SOA Security Programming Model

Anthony Nadalin
Distinguished Engineer
IBM Corporation

Presented by Mike Perks
Agenda

• Securing an on demand business
  • Business requirements
  • on demand security infrastructure

• Service Oriented Architecture and Security
  • Federation and trust management
  • Business driven application security
Security is a Business Requirement that ...

- Affects Business Strategy
- Impacts Business Processes and Operations
- Helps Secure Business Applications
- Needed to Secure the Infrastructure
# Customer Pain Points

| Protecting privacy and security of customer and employee information |
| Securing exchange of business critical information |
| Manage identity within and across enterprise(s) |
| Ensure integrity of the environment (delegated, federated) |
| Manage security policies to mitigate risks |
Understanding the pain points lead to ..
on demand security infrastructure

- Business Controls, Risk and Security Governance
- Identity and Access Management
- Data protection and disclosure control
- Secure Transactions
- Secure Systems and Networks
- Security Monitoring and audit

on demand security management disciplines

on demand security fabric

Tooling for model driven security infrastructure
that help secure an on demand environment..
So as to achieve ...

- Enterprise Integration and Virtualization
  - Security Services
  - Security components
  - Pluggability and customizability
  - Consistent and coherent model

- Based on
  - Service Oriented Architecture
  - Componentization
  - Standards based interoperability and integration
  - Loose coupling and virtualization
  - Adapters to legacy applications

- Using
  - Security policies from executives to IT staff
  - End to end tools from modeling to infrastructure management
  - Governance model and delegation of authority
Using Security Fabric that is Standards Based and Pluggable

On Demand Applications

Utility Business Services

Enterprise Service Bus

Business Application Services

Runtime Security APIs
(login, authorization, etc)

Administrative Security APIs
(create user, change policy, ...)

Vendor API extensions
(J2EE, Unix, ...)

Operating Environment Security Runtime
- Credential propagation, authentication, context establishment, authorization checks, audit, privacy,

Authentication SPI
Kerberos, RACF
3rd Party

User Registry
LDAP, OS registry
3rd Party

Authorization SPI
Authz provider
3rd Party

Cred Mapping SPI
Mapping provider
3rd Party

Identity Management
Management provider
3rd Party

Policy, Audit, Intrusion Detection, Privacy

Security Services Infrastructure

WS-Trust
WS-Attribute Service
WS-Authorization
WS-Trust
WS-Attribute Service
WS-Policy
WS-Privacy

WS-Federation
Agenda

• Securing an on demand business
  • Business requirements
  • on demand security infrastructure

• Service Oriented Architecture and Security
  • Federation and trust management
  • Business driven application security
Federated Lifecycle Management

Partner Enrollment

Business Driven Trust Agreements
- Technical Policies
- Operational Best Practices
- Security & Identity Agreements
- Audit Agreements
- Privacy Agreements

Partner Enrollment
- Credentials Management
- Partner-Role-Attribute Management
- User Life cycle Management
- Transaction/Data Agreements
- Scenario Management

Partner-User Enrollment
- Provisioning/Deprovisioning
- Role/Permission Management
- Attribute change Management
- Identity Relationship Management
- Federation/De-federation

Scenario Realization

Anthony Nadalin — SOA Security Programming Model
Federations Require Trust

- Trust
  - Reflects business relationship
  - Needs governance model
  - Implemented using technology

- Trust between Identity Provider and Service Providers
  - This can be implemented using technology
  - Trust can be provided by WS-Trust, WS-Security, WS-SecureConversation

- Trust between users and Identity Providers
  - This can be facilitated by technology
  - Requires business, legal and “faith based” solutions

- Trust by users of how IdP will use their information
  - This can be mitigated by WS-Policy family
  - Also requires business, legal and “faith based” solutions
Web Services Security Model

End to End Security model simplifies integration between companies
Each Web Services message can be individually authenticated, integrity & confidentiality protected and authorized

WS-Security Family
(Kerberos, X.509, SAML)

Soap
HTTPS, JMS, MQ
Web Services Security

Services Driven Interactions

Suppliers
Partners
Company Portal
Applications
Legacy Applications
Remote Portals

SOAP/HTTP
SOAP Web Services
Web Services Remote Portlets
Non Web Services
Web Services

How do we identify and authenticate the service requester?
How to we identify and authenticate the source of the message?
Is the client authorized to send this message?
Can we ensure message integrity & confidentiality?
How can I audit the access to Web Services?

Multiple layers of enforcement – perimeter, gateway, app server, application
End to End Message Security

(trust relationship)

Security Context

Requester → Intermediary → Web Service

(trust relationship)

Security Context

(trust relationship)
Managing Trust

[Diagram showing the flow of a security token service with nodes for Requestor, Security Token, Policy, Claims, and Web Service connected through Audit, Security Token Service, Policy, and Claims.]
Managing Integrity

- Manage trust

- Use Infrastructure components
  - May be shared
  - Need to be trusted components (they are the enforcement points)
  - Interaction (with partners, etc) and role played by infrastructure is managed
  - Delegated authority to LOBs

- Application specific policies
  - Shared infrastructure but different policies (specific to LOB, application, etc)
  - Gives flexibility and control

- Compliance
  - Audit and monitoring
  - Accountability and integrity
Web Services Security Roadmap

SOAP Foundation

WS-Security

WS-Policy

WS-PolicyFramework

WS-PolicyAttachments

WS-PolicyAssertions

WS-SecureConversation

WS-Federations

WS-Trust

WS-Privacy

WS-PolicyFramework

WS-Privacy

WS-Policy

WS-Security

WS-Trust

WS-Federations

WS-Privacy

WS-Policy

WS-Security

WS-Federations

WS-Privacy

WS-Policy

WS-Security

WS-Federations

WS-Privacy

WS-Policy

WS-Security

WS-Federations

WS-Privacy

WS-Policy

WS-Security

WS-Federations

WS-Privacy

WS-Policy

WS-Security

WS-Federations

WS-Privacy

WS-Policy

WS-Security

WS-Federations

WS-Privacy

WS-Policy

WS-Security

WS-Federations

WS-Privacy

WS-Policy

WS-Security

WS-Federations

WS-Privacy

WS-Policy

WS-Security

WS-Federations

WS-Privacy

WS-Policy

WS-Security

WS-Federations

WS-Privacy

WS-Policy

WS-Security

WS-Federations

WS-Privacy

WS-Policy

WS-Security

WS-Federations

WS-Privacy

WS-Policy

WS-Security

WS-Federations

WS-Privacy

WS-Policy

WS-Security

WS-Federations

WS-Privacy

WS-Policy

WS-Security

WS-Federations

WS-Privacy

WS-Policy

WS-Security

WS-Federations

WS-Privacy

WS-Policy

WS-Security

WS-Federations

WS-Privacy

WS-Policy

WS-Security

WS-Federations

WS-Privacy

WS-Policy

WS-Security

WS-Federations

WS-Privacy

WS-Policy

WS-Security

WS-Federations

WS-Privacy

WS-Policy

WS-Security

WS-Federations

WS-Privacy

WS-Policy

WS-Security

WS-Federations

WS-Privacy

WS-Policy

WS-Security

WS-Federations

WS-Privacy

WS-Policy

WS-Security

WS-Federations

WS-Privacy

WS-Policy

WS-Security

WS-Federations

WS-Privacy

WS-Policy

WS-Security

WS-Federations

WS-Privacy

WS-Policy

WS-Security

WS-Federations

WS-Privacy

WS-Policy

WS-Security

WS-Federations

WS-Privacy

WS-Policy

WS-Security

WS-Federations

WS-Privacy

WS-Policy

WS-Security

WS-Federations

WS-Privacy

WS-Policy

WS-Security

WS-Federations

WS-Privacy

WS-Policy

WS-Security

WS-Federations

WS-Privacy

WS-Policy

WS-Security

WS-Federations

WS-Privacy

WS-Policy

WS-Security

WS-Federations

WS-Privacy

WS-Policy

WS-Security

WS-Federations

WS-Privacy

WS-Policy

WS-Security

WS-Federations

WS-Privacy

WS-Policy

WS-Security

WS-Federations

WS-Privacy

WS-Policy

WS-Security

WS-Federations

WS-Privacy

WS-Policy

WS-Security

WS-Federations

WS-Privacy

WS-Policy

WS-Security

WS-Federations

WS-Privacy

WS-Policy

WS-Security

WS-Federations

WS-Privacy

WS-Policy

WS-Security

WS-Federations

WS-Privacy

WS-Policy

WS-Security

WS-Federations

WS-Privacy

WS-Policy

WS-Security

WS-Federations

WS-Privacy

WS-Policy

WS-Security

WS-Federations

WS-Privacy

WS-Policy

WS-Security

WS-Federations

WS-Privacy

WS-Policy

WS-Security

WS-Federations

WS-Privacy

WS-Policy

WS-Security

WS-Federations

WS-Privacy

WS-Policy

WS-Security

WS-Federations

WS-Privacy

WS-Policy

WS-Security

WS-Federations

WS-Privacy

WS-Policy

WS-Security

WS-Federations

WS-Privacy

WS-Policy

WS-Security

WS-Federations

WS-Privacy

WS-Policy

WS-Security

WS-Federations

WS-Privacy

WS-Policy

WS-Security

WS-Federations

WS-Privacy

WS-Policy

WS-Security

WS-Federations

WS-Privacy

WS-Policy

WS-Security

WS-Federations

WS-Privacy

WS-Policy

WS-Security

WS-Federations

WS-Privacy

WS-Policy

WS-Security

WS-Federations

WS-Privacy

WS-Policy

WS-Security

WS-Federations

WS-Privacy

WS-Policy

WS-Security

WS-Federations

WS-Privacy

WS-Policy

WS-Security

WS-Federations

WS-Privacy

WS-Policy

WS-Security

WS-Federations

WS-Privacy

WS-Policy

WS-Security

WS-Federations

WS-Privacy

WS-Policy

WS-Security

WS-Federations

WS-Privacy

WS-Policy

WS-Security

WS-Federations

WS-Privacy

WS-Policy

WS-Security

WS-Federations

WS-Privacy

WS-Policy
Application lifecycle and security policies

- Corporate policies and line of business/domain specific policies
- Relevance to business process and business applications
- Platform specific models
- Impact on IT infrastructure
- Compliance and monitoring
Business driven application security

Security policy officer
Security auditor
Business analyst

Model security requirements and application security

Define business and corporate security policies

Model security requirements and application security

Security architects
Application architects

Develop Iteratively
Focus on Architecture
Continuously Ensure Quality
Manage Change & Assets

Application programmer
Security developer

Declare application security policies;
Build and test secure applications
Business application policies

- Analyzing relevance to business processes and applications

- Translating intent/goals into enforceable policies

- Business vocabulary vs. implementation
Application modeling and security policies
Programming model:
Infrastructure vs. application managed

- Infrastructure managed (gateways, application container)
  - Let application concentrate on business logic
  - Let the infrastructure enforce the intended policies
  - Policies aligned with business goals and deployment patterns
  - Policies may come from
    - application artifacts (e.g., deployment descriptors),
    - system configuration (e.g., based on topology), and
    - published policies (based on target interactions e.g. ws-policy)

- Application managed
  - Architected and standardized call-outs
  - Abstract out as a security provider (e.g., JAAS, JACC)
Deployment and management

Corporate, IT policies, etc (e.g., use corporate LDAP)

Application policy (e.g., in deployment descriptors)

Solution Install

Consumer administrator

Consumer

Requestor (consumer)

Service Provider

Subscribe

Subscription time changes (e.g., High level security, Fabrikam as certificate authority)

ERP

Travel app

Managing Security

Transform, persist and distribute policies to security provider (e.g., Security XACML policies and coordinates with Tivoli AccessManager)

Administer policies

Initial policies are pushed or stored; updates are pushed or pulled

XACML policy docs

Security Policy Manager

e.g. Tivoli AccessManager

Manage/Administer & Runtime

Application Server runtime

Runtime Publication of Policies (e.g., WS-Policy)

(e.g., 128 bit SSL required, X.509 certs from Verisign)
Identity Management & Service Oriented Architecture

Identity Management Market “Identity”

Identity transformation from a product-centric view to a service-centric view – move to adoption of service-oriented architectures with federation characteristics for simplifying identity management and strengthening corporate compliance.
Identity Integration Problem

How to share information with trusted providers?

- Partners using WS-Federation
- Partners using Liberty
- Partners using SAML in their Portal or Web
- Partners using WS-Security

Identity Management as a business process for cross-enterprise collaboration
Identity & Web Services - Landscape

- Industry leveraging Federation to “simplify” Service Delivery and provide superior end user experience

- New Service Enablers are driving need for identity sharing based on Web services
  - Presence, Location, Group Management etc

- HTTP Centric Services still a dominant delivery model
  - i.e. Services are Built and Delivered using normal HTTP to browser-based clients
  - E.g. Location-based Services, Third-Party Content
  - Enables Mobile Operator to assume the role of “Trusted Identity Provider/Authority” in mediating value-add data services with third-parties
  - HTTP Identity Services Standards in Mobile Industry
    - Current Deployments happening with Liberty ID FF 1.1/1.2
    - Role of SAML 1.0/1.1 very minimal in mobile industry (due to Liberty uptake)
    - SAML 2.0 will converge Liberty ID FF 1.1/1.2 and SAML 1.0/1.1 but adoption of SAML 2.0 not likely until 2006
    - WS-Federation becomes a critical strategy for integration with Microsoft Active Directory and Microsoft .NET Services

- Federation of Web Services is a dominant theme in “Service Oriented Architecture”
  - i.e. Services are discovered using Web Services (WSDL)
  - Dominant Web Services Security Platform is WS-Security
  - WS-Security now an official OASIS standard and implementations available from leading middleware platforms from Microsoft .NET and IBM
Best Practice – Enterprise User Provisioning

Self-Care

Password Sync/Reset
Workflow
Delegated Admin
Account Provisioning

Identity Management

Legacy
ERP
Portal
Directory

Enterprise Identity Foundation

Bi-directional Provisioning

HR Feed

Authoritative Feeds

DAML/DSML

Legacy
ERP
Portal
LDAP

Self-Care

Anthony Nadalin — SOA Security Programming Model
Best Practices – Access Management

Federated Access

Third-Party Access

Partner
Third Party

Partners using Microsoft®

Partners using SAML

Partners using Liberty

WS-Security/WS-Federation/SAML/Liberty

Direct Access

User

Federated ID

Web Access / Web SSO

Web SSO

Web SSO

Benefits Service

Billing Service

Portal Service

Micro SSO/Authentication/Authorization

Partners using Liberty

Partners using SAML

Partners using Liberty
Deployment Patterns & Roles – Federated Web Services

Patterns

- C2B / E2B HTTP
- C2B – Web Services
- B2B – Web Services
- Composite Patterns – C2B + B2B

Roles

- Identity Provider, Service Provider
- Web Services Client, WS Provider
- Web Services Client, WS Provider
- Identity Provider; WS Client, Service Provider; WS Provider

Consumer-2-Business (C2B)
Employee-2-Business (E2B)
Business-to-Business (B2B, e.g. Portal to Portal)
C2B2B - Portal to Portal – Deployment

Third-party User

PORTAL (Identity Provider)

XML/Web Services Gateway

Security Token

SOAP Request
WS-Security

Service Provider/WSP

Web Services Provider

Web Services Client

Third Party

local ID

WS-Trust

Token

Token

local ID

WS-Trust

Enterprise Directory

Identity Service

Security Service

Policy Service

Enterprise Directory

Identity Service

Security Service

Policy Service

Anthony Nadalin — SOA Security Programming Model
Identity + Web Services - Architecture

Clients
Browser
Rich Client
Mobile Terminal

Federated Identity Provider (Liberty)

SAML

WS-Federation

Federated Identity Provider (SAML)

Enterprise ID Gateway

Identity Services

Security Services

SAML

WS-Trust/WS-Security

WS-Security

Partner Spokes

Enterprise Web Services Platforms

I “know” this subscriber from my partner company

I “know” how to connect the “user” to authorized services
Compliance – Auditing the Integrity of Mortgage Approval Business Process

Personas involved:
Customer, Branch Officers, Call Center Reps, Loan Approvers, Loan Providers, Loan Officers, Credit Exception Processors

End-to-End View is Needed to demonstrate integrity
Integrated Audit Trail: Identity, Access, Change
SIMPLE IDENTITY & CHANGE AUDIT FOR CONTINUOUS COMPLIANCE

INPUT

Audit Process

Business Services

XML Policy

CCMDB/Warehouse

Processes/WBI

Identity, Access (Company & Partner)

XML Security Policy

TIM/TAM, FM/SCM

ERP/CRM

Database

Change Events/Alerts

Security Events/Alerts

CEI, CBE

CEI, CBE

OUTPUT

CARS

Central Audit Service

Compliance Data (Security, Change, Archive)

SQL

Analytics/Correlation Engine

Abnormal Events/Alerts

Change & Remediation Process

DB2 AlphaBlox

Workplace for BCR (Communicate, Track)

Events/State Changes

CEI, CBE

Dashboard Business & IT Reports

TPM, TCM, TIM, TAM, FIM

Network Remediation

Rational Requisite Pro

SOX

Basel II

Visa CISP

EU/Japan Privacy Law

Corporate Security Policies

US Patriot Act

Compliance Drivers

Anthony Nadalin — SOA Security Programming Model
Summary

- Security is about business, no longer just about technology
- SOA enables better Application Integration
- Web Services Security standards optimizes the development, deployment and management of Composite Applications
- Federation is the “bridge” by which web services security integrates with Service Oriented Architectures