Web Services Security Standards

Sang Shin
Michèle Garoche
www.javapassion.com
"Learning is fun!"

Agenda

- Web services security requirements
- Web services & SOA security standards
  - XML signature, XML encryption
  - SAML
  - WS-Security

Web Services Security Requirements

Web Services Security Requirements

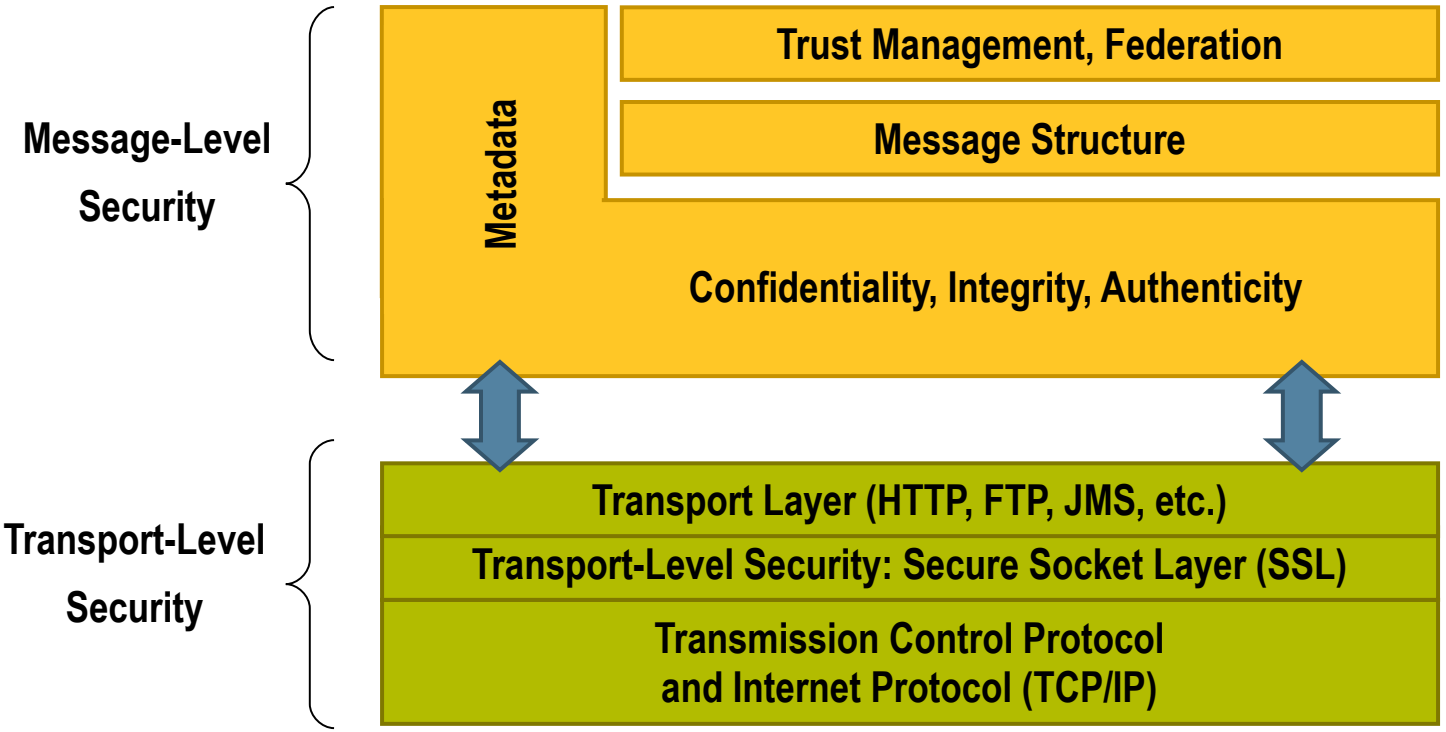
- Access to resources and services over HTTP (mainly)
  - Readable messages (XML)—Message-level security required
- Declarative security
  - No hard-coded security
- Define security centrally
  - Policies are in a single point of control and administration
- Enforce security locally
  - Policy enforcement points are distributed across the environment
- Heterogeneous environments

Security Features Needed

- Authentication
- Authorization—Access Control
- Confidentiality
- Integrity
- Non-repudiation
- Credential mediation
  - Exchange security tokens in a trusted environment
- Service capabilities and constraints
  - Define what a service can do, under what circumstances

Web Services & SOA Security Standards

Key Industry-Standard Security Frameworks



JMS = Java Message Service

Message Level Web Services Security Standards

- XML Signature and XML Encryption
- WS-Security 1.0 and 1.1
- SAML

XML Signature, XML Encryption

Web Services & SOA Security Standards

XML Encryption, XML Signature

- XML Encryption (data confidentiality)
  - How digital content is encrypted and decrypted
  - How the encryption key information is passed to a recipient
  - How encrypted data is identified to facilitate decryption
- XML Signature (data integrity, authenticity)
  - Bind the sender's identity (or "signing entity") to an XML document
    - Signing/signature verification can be done using asymmetric or symmetric keys
  - Ensure non-repudiation of the signing entity
    - Proves that messages have not been altered since they were signed

SAML

Web Services & SOA Security Standards

What is SAML?

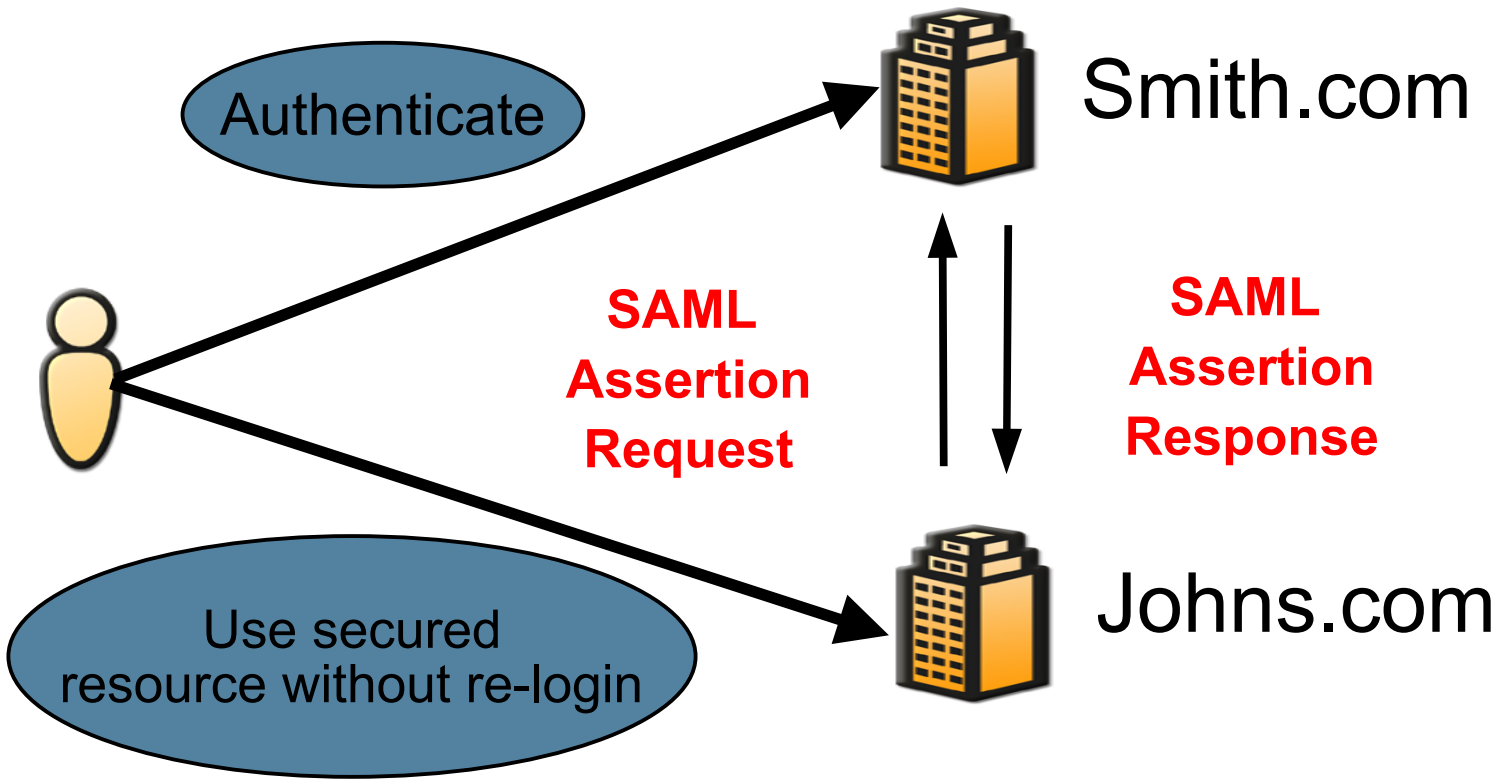
- Define an XML framework for exchanging authentication and authorization information
  - Various XML security assertions: credentials, authentication, attribute, authorization, etc...
  - Request & response protocol
- Enables Single Sign-On (SSO)
- OASIS Standard
- JSR-155

Use cases for sharing security information thru SAML

- SAML developed three “use cases” to drive its requirements and design:
  - Single sign-on (SSO)
  - Distributed transaction
  - Authorization service

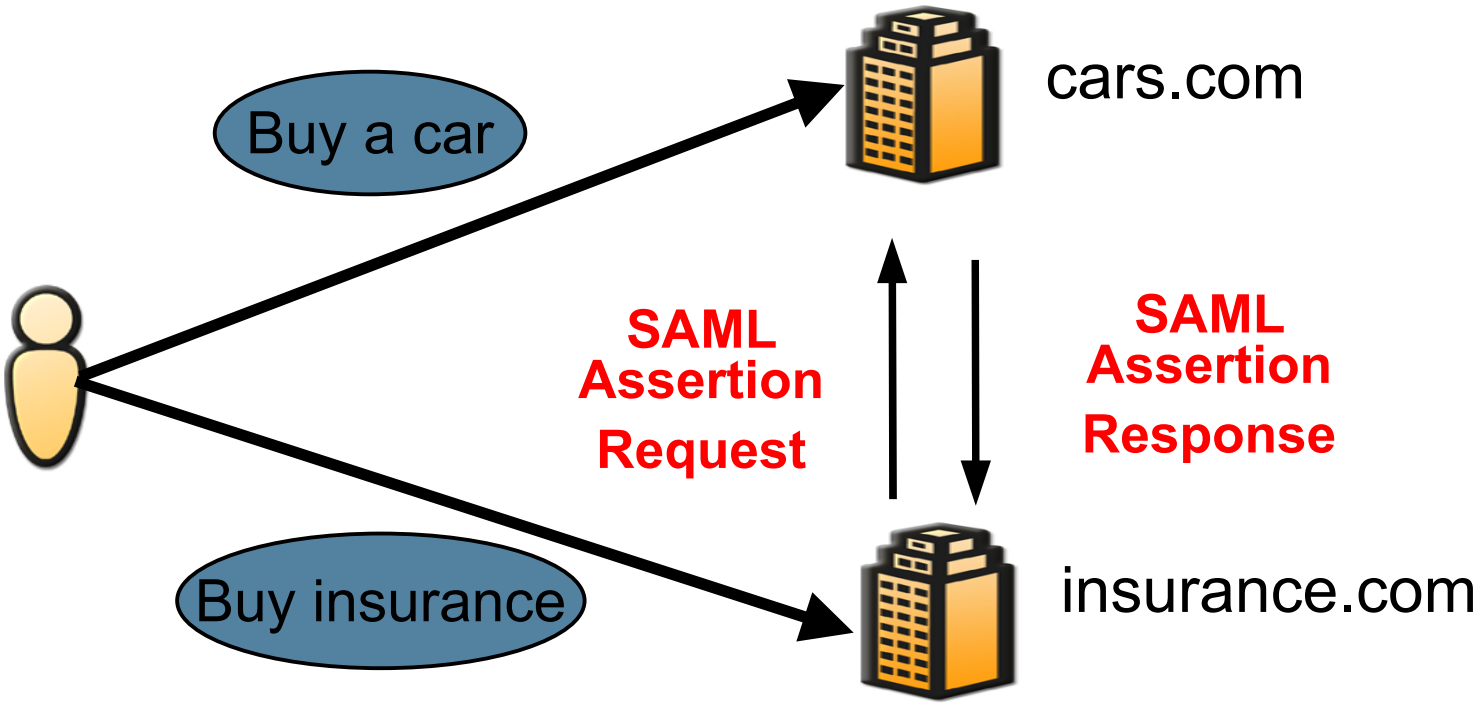
#1 Single Sign On (SSO)

- Logged-in (authenticated) users of Smith.com are allowed to access to sister site Johns.com without relogin



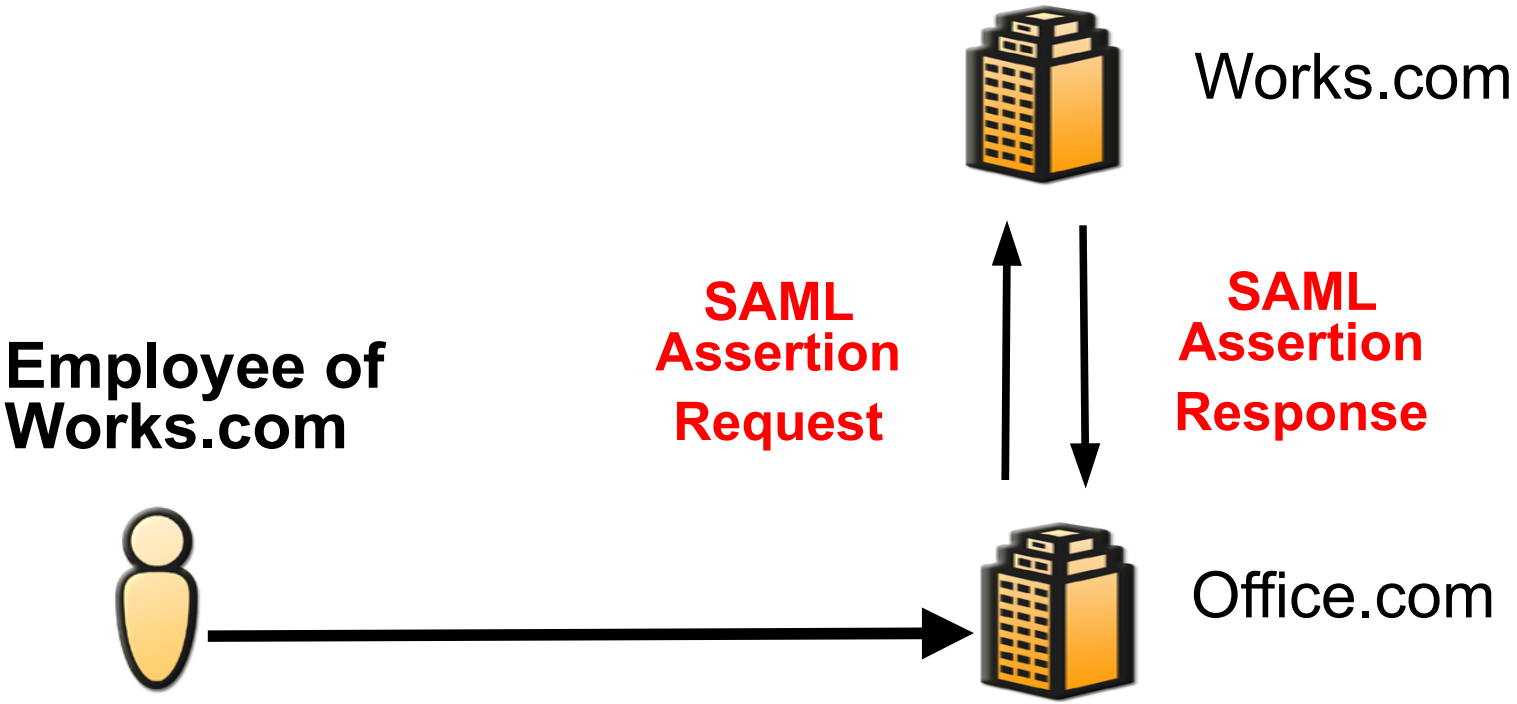
#2 Distributed Transaction

- A car buyer also purchases an auto insurance from insurance.com which is affiliated with cars.com



#3 Authorization Service

- An employee of Works.com orders office supplies directly from Office.com, which performs its own authorization



SAML in a nutshell

- It's an XML-based framework for exchanging security information
  - XML-encoded security "assertions"
  - XML-encoded request/response protocol
  - Rules on using assertions with standard transport and messaging frameworks

SAML Assertions

- Assertions are declarations of fact, according to someone
- SAML assertions are compounds of one or more of three kinds of "statement" about "subject" (human or program)
  - Authentication
  - Attribute
  - Authorization

Authentication statement

- An issuing authority asserts that
  - subject S was authenticated
  - by means M
  - at time T
- Targeted towards Single Sign On uses

Example assertion with authentication statement

```
<saml:Assertion …>
  <saml:AuthenticationStatement
    AuthenticationMethod="password"                    (By means M)
    AuthenticationInstant="2001-12-03T10:02:00Z">      (At time T)
    <saml:Subject>                                     (Subject S)
      <saml:NameIdentifier
        SecurityDomain="sun.com"
        Name="Sang" />
      <saml:ConfirmationMethod>
        http://…core-25/sender-vouches
      </saml:ConfirmationMethod>
    </saml:Subject>
  </saml:AuthenticationStatement>
 </saml:Assertion>
```

Attribute statement

- An issuing authority asserts that
  - Subject S is associated with
  - attributes A, B, … with values “a”, “b”, “c”…
- Useful for distributed transactions and authorization services

Example assertion with two attribute statements

```
<saml:Assertion …>
  <saml:AttributeStatement>
    <saml:Subject>..Sang..</saml:Subject>
    <saml:Attribute
      AttributeName="PaidStatus"                    (attribute A)
      AttributeNamespace="http://smithco.com">
      <saml:AttributeValue>                        (with value a)
        PaidUp
      </saml:AttributeValue>
    </saml:Attribute>
    <saml:Attribute
      AttributeName="CreditLimit"                   (attribute B)
      AttributeNamespace="http://smithco.com">
      <saml:AttributeValue>                        (with value b)
        <my:amount currency="USD">500.00
        </my:amount>
      </saml:AttributeValue>
    </saml:Attribute>
  </saml:AttributeStatement>
</saml:Assertion>
```

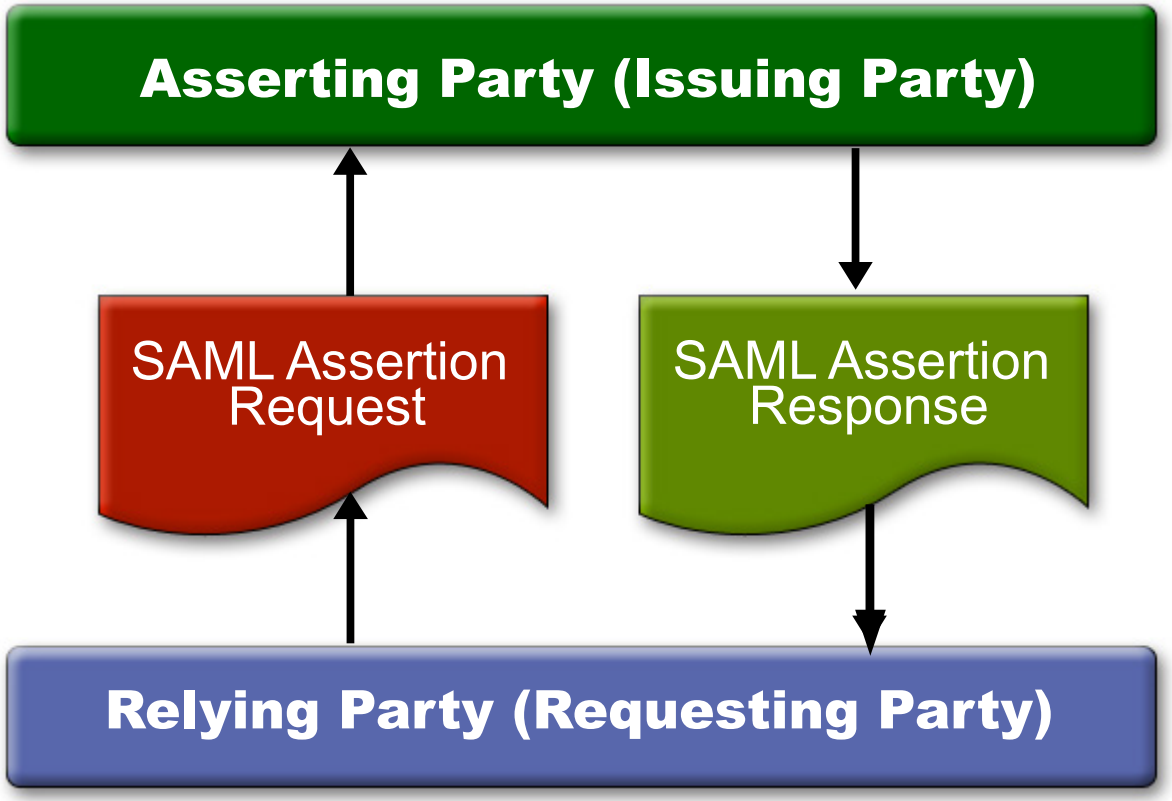
Authorization statement

- An issuing authority decides
  - whether to grant the request by subject S
  - for access type A to resource R
  - given evidence E
- The subject could be a human or a program
- The resource could be a web page or a web service, for example

Example assertion with authorization statement

```
<saml:Assertion …>
  <saml:AuthorizationStatement
    Decision="Permit"                          (Whether to grant request)
    Resource="http://jonesco.com/rpt_12345.html">(for res. R)
    <saml:Subject>…</saml:Subject>                          (by Subject S)
    <saml:Actions
      ActionNamespace="http://…core-25/rwedc">
      <saml:Action>Read</saml:Action>          (for access type A)
    </saml:Actions>
  </saml:AuthorizationStatement>
</saml:Assertion>
```

Protocol for Requesting & Receiving Assertions

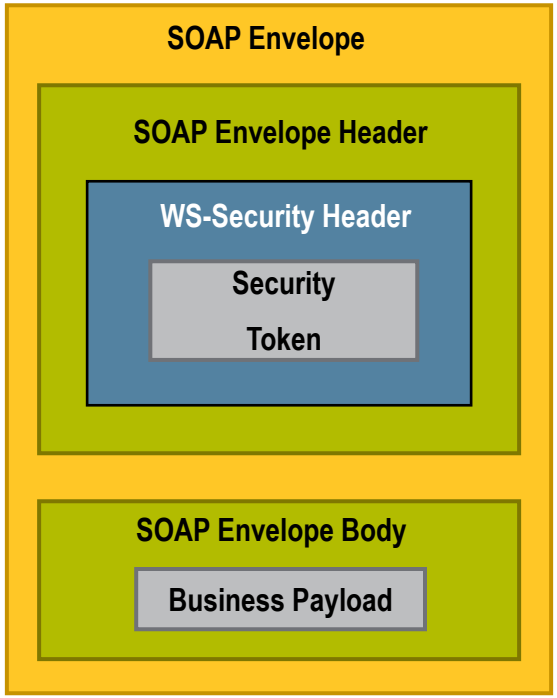


WS-Security

Web Services & SOA Security Standards

WS-Security

- WS-Security defines how to attach XML Signature and XML Encryption headers to SOAP messages
- WS-Security provides profiles for 5 security tokens
  - Username (with opt. pwd digest)
  - X.509 cert
  - Kerberos ticket
  - SAML assertion
  - REL (Rights Expression Language) document

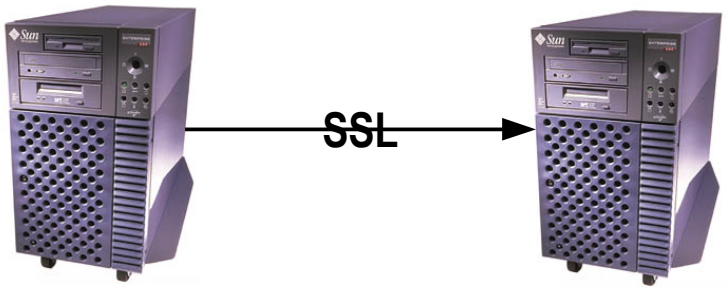


WS-Security With SAML Security Token

- SAML assertions and references to assertion identifiers are contained in the <*wsse:Security*> element, which in turn is included in the <*SOAP-ENV:Header*> element (described in the WS-Security SAML Token Profile)

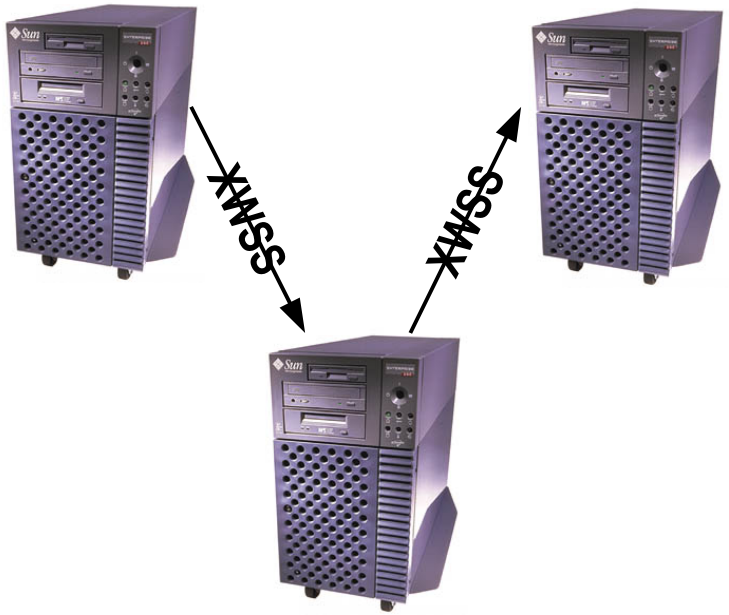
```
<SOAP-ENV:Envelope>
  <SOAP-ENV:Header>
    <wsse:Security>
      <saml:Assertion> - - - </saml:Assertion>
    </wsse:Security>
  </SOAP-ENV:Header>
  <SOAP-ENV:Body> - - - </SOAP-ENV:Body>
</SOAP-ENV:Envelope>
```

WS-Security: Before and After



Before WS-Security

- SSL/HTTPS
- Security at transport layer
- All or nothing granularity
- Point-to-point



WS-Security

- Security at SOAP message layer
- Fine granularity possible
  - Only sign/encrypt credit card # (e.g., XML subtree)
- Works on non-TCP/IP transports
- Integrity, Confidentiality, Authentication
- W3C XML Signature/Encryption

Thank you!

Sang Shin
Michèle Garoche
www.javapassion.com
"Learning is fun!"