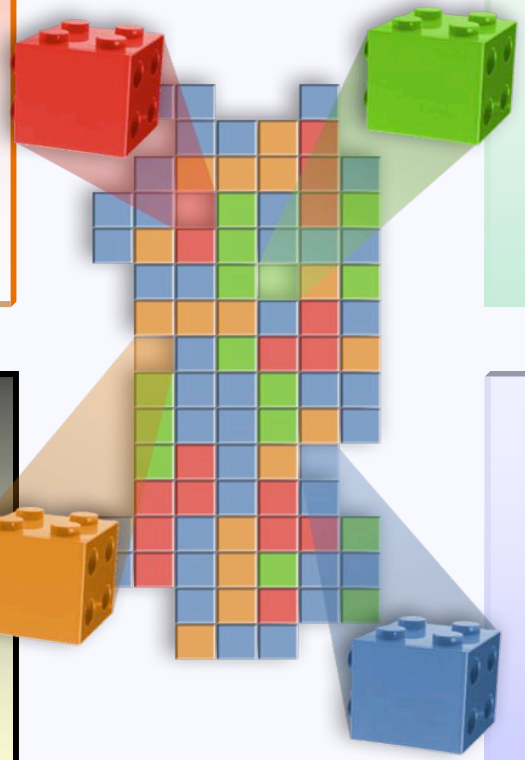
Agenda

1	SOA en deux mots!
2	La sécurité dans un contexte SOA
3	Le modèle WS-Security
4	Les problématiques liées à la sécurisation des services Web
5	La sécurité SOA dans un environnement Tivoli et WebSphere
6	Annexe

Définitions clés du SOA: “Qu’est ce qu’est…”

… un service?

Une opération répétitive



… une orientation service?

Une façon d'intégrer dans le système d’information **les services liés aux besoins de l’entreprise**

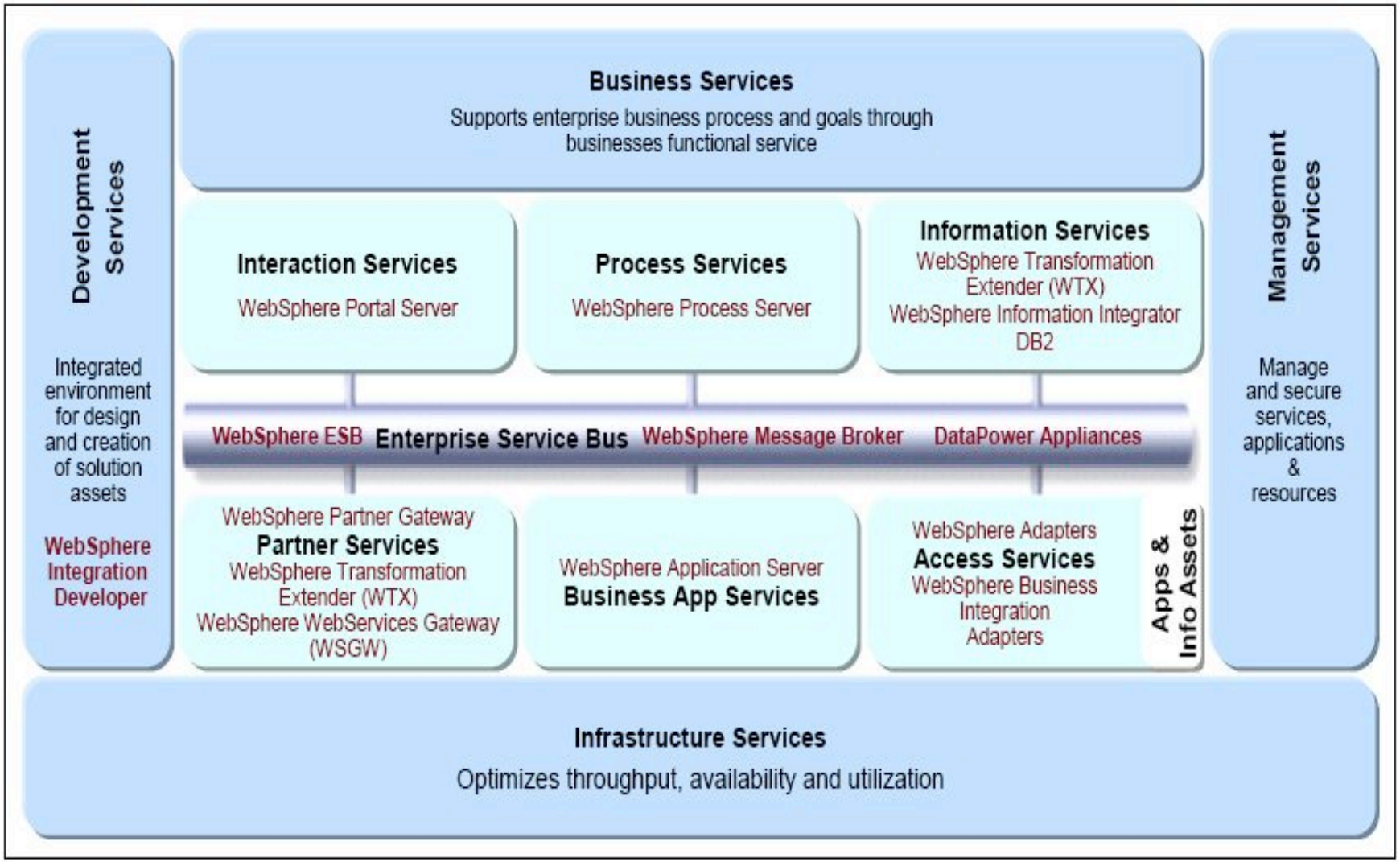
… une architecture orientée service (SOA)?

Un **modèle d’infrastructure IT** qui soutient **l'orientation service**

… une application composée?

Un ensemble de **services connexes et intégrés** qui soutient un processus métier construit sur un modèle SOA

Mappage des produits sur le modèle de référence d'architecture SOA



Agenda

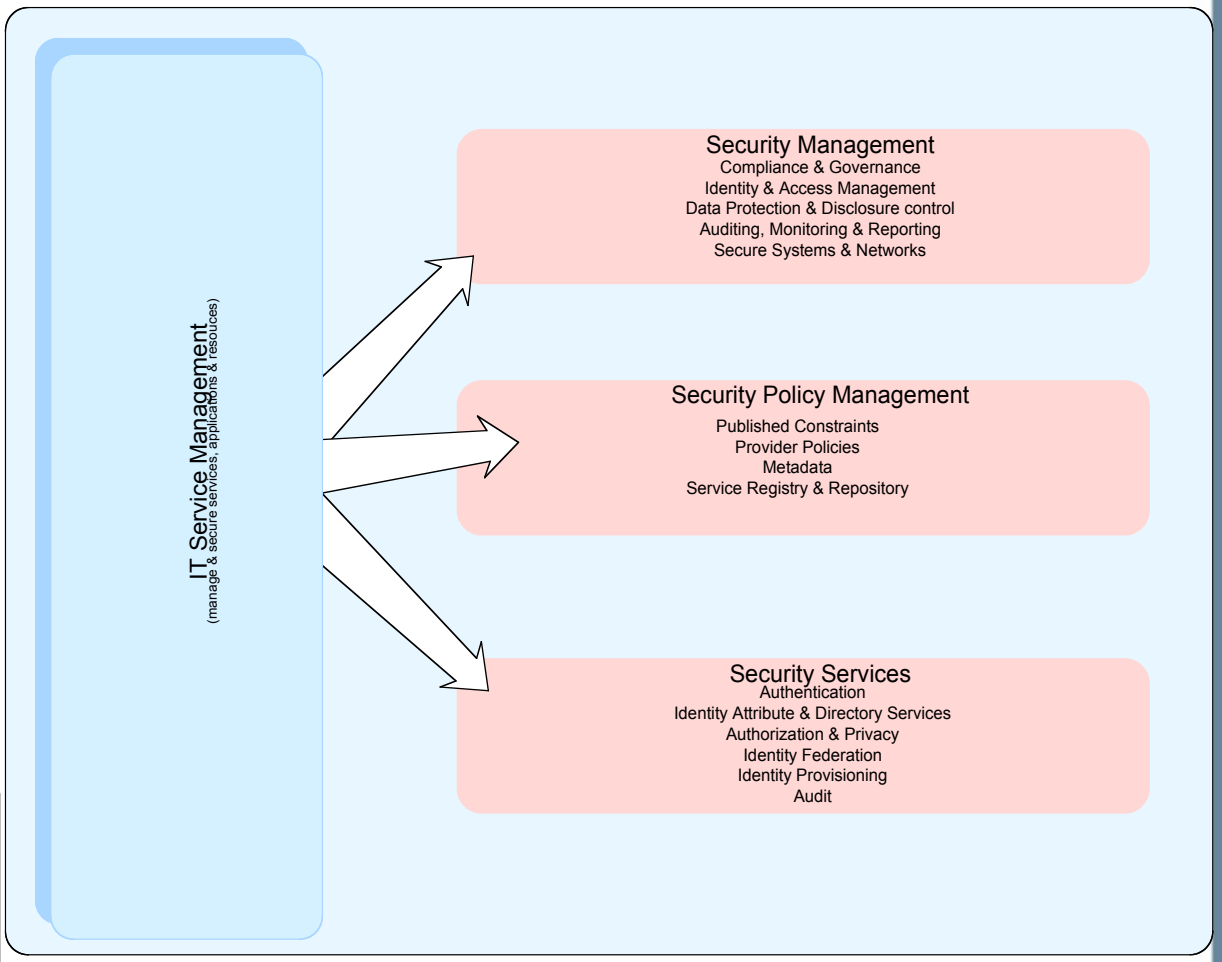
1	SOA en deux mots!
2	La sécurité dans un contexte SOA
3	Le modèle WS-Security
4	Les problématiques liées à la sécurisation des services Web
5	La sécurité SOA dans un environnement Tivoli et WebSphere
6	Annexe

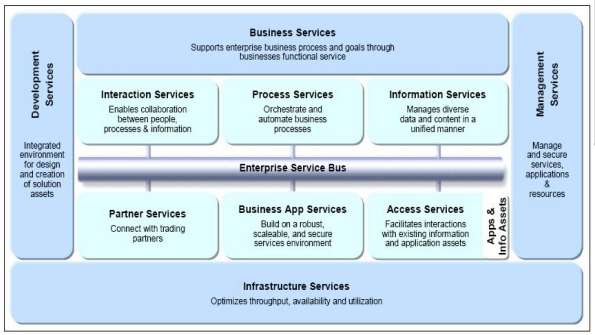
La sécurité SOA

- **Approche métier sur les politiques et les relations**
  - Les règles métier à propos de la sécurité doivent être intégrées dans tout le cycle de vie
  - Les relations de confiance sont différentes en interne et en externe
  - La fédération des services a des implications (en terme de confiance, de technologie et de règles) au delà des frontières imposées
- **Approche architecturale**
  - Faible couplage – L'utilisation des services doit prendre en compte les règles de sécurité
  - Flexibilité et réutilisation - Interopérabilité (standards), Intégration
- **Développement d'applications composites**
  - Les métiers pilotent la sécurité des applications
  - Utilisation de modèles pour simplifier les spécifications des règles de sécurité
- **Approche managériale – les règles et processus**
  - Pilotage de la sécurité avec des règles et des processus
  - Audit, reporting, correctifs, etc inclus dans les processus métier

Modèle de référence de la sécurité SOA

- Les pratiques de Sécurité doivent être alignées avec les processus business
- La sécurité est un service géré par l'infrastructure
- Les applications (services) sont dissociées des règles de sécurité





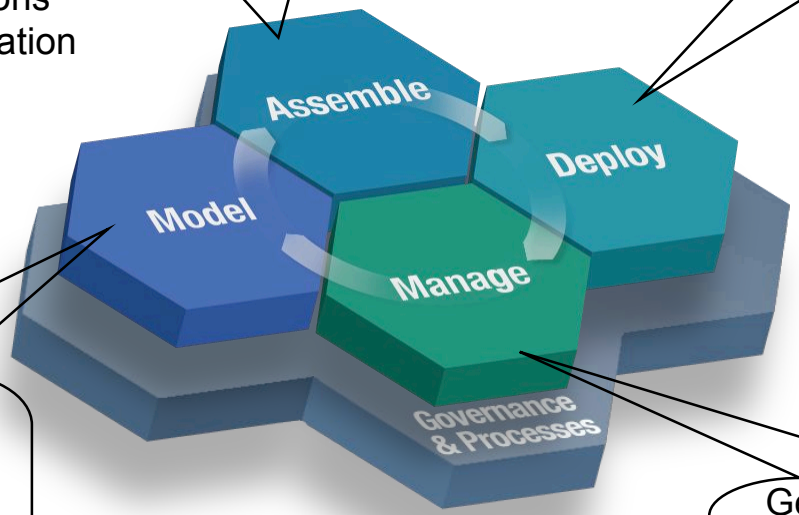
La sécurité englobe tous les aspects du cycle de vie SOA

Déclaration des règles de sécurité pour les applications;
Construction et test d'applications sécurisé

Architecte sécurité
Architecte d'applications
Développeur d'application

Configuration de l'infrastructure pour la sécurité des applications;
Intégration des utilisateurs, des processus et des données

Administrateur d'application
Administrateur sécurité
Développeur sécurité



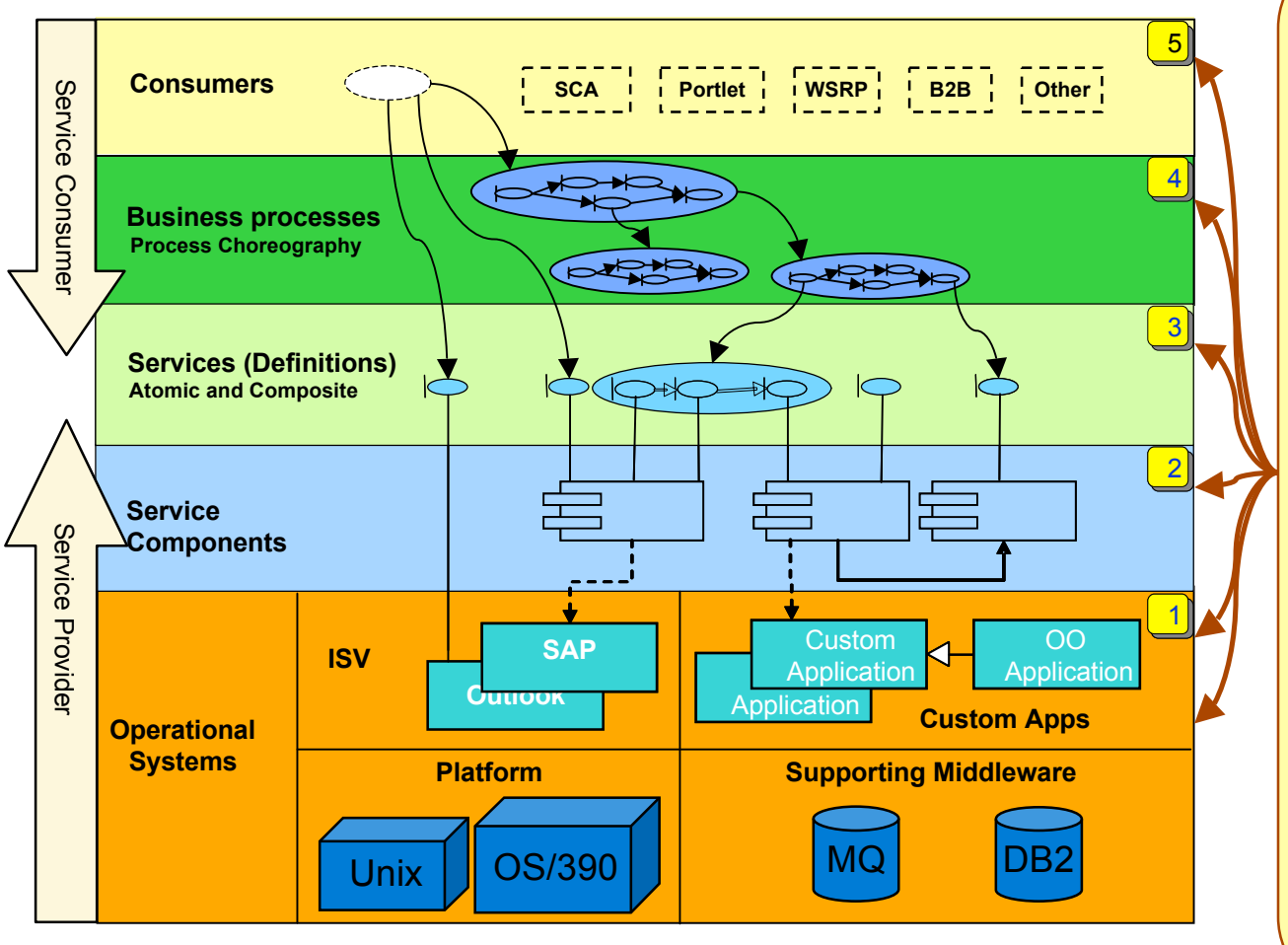
Resp. de la politique de sécurité
Auditeurs sécurité
Analyste métier

Définition des règles de sécurité métiers et de l'entreprise; modélisation des obligations de sécurité et de la sécurité des applications

Administrateur IT
Administrateur sécurité
Exploitant

Gestion de la sécurité des applications;
Gestion des identités et du monitoring pour la conformité

La sécurité englobe tous les aspects du cycle de vie SOA



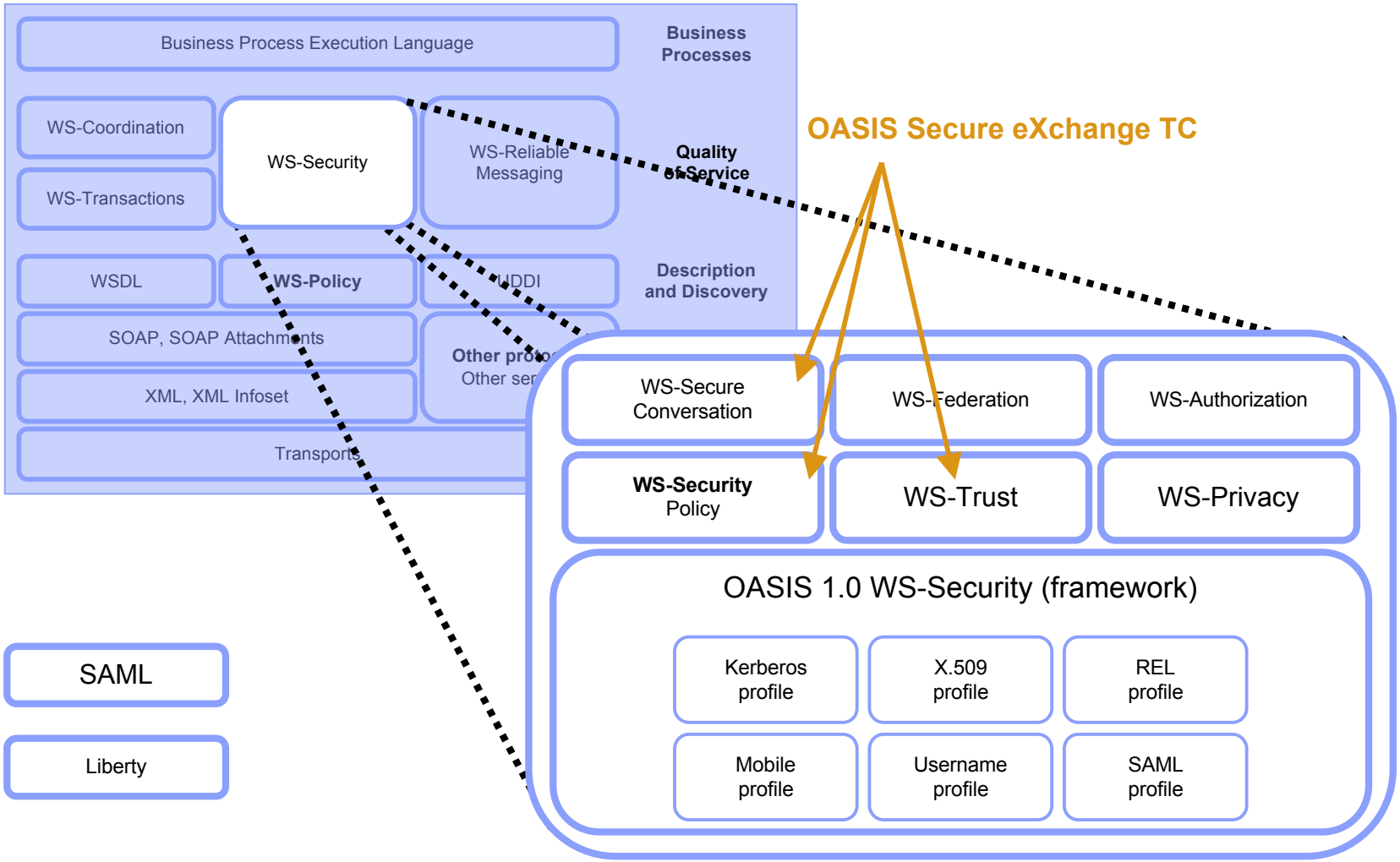
Sécurité SOA

- Identification
- Authentification
- Autorisation
- Audit
- Confidentialité, Intégrité et disponibilité
- Audit et conformité
- Administration et gestion des règles de sécurité

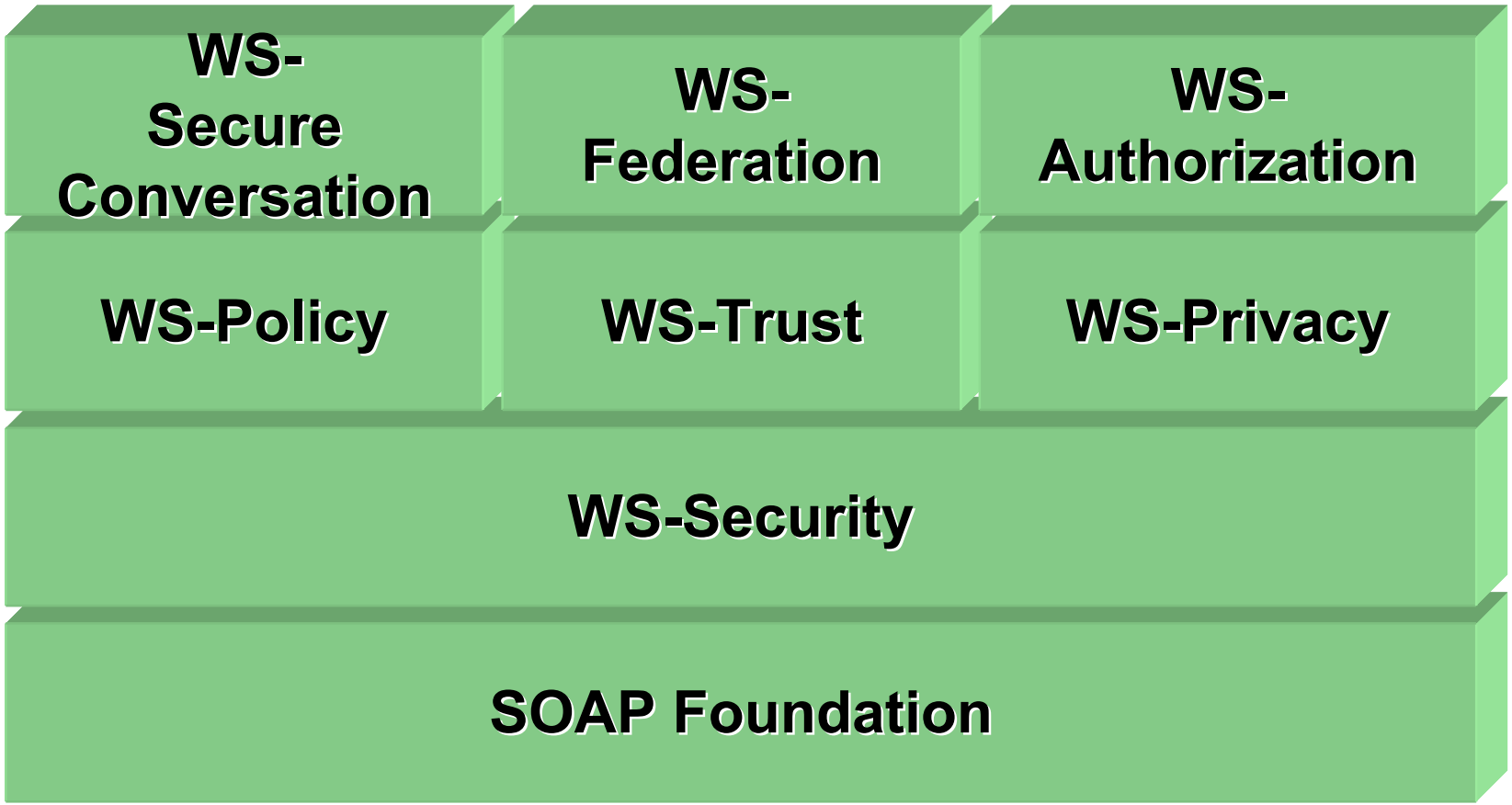
Agenda

1	SOA en deux mots!
2	La sécurité dans un contexte SOA
3	Le modèle WS-Security
4	Les problématiques liées à la sécurisation des services Web
5	La sécurité SOA dans un environnement Tivoli et WebSphere
6	Annexe

Modèle WS-Security



Framework de la sécurité des services Web



Agenda

1	SOA en deux mots!
2	La sécurité dans un contexte SOA
3	Le modèle WS-Security
4	Les problématiques liées à la sécurisation des services Web
5	La sécurité SOA dans un environnement Tivoli et WebSphere
6	Annexe

Problèmes liés à la sécurité des services Web

- La SOA et les services Web fonctionnent avec des technologies basées sur le Web, ils héritent donc de tous les risques de cette technologie
- La mise en oeuvre d'une SOA et des services Web héritent des limitations de sécurité de l'existant :
  - Les règles et processus organisationnels
  - L'architecture de la sécurité de l'entreprise
- La mise en oeuvre d'une SOA et de services Web nécessite la publication des services et de leur description
  - Des mesures de sécurité explicites doivent être utilisées pour assurer la confidentialité et établir les règles de confiance

Problématiques liées à la sécurité des services Web

Les menaces au niveau de la sécurité des messages incluent :

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

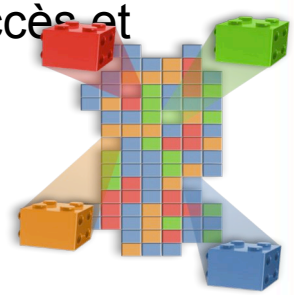
System Compromise – Corrupting the Web Service itself or the servers that host it

Agenda

1	SOA en deux mots!
2	La sécurité dans un contexte SOA
3	Le modèle WS-Security
4	Les problématiques liées à la sécurisation des services Web
5	La sécurité SOA dans un environnement Tivoli et WebSphere
6	Annexe

La sécurité SOA : les apports de Tivoli

- Un service métier est une tâche métier répétitive
- Les applications métier sont créées en combinant une série de services métiers
- Une infrastructure de sécurité permet à une application de ne pas se soucier de la sécurité
- Ce framework permet aux données et processus de sécurité d'être gérés par l'infrastructure ou le middleware
- Une architecture IAM (Identity and Access Management) commune peut vous aider :
  - à éliminer les coûts associés à la conception et au développement "one-off" dans chaque groupe d'applications
  - à réduire ou éliminer le matériel et les logiciels spécifiques aux plateformes qui supportent l'administration de la sécurité
  - à faciliter l'intégration des applications en fournissant une infrastructure d'authentification et d'autorisation communes telles que la gestion des répertoires, des mots de passe, des utilisateurs, des contrôles d'accès et des produits de fédération



Web Services Security Framework

- **Tivoli Access Manager for e-Business (TAM)**
  - Moteur d'identification et de contrôle d'accès
- **Tivoli Identity Manager (TIM)**
  - Moteur de provisioning
- **Tivoli Federated Identity Manager (TFIM)**
  - Moteur SSO fédéré et WS-Security
- **WebSphere DataPower (XS40)**
  - Renforce la sécurité des flux XML et des Web Services
- **WebSphere Partner Gateway**

Composants TAM

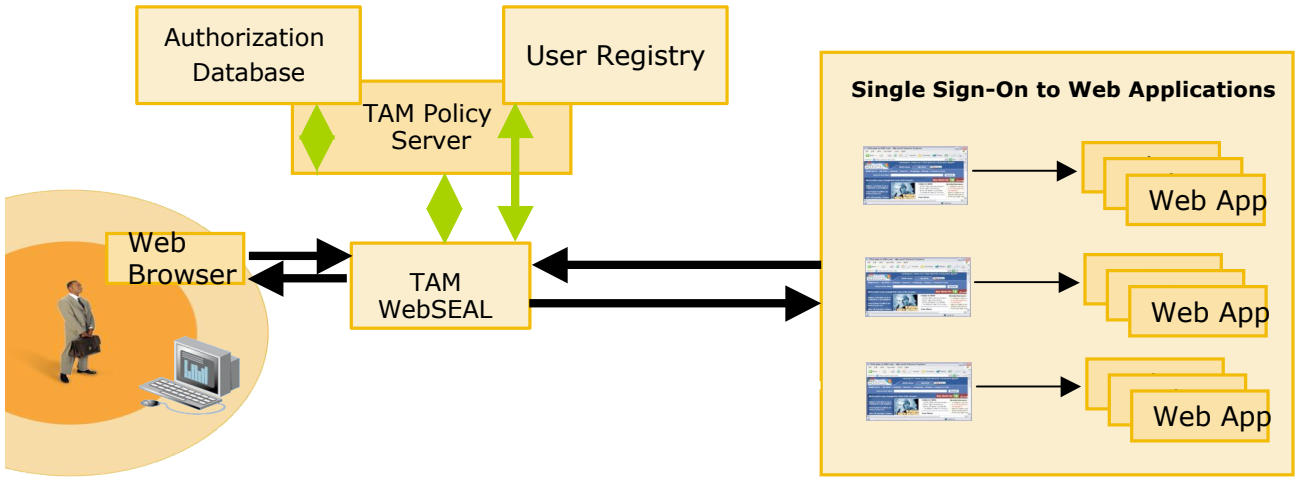
Tivoli Access Manager, une famille de poduits incluant :

- Tivoli Access Manager pour l'e-business
  - Tivoli Access Manager WebSEAL
  - Tivoli Access Manager Plug-In for Web Servers
  - Tivoli Access Manager JACC (WebSphere)
  - Tivoli Access Manager pour WebLogic
  - Tivoli Access Manager pour .NET
  - Tivoli Access Manager Web Portal Manager
  - WebSphere Application Server (Single Server)
  - Tivoli Directory Integrator
  - Tivoli Directory Server
  - DB2 UDB
- Tivoli Access Manager for Enterprise Single Sign-On (Passlogix)
  - Environnement de postes clients windows uniquement
- Tivoli Access Manager for Operation Systems (TAMOS)
  - Unix et Linux seulement

Avantages TAM

- Identification, Accès et Audit centralisés
- Permet le SSO
- Modèle de sécurité commun
- Base pour la fédération d'identité
- Guidé par la politique
- Administration centralisée
- S'intègre à Tivoli Identity Management

Exemple



IBM Tivoli Federated Identity Manager

L'objectif de TFIM est de fournir la sécurité et l'identité relative aux services à un environnement SOA.

Domaines de focus actuels :

- Single Sign-On (SSO)
  - SSO fédéré, basé sur le navigateur
  - Médiation d'identité pour les services Web
    - Mappage des identités entre les domaines
    - Mappage des formats d'échange des identités entre les domaines
    - Interface vers les services d'autorisation
- Gestion de la politique de médiation d'identité
  - Service de jeton (Token) de sécurité (STS) basé sur WS-Trust
    - Gestion intégrée des identités et des pré requis des formats d'échanges d'identité pour les fournisseurs et les utilisateurs des services.

Gestion fédérée de l'identité (Federated Identity Management)

- **Définition**
  - Une "fédération d'identité" est une fédération dans laquelle la gestion de l'identité (identification, contrôle d'accès, audit et provisioning), est distribuée entre les partenaires selon leur rôle dans la fédération.
  - Une fédération d'identité peut permettre aux utilisateurs d'un des partenaires de la fédération d'accéder ***sans accro*** aux ressources d'un autre partenaire de manière sécurisée et ***fiable***.
- **Rôles**
  - Utilisateur final
  - Identity Provider (IdP) – fournisseur d'identité
  - Service Provider (SP) – fournisseur de service
- **Fonctions**
  - Single Sign-On/Sign-Off (incluant le "global" sign-off)
  - Provisioning/De-provisioning

Capacités de Tivoli Federated Identity Manager (TFIM)

- Single sign-on (SSO)
- SSO fédéré basé sur le navigateur
- Médiation d'identité pour les Web Services
- Mappage des identités entre les domaines
- Mappage des formats d'échanges d'identités entre les domaines
- Interface avec les services d'autorisation
- Gestion de la politique de médiation d'identité
- Services de jeton de sécurité WS-Trust, Security Token Services (STS)
- Gestion des identités des fournisseurs et consommateurs de services

IBM DataPower XS40 Security Gateway Appliance
L'appliance qui assure aux Web Services XML une sécurité complète à la vitesse du réseau

Sécurité SOA (XML et Web Services)
Administration centralisée de la sécurité

Pare-feu XML/SOAP Firewall – Filtre sur tout type de contenu, méta-données ou variables réseau

Validation des données – Vérifie le trafic XML et SOAP entrant/sortant à la vitesse du réseau

Sécurité au niveau du champ - WS-Security, chiffre et déchiffre des champs individuels, non répudiation

Contrôle d'accès XML et Web Services (AAA) - SAML, LDAP, RADIUS, etc.

Routage du message basé sur le contenu

- Enrichissement du message

MultiStep - Pipeline d'exécution des traitements

Administration des Web Services Management – Gestion des niveaux de service, Virtualisation de service, Administration de la politique

Flexibilité au niveau du transport - HTTP, HTTPS, SSL

Administration et configuration aisée - Interface graphique Web, CLI, IDE et Eclipse
Configuration pour adresser tous les besoins de l'entreprise (Architectes, Développeurs, Administrateurs réseau, Administrateurs de la sécurité, etc.)

Sécurité complète pour les Web Services

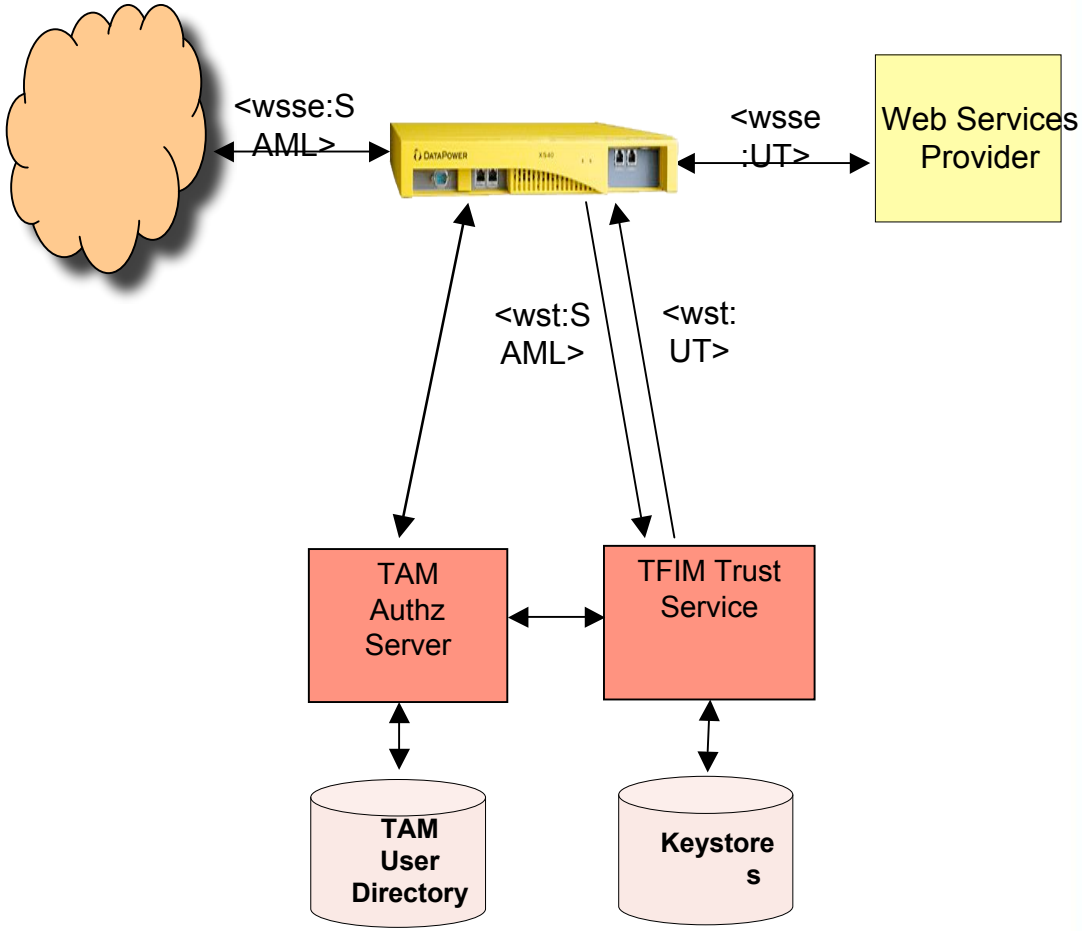
XA35

- 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

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



धन्यवाद
Hindi

Grazie
Italian

Спасибо
Russian

شكرا
Arabic

Gracias
Spanish

Obrigado
Portuguese

Merci
French

多謝
Traditional Chinese

Thank You
English

Danke
German

多谢
Simplified Chinese

ขอบคุณ
Thai

감사합니다 감사합니다
감사합니다 감사합니다
감사합니다 감사합니다
Korean

ありがとうございました
Japanese

நன்றி
Tamil

Fonctions Sécurité SOA – Spécifications

- ***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.

Agenda

1	SOA en deux mots!
2	La sécurité dans un contexte SOA
3	Le modèle WS-Security
4	Les problématiques liées à la sécurisation des services Web
5	La sécurité SOA dans un environnement Tivoli et WebSphere
6	Annexe

WS-Security

Un ensemble de spécifications qui :

- Assure la sécurité des messages de bout en bout
- Est indépendant de la couche transport
- Supporte SOAP, PKI, Kerberos, et SSL
- Supporte de multiples formats de jetons de sécurité (security token)
- Supporte de multiples domaines de confiance
- Supporte de multiples formats de signatures
- Assure l'intégrité des message via des signatures et des jetons de sécurité XML
- Assure la confidentialité des message via le cryptage et les jetons de sécurité XML

WS-Policy

- C’est une syntaxe extensible pour identifier les possibilités, les besoins et les caractéristiques générales de chaque entité
- C’est un ensemble de spécifications (i.e. schéma d’authentification, protocoles, caractéristiques QoS, besoins de cryptage, durée de vie des jetons de sécurité, types de jetons de sécurité, etc.)
- Ne spécifie PAS la manière dont les règles sont associées aux entités

WS-Federation

- Spécifie la manière dont la fédération des entités est implémentée
- Décrit comment la sécurité des services Web existants est implémentée pour fournir des mécanismes de confiance, gestion des attributs et SSO
- Est particulièrement concerné par les relations entre les parties fédérées
- Fournit une identité numérique sécurisée basée sur des standards et des plateformes de confiance pour des plateformes de services Web

WS-Trust

- Est un framework pour l'interopérabilité des modèles de confiance
- Permet d'étendre WS-Security pour supporter l'émission, l'échange et la validation des jetons de sécurité
- Permet l'émission et la diffusion des certificats de sécurité à travers différents domaines

WS-Privacy

- Spécifie la communication des préférences en matière de confidentialité décrite par WS-Policy
- Est un modèle utilisé par WS-Security pour associer aux messages une déclaration de confidentialité
- Permet à WS-Trust d'évaluer à la fois les préférences utilisateurs et les règles de l'entreprise concernant les déclarations de confidentialité

WS-Authorization

- Est un framework pour gérer les autorisations
- Définit la manière dont les politiques d'accès sont définies et gérées

WS-Secure Conversation

- Étend WS-Security et WS-Policy pour sécuriser les communications entre services Web
- Est focalisé sur l'authentification des messages
- Est un mécanisme pour établir et partager les contextes de sécurité
- Décrit la méthode pour extraire les clés d'un contexte sécurité

WS-Security Policy

- Décrit comment les messages doivent être sécurisés
- Est un ensemble de règles pour la sécurité des messages SOAP, WS-Trust et WS-Conversation
- Supporte de multiples méthodes de cryptage et types de jetons

WS-Provisioning

- Interfaces de programmation (API) et schéma pour l'interopérabilité entre les solutions de provisioning
- Est basé sur des concepts directoires
- Tire profit des schémas WSDL et XML

Security Assertions Markup Language (SAML)

- Est développé par un consortium d'éditeurs, incluant IBM, sous la direction de OASIS
- A pour but de fournir des standards pour une interopérabilité de SSO entre les vendeurs
- Est une assertion au format XML
- Inclut des informations sur l'identité de l'utilisateur
- Est indépendant de l'éditeur
- Versions 1.0 et 1.1 focalisés sur SSO
- Version 2.0 supporte la gestion de tout le cycle de vie de l'identité de l'utilisateur
- Version 2.0 est influencée par le projet Shibboleth et la norme Liberty ID-FF 1.2

eXtensible Access Control Markup Language (XACML)

Est le langage commun pour définir les besoins et les règles en matière de contrôle d'accès. Il supporte les fonctions suivantes :

- Définition des règles
- Attribution des critères d'évaluation des règles
- Évaluation des règles
- Exécution des règles

Java Authorization Contract for Containers (JACC)

- Définit des nouvelles classes de permissions pour EJB et de nouvelles permissions web dans les descripteurs de déploiement J2EE
- Fournit des interfaces et des règles permettant aux fournisseurs des autorisations de communiquer avec des containers d'applications J2EE
- Retire les décisions d'accès du serveur d'applications
- Fournit des standards pour permettre aux fournisseurs d'autorisations de s'interfacer avec les serveurs applicatifs

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.