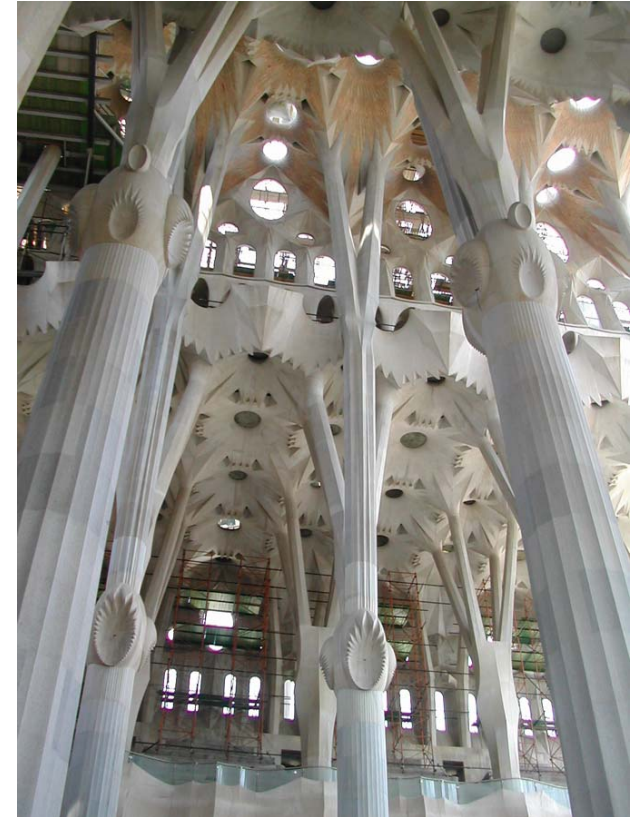


THE LEADER IN WEB SERVICES & SOA SECURITY

Foundations of Secure Web Services

Starting with Identity Management

Sagrada Familia – Antonio Gaudi



- Started in 1883 – Work In Progress
- Only 60% complete
- Work accelerated with new materials
- Work accelerated by visitors
- Well thought out architecture, even after 1936 fire destroyed 25% of drawings

Agenda

- Foundations of secure Web Services
 - I. Start with Web Services Identity Management
 - II. Establish Web Services Trust
 - III. Counter Web Services Threat
 - IV. Enforce Web Services Interoperability
 - V. Test Web Services Thoroughly
- Components of Web Services-based SOA
- Best Practices

Foundations of secure Web Services

Trust Management

- Message Integrity – Sign & Verify
- Message Privacy – Encrypt & Decrypt

Threat Management

- Filter all SOAP/XML for Threats/Information Leak
- Attack Prevention – Denial of Service

Identity Management

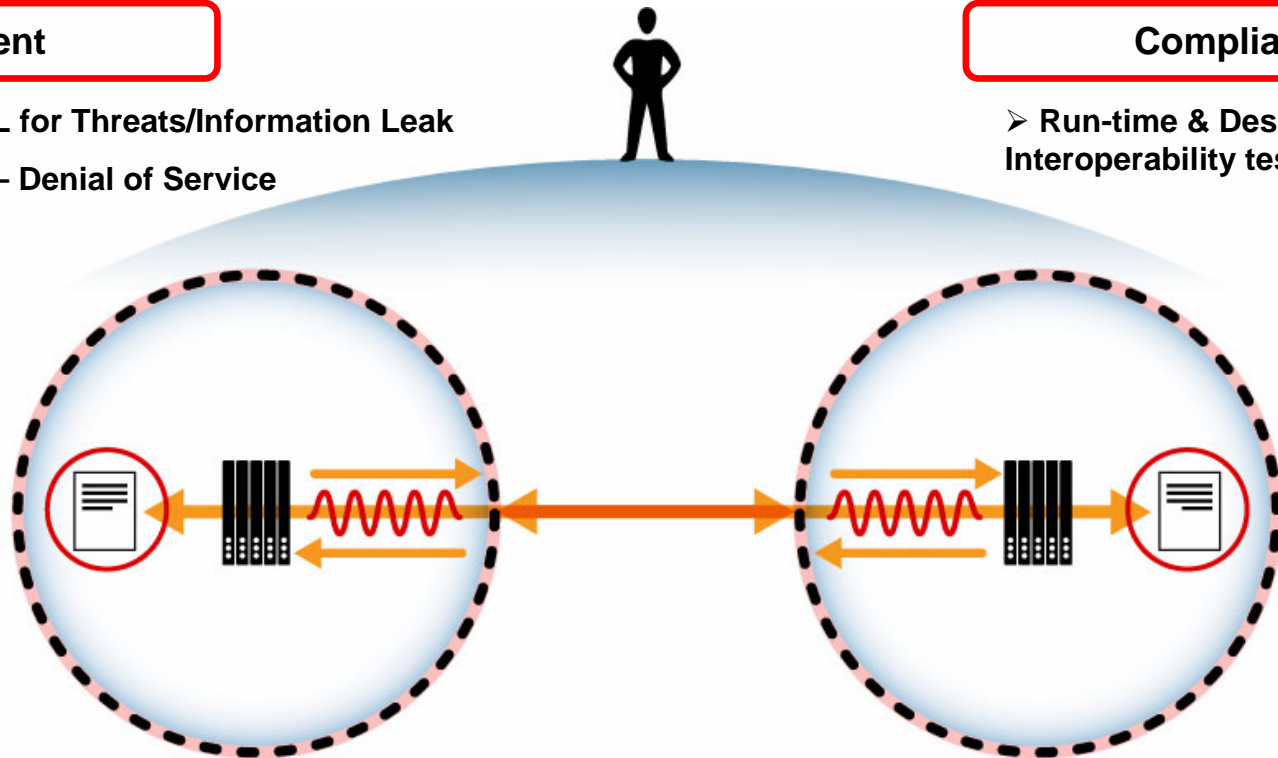
- Leverage existing SSO Infrastructure
- WS Authentication & Access Control
- Identity Bridging

Diagnostics

- Pre-production & Post-production Testing
- Functional, Performance, Interop, Vulnerability

Compliance

- Run-time & Design-time Interoperability testing

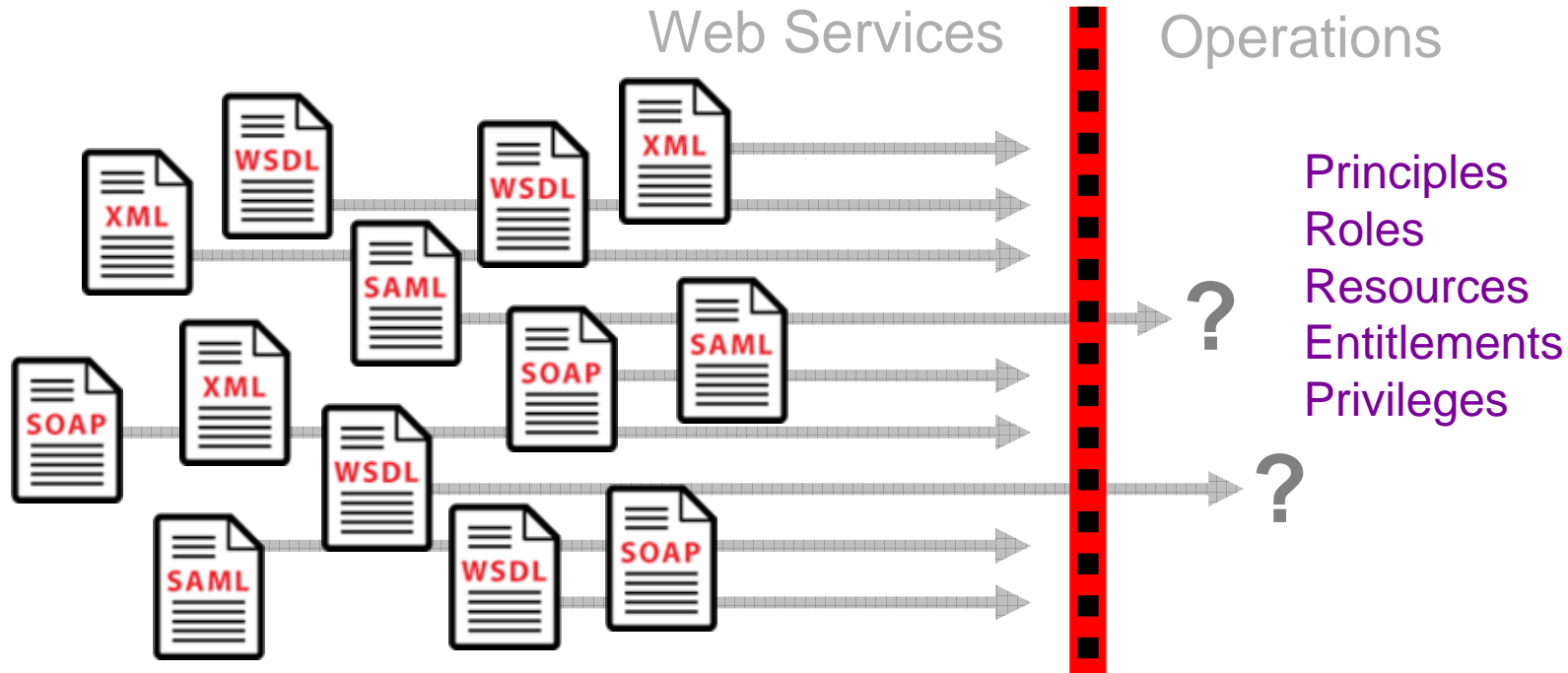


I. Start with Web Services Identity Management

- Leverage existing SSO Infrastructure
- Web Services Authentication & Access Control (Provision + Execute)
- Identity Bridging

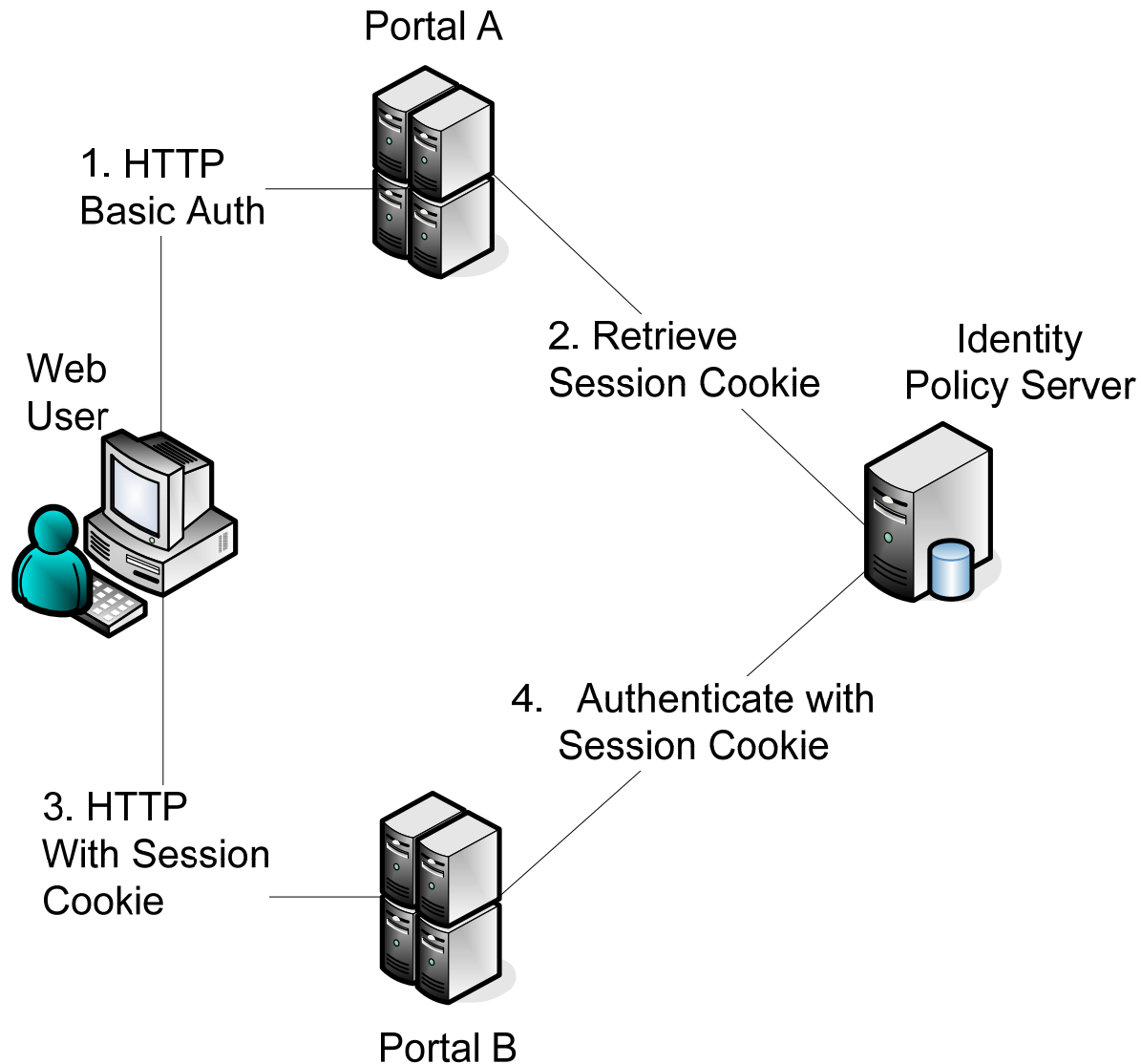
Why Identity-Driven SOA's?

Knock, Knock. Who's There?

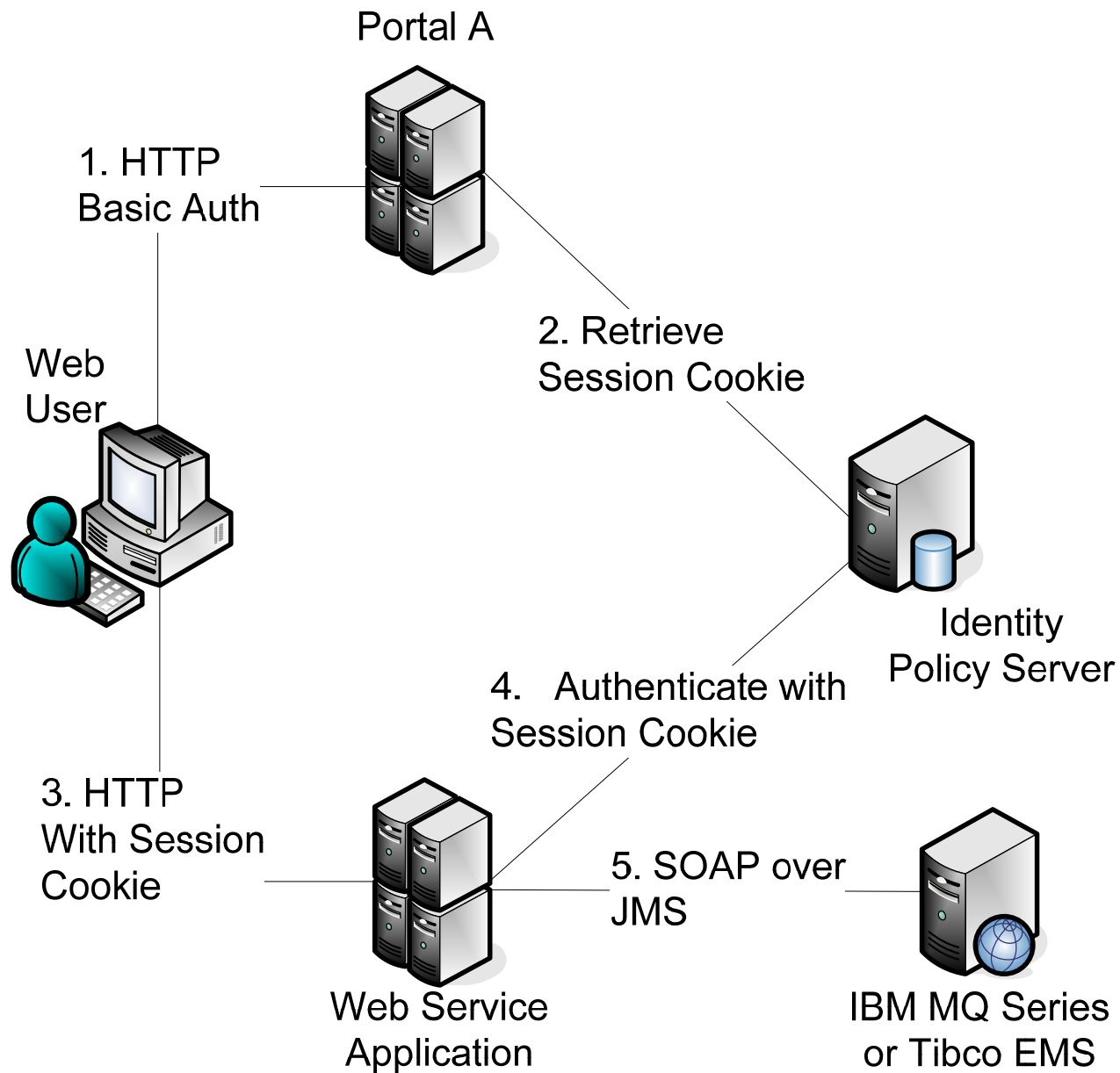


1. What business functions can be accessed; by whom?
2. How do you model complex business process trust relationships?
3. How do you uniformly enforce security policies?
4. How do you mitigate the risks of incorrect authorizations?

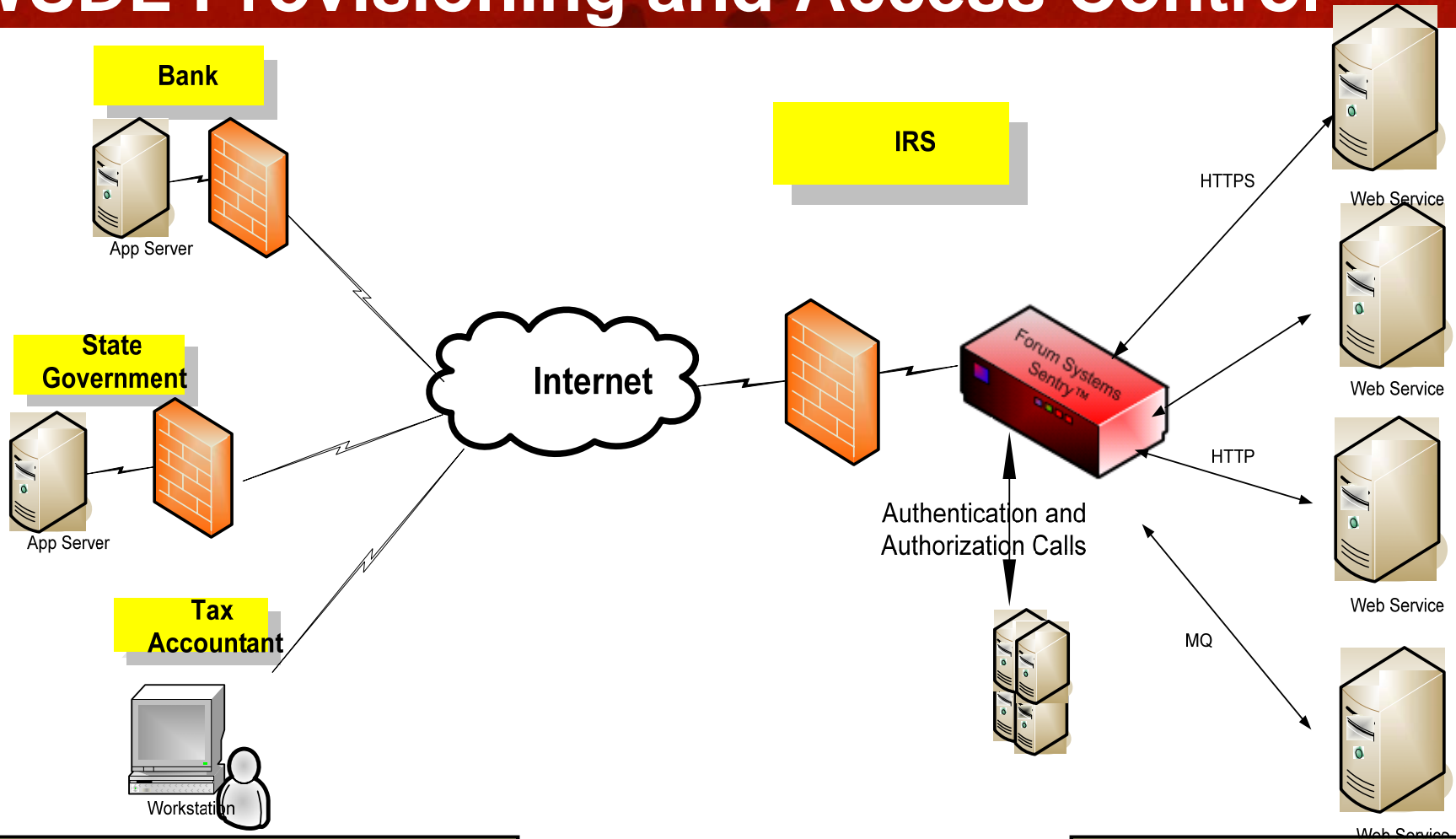
Typical SSO Identity Use



Extending SSO Identity Systems to SOA



WSDL Provisioning and Access Control

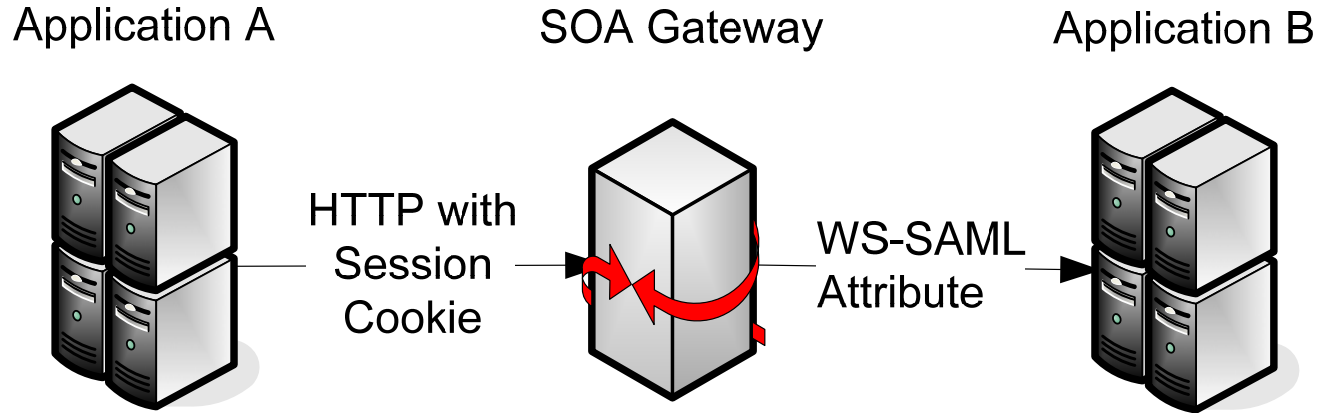


Web Service client retrieves a dynamically generated WSDL file from Sentry.
Web Service generates a request and sends it to Sentry

Sentry authenticates
Sentry Authorizes
passes the request to the appropriate Web Service.

Web Service processes the request and generates a response sent back to the user through Sentry

Identity Bridging



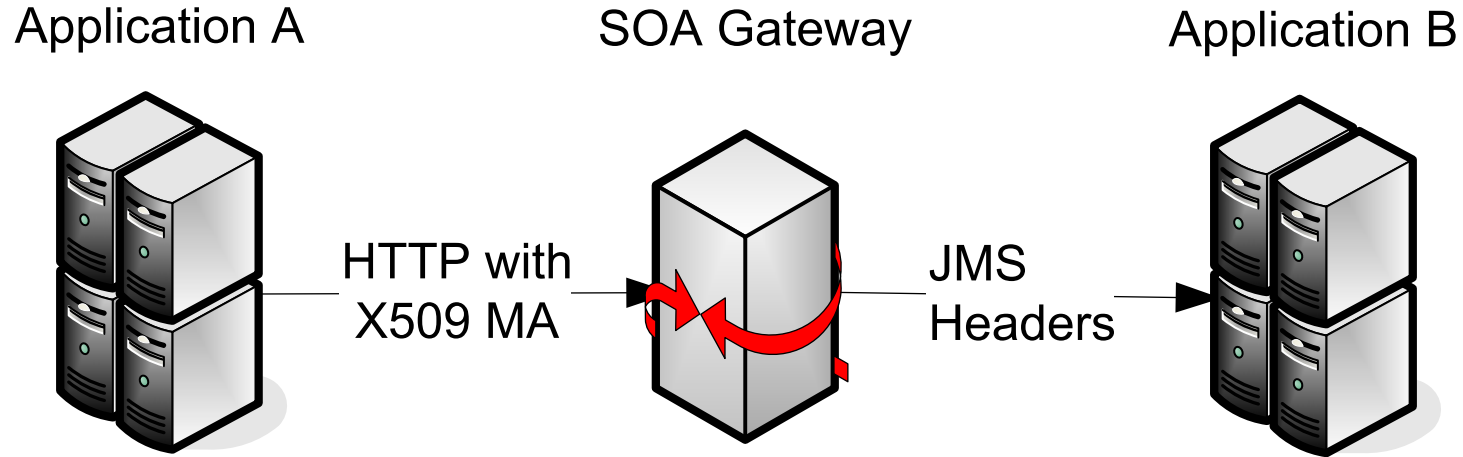
1. Inbound Protocol Auth
 - HTTPS Termination – BA or MA
2. Inbound Message Auth
 - A. WS-Security User Name Token
 - B. WS-Security X509 Token
 - C. WS-Security SAML Assertion
 - D. WS-Security Kerberos

1. Outbound Protocol Auth
 - HTTPS Initiation – BA or MA
2. Outbound Message Auth
 - A. WS-Security User Name Token
 - B. WS-Security X509 Token
 - C. WS-Security SAML Assertion

II. Establish Web Services Trust

- **Message Integrity – Sign & Verify**
- **Message Privacy – Encrypt & Decrypt**

Establish Trust



1. **Encrypt SOAP based on Application A X509 or Gateway X509**
2. **Sign with SOA Gateway Private Key**
3. **Stuff JMS Headers using XPath**
4. **Protocol Bridging is common**
5. **Response Processing is as important as Request Processing**

THE LEADER IN WEB SERVICES & SOA SECURITY

III. Counter Web Services Threat

Sample SOA Threats

- I. Existing Vulnerabilities - New Attack Vector
 - SwA - with Malicious Attachments
 - SQL Injection

- II. New Vulnerabilities
 - Large Buffer Attack
 - Coercive Parsing
 - Parameter Tampering
 - Recursive Payloads

Threat: Malware in SOAP with Attachments

```
MIME-Version: 1.0
Content-Type: Multipart/Related; boundary="-----_MIME_boundary";
type="text/xml"; start="<SwAStart@maliciouspartner.com>"
Content-Description:

-----_MIME_boundary
Content-Type: text/xml; charset=UTF-8
Content-Transfer-Encoding: 8bit
Content-ID: <SwAStart@maliciouspartner.com>
Content-Location: Echo.xml

<?xml version="1.0" encoding="utf-8"?>
<soap:Envelope xmlns:soap="http://schemas.xmlsoap.org/soap/envelope/"
xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance"
xmlns:xsd="http://www.w3.org/2001/XMLSchema" xmlns:s0="http://qa.forumsys.com/ws">
  <soap:Body>
    <s0:Echo>
      <s0:Buf></s0:Buf>
    </s0:Echo>
  </soap:Body>
</soap:Envelope>

-----_MIME_boundary
Content-Type: application/octet-stream
Content-Transfer-Encoding: base64
Content-ID: <Trojan.scr@maliciouspartner.com>
Content-Location: Trojan.scr

VmlzdWFsIEJhc2ljIFZpcnVzIEZpbGUuICBTYW1wbGUgTWVzc2FnZSsgbW90IGFuIGFjdHVhbCB2
aXJ1cy4NC1Zpc3VhbCVCYXNpYyBwaXJ1cyBGaWxlLiAgU2FtcGx1IE1lc3NhZ2UsIG5vdCBhbiBh
Y3R1YWwgdmlydXMudQpWaxN1YWwgQmFzaWNgVmlldXMgRmlsZS4gIFNhbXBzZSBnZXNzYWdlLlCBu
b3QgYW4gYWN0dWFsIHZpcnVzLgOKVmlzdWFsIEJhc2ljIFZpcnVzIEZpbGUuICBTYW1wbGUgTWVz
c2FnZSsgbW90IGFuIGFjdHVhbCB2aXJ1cy4NC1Zpc3VhbCVCYXNpYyBwaXJ1cyBGaWxlLiAgU2Ft
cGx1IE1lc3NhZ2UsIG5vdCBhbiBhY3R1YWwgdmlydXMudQpWaxN1YWwgQmFzaWNgVmlldXMgRmls
ZS4gIFNhbXBzZSBnZXNzYWdlLlCBub3QgYW4gYWN0dWFsIHZpcnVzLgOKVmlzdWFsIEJhc2ljIFZp
cnVzIEZpbGUuICBTYW1wbGUgTWVzc2FnZSsgbW90IGFuIGFjdHVhbCB2aXJ1cy4NCg==

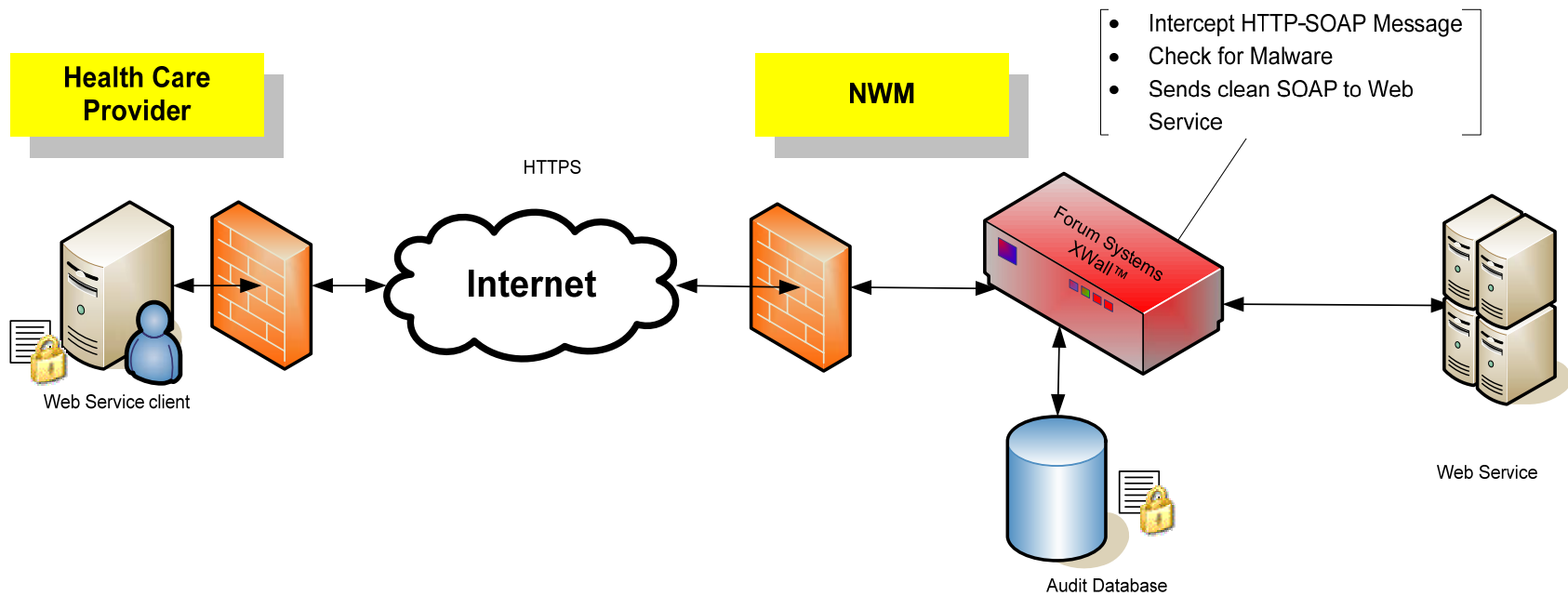
-----_MIME_boundary--
```

HTTP Header

SOAP Message

Malicious Attachment

Threat: Malware



Trading Partner sends Purchase Order as SwA

XWall checks for Malware

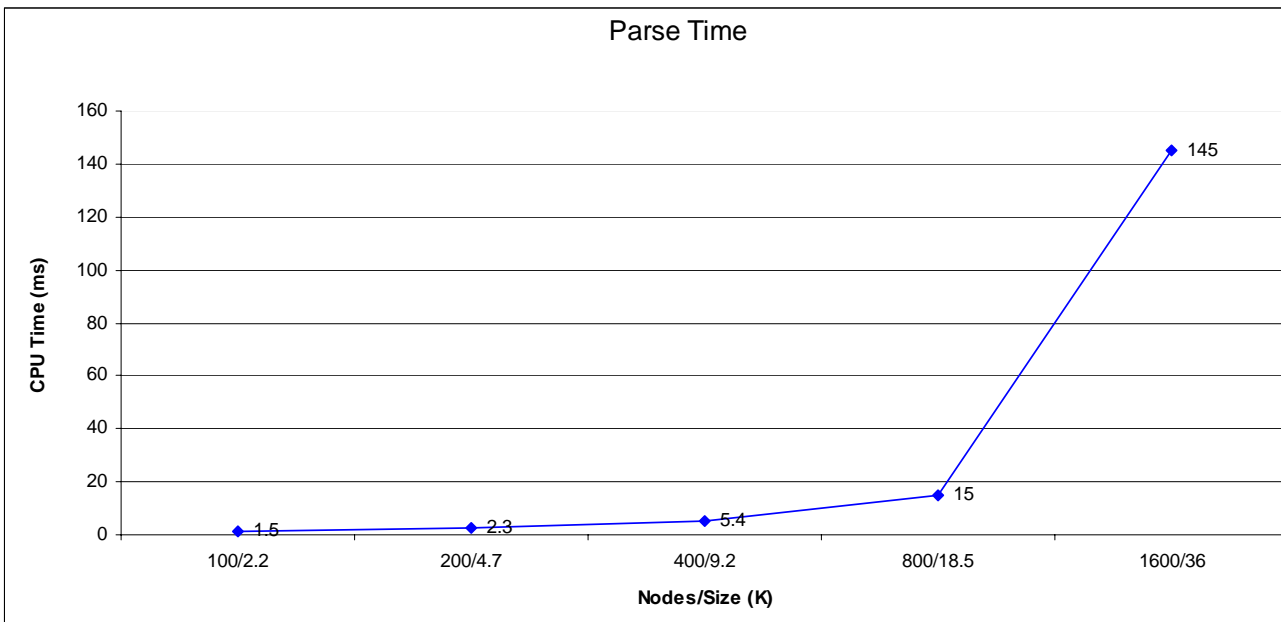
Clean PO sent to Web Service

Threat: Countermeasures

1. Anti-virus scanning for all SwA entering the enterprise
 - Required Protocol Mixing can cause Virus to spread rapidly
 - HTTP – SMTP
 - HTTP – JMS (MQ, Tibco)
2. Need to Decrypt before scan – Onboard Integration
 - SSL termination required
 - SwA Decryption required
3. Block Offending client IP addresses and users
 - Setup alerts for notifying administrator
 - Automatically THROTTLE/BLOCK SOAP traffic from IP addresses and/or users
 - Quarantine Malicious Messages

Threats: Recursive Payload Attack

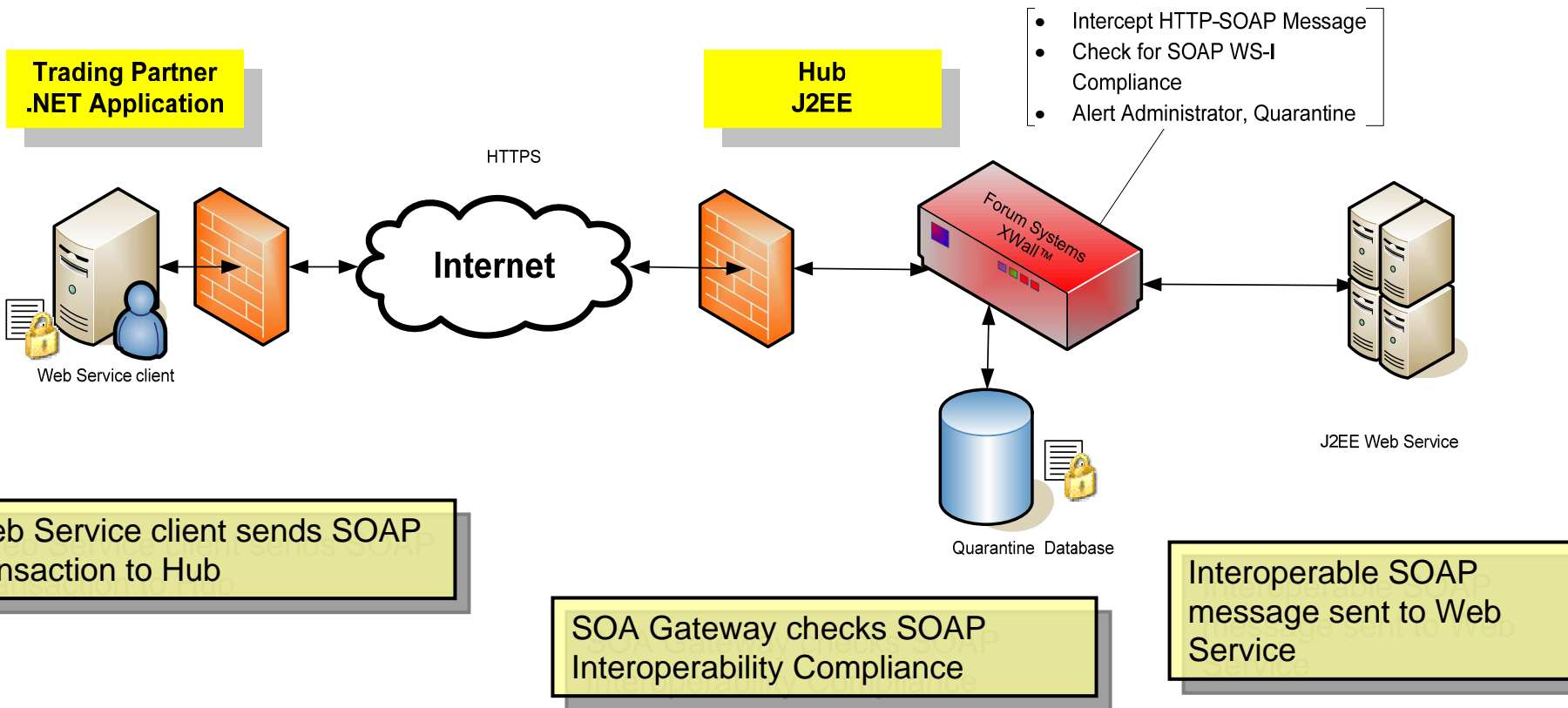
```
1 <?xml version="1.0" encoding="utf-8"?>
2 <soap:Envelope xmlns:soap="http://schemas.xmlsoap.org/soap/enve
3   <soap:Body>
4     <BuildNestedXMLResponse xmlns="http://qa.forumsys.com/ws">
5       <BuildNestedXMLResult>
6         <XML_1>
7           <XML_2>
8             <XML_3>
9               <XML_4 />
10            </XML_3>
11           </XML_2>
12          </XML_1>
13        </BuildNestedXMLResult>
14      </BuildNestedXMLResponse>
15    </soap:Body>
16  </soap:Envelope>
```



THE LEADER IN WEB SERVICES & SOA SECURITY

IV. Enforce Web Services Interoperability

Interoperability: WS-I BP 1.1



- Interoperability Compliance Requires
 - Design Time WSDL Compliance Checks
 - Run Time Test

THE LEADER IN WEB SERVICES & SOA SECURITY

V. Test Web Services Thoroughly

Pillars of SOA Testing

I. Functional Testing

- Regression → Operation Chaining
- Security → WS-Signatures, Encryption
- Identity → SAML, Kerberos, Username token, X509

II. Performance & Scalability Testing

- Concurrent Connections/Transactions
- TPS & Throughput

III. Interoperability Compliance

- Runtime & Design Time
- WS-I BP 1.1 & WS-I BSP 1.0

IV. Vulnerability Assessment

- Schema character: reckless vs. guarded
- Information leak
- Denial of Services Attacks

THE LEADER IN WEB SERVICES & SOA SECURITY

SOA Components

Typical SOA Components

- Identity Management
- SOA Gateway
- Management & Monitoring
- Registry
 - Web Services Lookup
- Diagnostics
 - Pre-production
 - Post-production
- Orchestration
- Existing Components
 - Databases
 - Application Servers
 - ESBs

SOA Component Vendors

Identity Management

RSA Clear Trust

IBM Tivoli

Oracle Core ID

CA SiteMinder

Orchestration

ActiveEndpoints

Oracle BPEL

Management & Monitoring

AmberPoint

HP SOA Manager

Oracle WSM

CA WSDM

SOA Gateway

Forum Systems

IBM/DP

Reactivity

Layer7

Diagnostics

Crosscheck Networks

Parasoft

Registry

Mercury/Systinet

SOA Software

Infravio

THE LEADER IN WEB SERVICES & SOA SECURITY

Best Practices for building a secure SOA

SOA Best Practices

- Identity Management
 - Start from Simple HTTP Basic Auth
 - Move to X509 MA
 - Consider Message-based Identities
 - Prepare for Identity Bridging
 - Tie-in with existing Identity Management
 - Don't stop at Authentication → Authorize operations
- Encryption & Signatures
 - SSL is good for point-to-point
 - Consider WS-Encryption
 - Have default out-bound encryption rules
 - Sign all out-bout SOAP/XML Messages - archive
- Monitoring
 - Avoid yet another proxy
 - SLA is not easy – plan ahead
- Registry
 - Must have for SOA
 - Part of WSDL life-cycle
 - Usually deployed later in the game
- Diagnostics
 - Test early, test often
 - Pre-production, Post-production
 - Look at all aspects of Diagnostics
- Orchestration
 - Challenging ESBs
 - BPEL is just a part of the solution

Sagrada Familia – Antonio Gaudi



- Started in 1883 – Work In Progress → SOA is a process not an event
- Only 60% complete → SOA is never complete
- Work accelerated with new materials → New standards accelerated SOA
- Work accelerated by visitors → Users help fund SOA
- Well thought out architecture, even after 1936 fire destroyed 25% of drawings → A well thought out SOA has resilience

THE LEADER IN WEB SERVICES & SOA SECURITY

Questions?