



XML Security Gateway Evaluation Criteria Project Update

**6th OWASP
AppSec
Conference**
Milan - May 2007

**Gunnar Peterson, OWASP XSGEC Project
Lead**
Managing Principal, Arctec Group
gunnar@arctecgroup.net

Copyright © 2007 - The OWASP Foundation
Permission is granted to copy, distribute and/or modify this document under the
terms of the Creative Commons Attribution-ShareAlike 2.5 License. To view this
license, visit <http://creativecommons.org/licenses/by-sa/2.5/>

The OWASP Foundation
<http://www.owasp.org/>

About Arctec Group

- Best in class enterprise architecture consulting provider focused on enterprise, software, and security architecture
- Client list includes numerous global 500 companies, world's largest electronic financial exchanges, emerging startups and Dept. Homeland Security
- Headquarters: IDS Center, Minneapolis, MN; Clientele: global
- Web: www.arctecgroup.net



About the speaker

Gunnar Peterson

Managing Principal, Arctec Group

Editor Build Security In software security column for IEEE Security & Privacy Journal

(www.computer.org/security)

Primary and contributing author for DHS/CERT Build Security In portal on Web Services security, Identity, and Risk management (<https://buildsecurityin.us-cert.gov/daisy/bsi/home.html>)

Project lead: OWASP XML Security Gateway Evaluation Criteria Project

http://www.owasp.org/index.php/Category:OWASP_XML_Security_Gateway_Evaluation_Criteria_Project

Associate editor Information Security Bulletin (www.chi-publishing.com)

Contributor Web Application Firewall Evaluation Criteria

(<http://www.webappsec.org/projects/wafec/>)

Blog: (<http://1raindrop.typepad.com>)

Slides/presentations (<http://www.arctecgroup.net/articles.htm>)



OWASP XML Security Gateway Evaluation Criteria Project (XSGEC)

■ Goals:

- ▶ Defines an open standard for evaluating XML Security Gateways such as those used to protect and provide security services for Web services applications
- ▶ Add clarity to the process of assessing the XML Security Gateway strengths and weaknesses
- ▶ Enlighten the community as to the utility of XML Security Gateways to deliver security services for distributed systems.

■ Team: Mix of industry professionals, vendors, and consultants



XSGEC Guiding Principles

- Define evaluation criteria supporting a transparent, level playing field for XML Security Gateway solutions to define their solution's key value proposition
- Where practical, attempt to standardize nomenclature and metrics
- Educate the community on the design considerations for XML security



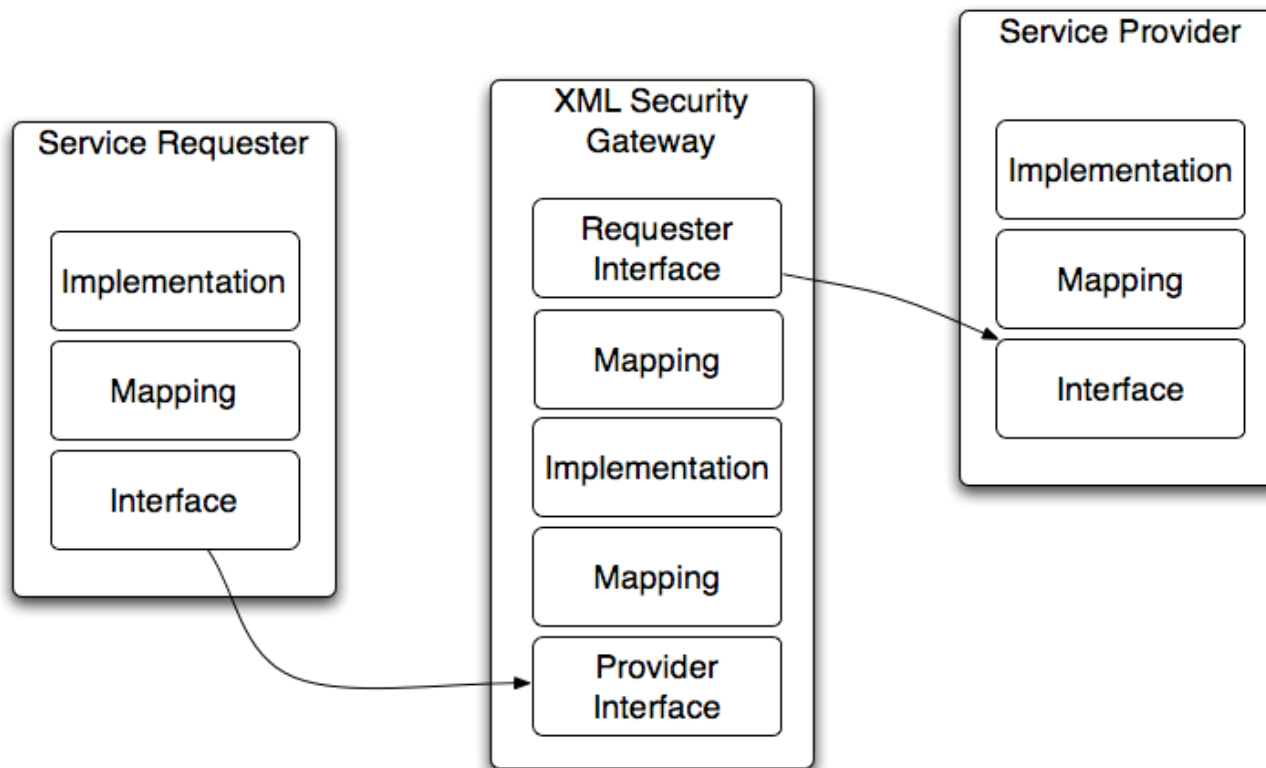
XML Security Gateway Pattern

- Context: The primary goal of Web services is to solve interoperability and integration problems. Web services traverse multiple technologies and runtimes.
- Problem: Web service requesters and providers do not agree upon binary runtimes like J2EE, instead they agree upon service contracts, message exchange patterns, and schema. Service and message level authentication, authorization, and auditing services for Web services are not delivered by a single container, rather these services must span technical and organizational boundaries



XML Security Gateway Pattern

- Solution: Use a XML Security Gateway to provide decentralized security services for Web services



SOAP in the clear

```
<soap:Envelope
xmlns:soap="http://schemas.xmlsoap.org/soap/envelope/">

  <soap:Body>

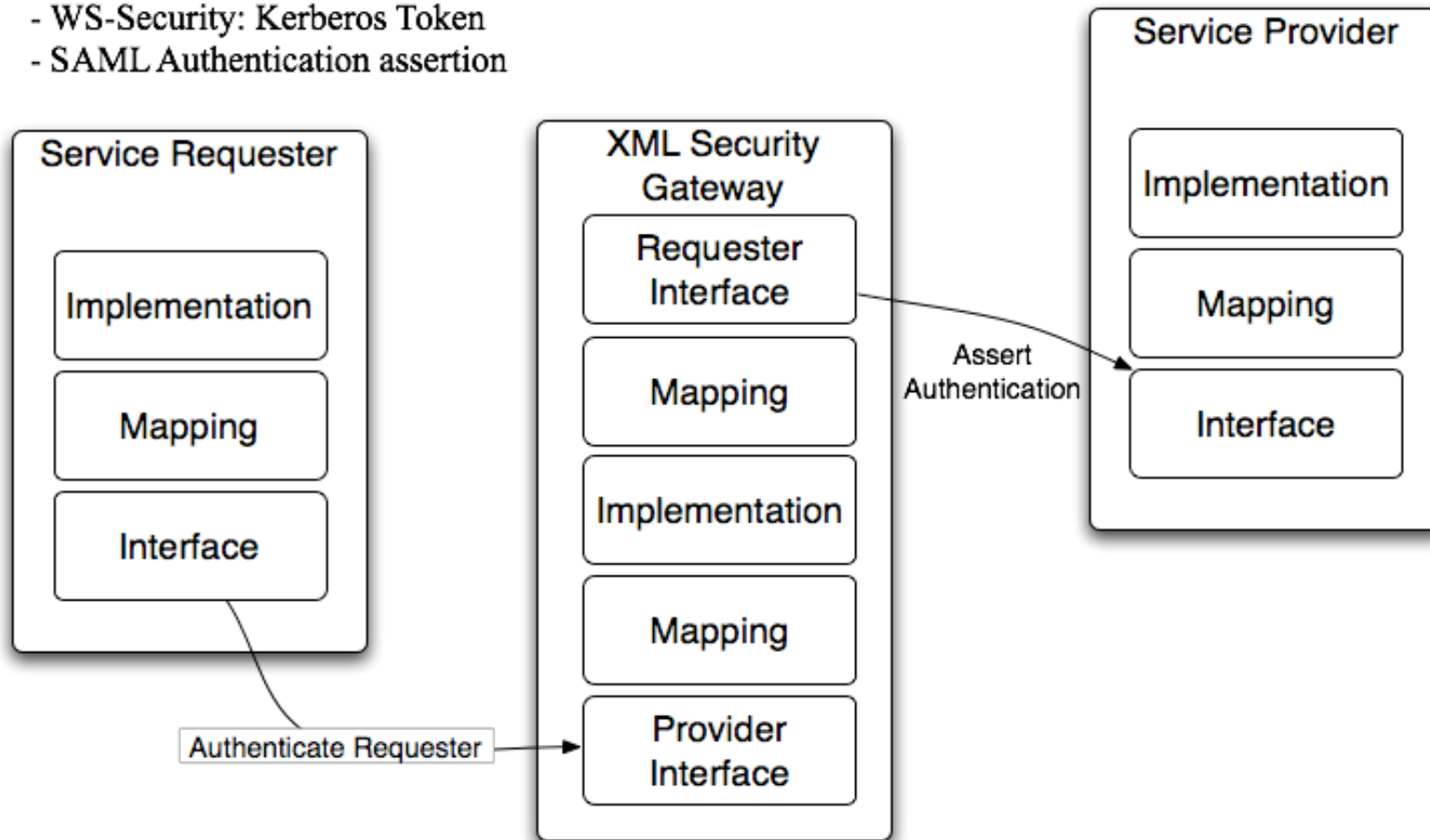
    <getCustomerDetails xmlns="http://servicehost"/>
      <name>Joe Smith</name>
      <password>hard2guess</password>
      <customernumber>1234</customernumber>

  </soap:Body>
</soap:Envelope>
```



Authentication Services

- Mutual SSL
- HTTP Basic Authentication
- HTTP Digest Authentication
- WS-Security Username Token
- WS-Security X.509 Certificate
- WS-Security: Kerberos Token
- SAML Authentication assertion



Let's authenticate the message

```
<soap:Envelope
xmlns:soap="http://schemas.xmlsoap.org/soap/envelope/">
  <soap:Header>
    <wsse:Security
xmlns:wsse="http://schemas.xmlsoap.org/ws/2003/06/secext">
      <wsse:UsernameToken
xmlns:wsu="http://schemas.xmlsoap.org/ws/2003/06/utility"
wsu:Id="Id-00000112932fa600-00000000000000003">

        <wsse:Username>joesmith</wsse:Username>

        <wsse:Password
Type="wsse:PasswordText">hard2guess</wsse:Password>

        <wsu:Created>2007-05-16T04:40:12Z</wsu:Created>
      </wsse:UsernameToken>
    </wsse:Security>
  </soap:Header>

  <soap:Body>
<ns0:getCustomerDetails xmlns:ns0="http://servicehost"/>
<customernumber>1234</customernumber>
```

...



Can we make it stronger?

```
<soap:Envelope xmlns:soap="http://schemas.xmlsoap.org/soap/envelope/">
  <soap:Header>

    <wsse:Security xmlns:wsse="http://schemas.xmlsoap.org/ws/2003/06/secext">
      <wsse:UsernameToken
xmlns:wsu="http://schemas.xmlsoap.org/ws/2003/06/utility" wsu:Id="Id-
00000112933021b1-00000000000000004">

        <wsse:Username>joesmith</wsse:Username>

        <wsse:Nonce EncodingType="utf-
8">2rxMB18VSv3jctE9Nr+xKRWpK0VZu8sp7wg527Fr+7U=</wsse:Nonce>
        <wsse:Password
Type="wsse:PasswordDigest">mkCDa1Qj1nGA32+1L2ywCp4oMT8=</wsse:Password>

        <wsu:Created>2007-05-16T04:40:44Z</wsu:Created>
      </wsse:UsernameToken>
    </wsse:Security>
  </soap:Header>
  <soap:Body>
<ns0:getCustomerDetails xmlns:ns0="http://servicehost"/>
<customernumber>1234</customernumber>
  </soap:Body>
</soap:Envelope>
```



Can we make it stronger?

```
<soap:Envelope xmlns:soap="http://schemas.xmlsoap.org/soap/envelope/">
  <soap:Header>
    <wsse:Security xmlns:wsse="http://schemas.xmlsoap.org/ws/2003/06/secext">
      <dsig:Signature xmlns:dsig="http://www.w3.org/2000/09/xmldsig#" Id="Id-000001129332ad32-0000000000000000">
        <dsig:SignedInfo>
          <dsig:SignatureMethod Algorithm="http://www.w3.org/2000/09/xmldsig#rsa-sha1"/>
          <dsig:DigestMethod Algorithm="http://www.w3.org/2000/09/xmldsig#sha1"/>
            <dsig:DigestValue>dZdbQbIysLPvzuS5xsf57nUMB/M=</dsig:DigestValue>

          <dsig:SignatureValue>VM2cLToMCNi9I9+TXtJYrI2FBXSfuKzazY8UUK4r4hNNrQu4KhDnn0Fq/mWhROTB8DELXF6BDkoGmKRzTi5pgxg6+FGgy/v0I+Kmk1R4Q3+2fzMVSZJy2i5607oR9pJ3fm8nAYf3ceamz0s43am07S9uDG+0E0zdbfSiGLTx4+o=</dsig:SignatureValue>
            <dsig:KeyInfo Id="Id-000001129332ad32-00000000000000001">
              <dsig:X509Data>
                <dsig:X509Certificate>
CRDCCAa0CBEX67+4wDQYJKoZIhvcNAQEEBQAwaTEQMA4GA1UEBhMHVW5rbm93bjEQMA4GA1UE...
                </dsig:X509Certificate>
              </dsig:X509Data>
            </dsig:KeyInfo>
          </dsig:SignedInfo>
        </dsig:Signature>
      </wsse:Security>
    </soap:Header> ...
  <ns0:getCustomerDetails xmlns:ns0="http://servicehost"/>
    <customernumber>1234</customernumber>
  </soap:Envelope>
```



XSGEC Authentication

- Evaluate XSG's ability to
 - ▶ Authenticate service requesters
 - ▶ Assert security tokens and other authentication primitives to service providers



What about the message content?

- XML Messages can contain a number of nasty things...
 - ▶ Injection attacks
 - SQL Injection, Xpath Injection, Xquery Injection
 - ▶ XML Denial of Service (XDoS)
 - Using XML as an attack vector
 - Jumbo payloads
 - Recursion
 - ▶ Virus in SOAP attachments



XSG Validation Services

■ Schema validation based on hardened schemas

```
<xs:simpleType name="Zipcode">
  <xs:restriction base="xs:string"
    <xs:pattern value="([0-9]{5})-([0-9]{4}) "/>
  </xs:restriction>
</xs:simpleType>
```

■ Semantic validation based on white list or blacklist

- ▶ Regex

■ Virus scanning

■ XDoS Countermeasures

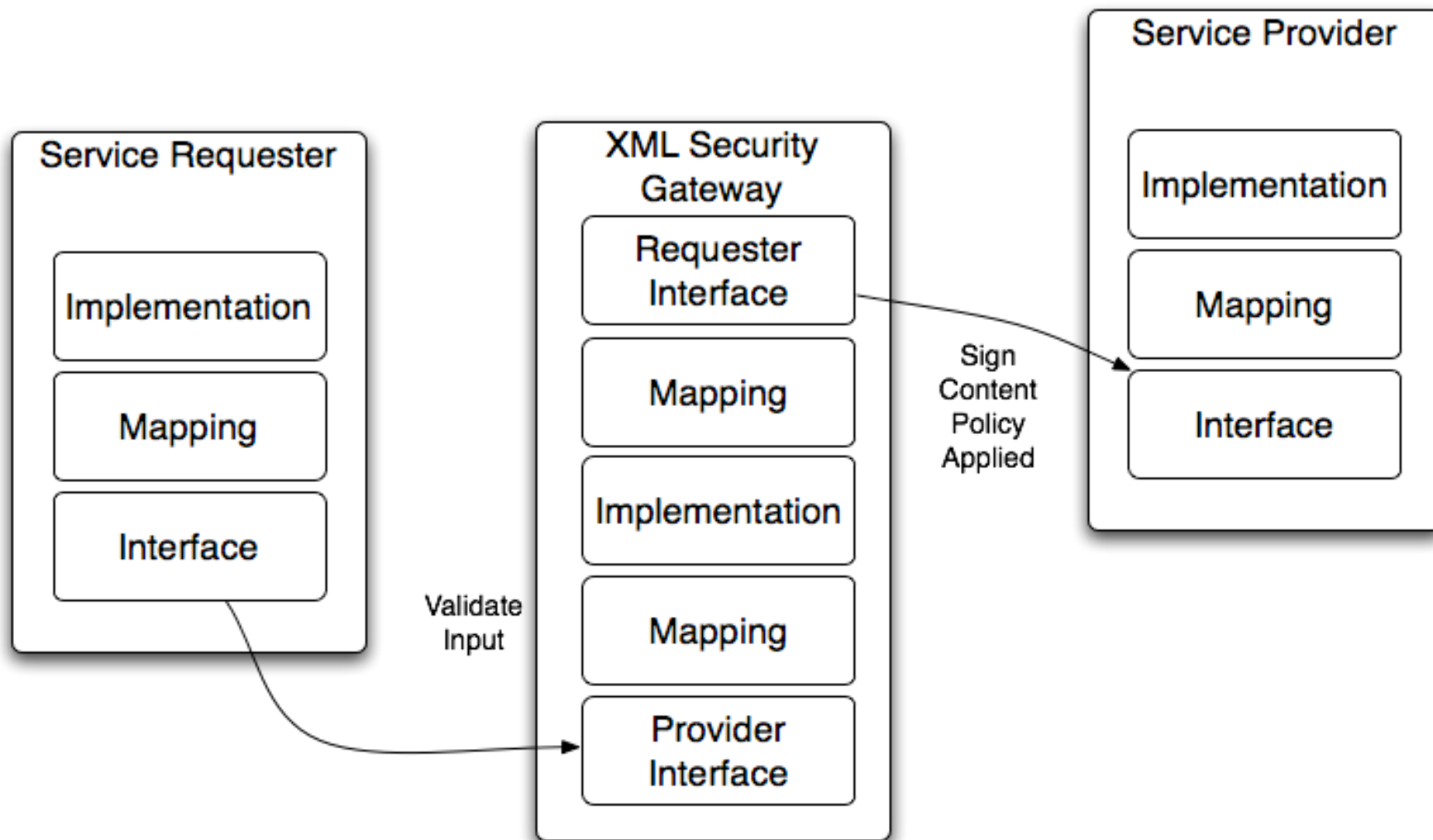
- ▶ Example: min/max message size



XSGEC Content Validation

- Evaluate XSG's ability to enable
 - ▶ Schema validation
 - ▶ Semantic validation
 - ▶ XDoS protection
 - ▶ Virus scanning





XSG Sign Request

```
<wsse:Security
xmlns:wsse="http://schemas.xmlsoap.org/ws/2003/06/secext">
  <wsse:UsernameToken
xmlns:wsu="http://schemas.xmlsoap.org/ws/2003/06/utility
" wsu:Id="Id-000001129356fac9-0000000000000000e">

    <wsse:Username>XSG</wsse:Username>

    <wsse:Nonce EncodingType="utf-
8">hF0W+PM/JIwKVQUz11Xt/r1EE73Wx1SPyqAfi jguG
Mk=</wsse:Nonce>

    <wsse:Password
Type="wsse:PasswordDigest">7jwftIDmLZjBSN5zopmyEd4iY6w=</ws
se:Password>
    <wsu:Created>2007-05-16T05:23:10Z</wsu:Created>
  </wsse:UsernameToken>
</wsse:Security>
</soap:Header>
```



Sign Content - Policy Applied

```
<wsse:Security xmlns:wsse="http://schemas.xmlsoap.org/ws/2003/06/secext">
  <saml:Assertion xmlns:saml="urn:oasis:names:tc:SAML:1.0:assertion"
AssertionID="Id-000001129354af1c-0000000000000002" IssueInstant="2007-05-
16T05:20:39Z" Issuer="CN=Test,OU=Unknown" MajorVersion="1" MinorVersion="1">
  <saml:Conditions NotBefore="2007-05-16T04:40:35Z" NotOnOrAfter="2007-05-
16T06:40:35Z"/>
  <saml:AuthorizationDecisionStatement Decision="Permit"
Resource="http://host/service">
    <saml:Subject>
      <saml:NameIdentifier Format="urn:oasis:names:tc:SAML:1.1:nameid-
format:X509SubjectName">Test</saml:NameIdentifier>
    </saml:Subject>
    <saml:Action>getCustomerDetails</saml:Action>
  </saml:AuthorizationDecisionStatement>
  <dsig:SignatureValue>V6pRh0SnrvS8xT+WXIbNv1r0hVkaUMVI4YZ27KfG/jDLMwSbrsD6E3tA4
0rI6naL
U+gt20sYr58rD+AILpxNk0uxZMwdLcj3zr0gljt339DvYL6MRJBZ3KvpDmrw16PM
w8Wo7ac1tGcLFVW5PV5locPs+f0V+r0GHafYTGGlubQ=</dsig:SignatureValue>
  <dsig:KeyInfo Id="Id-000001129354af1d-0000000000000004">
    ...
  </saml:Assertion>
</wsse:Security>
</soap:Header>
<soap:Body>
<ns0:getCustomerDetails xmlns:ns0="http://servicehost"/>
<customernumber>1234</customernumber>
```

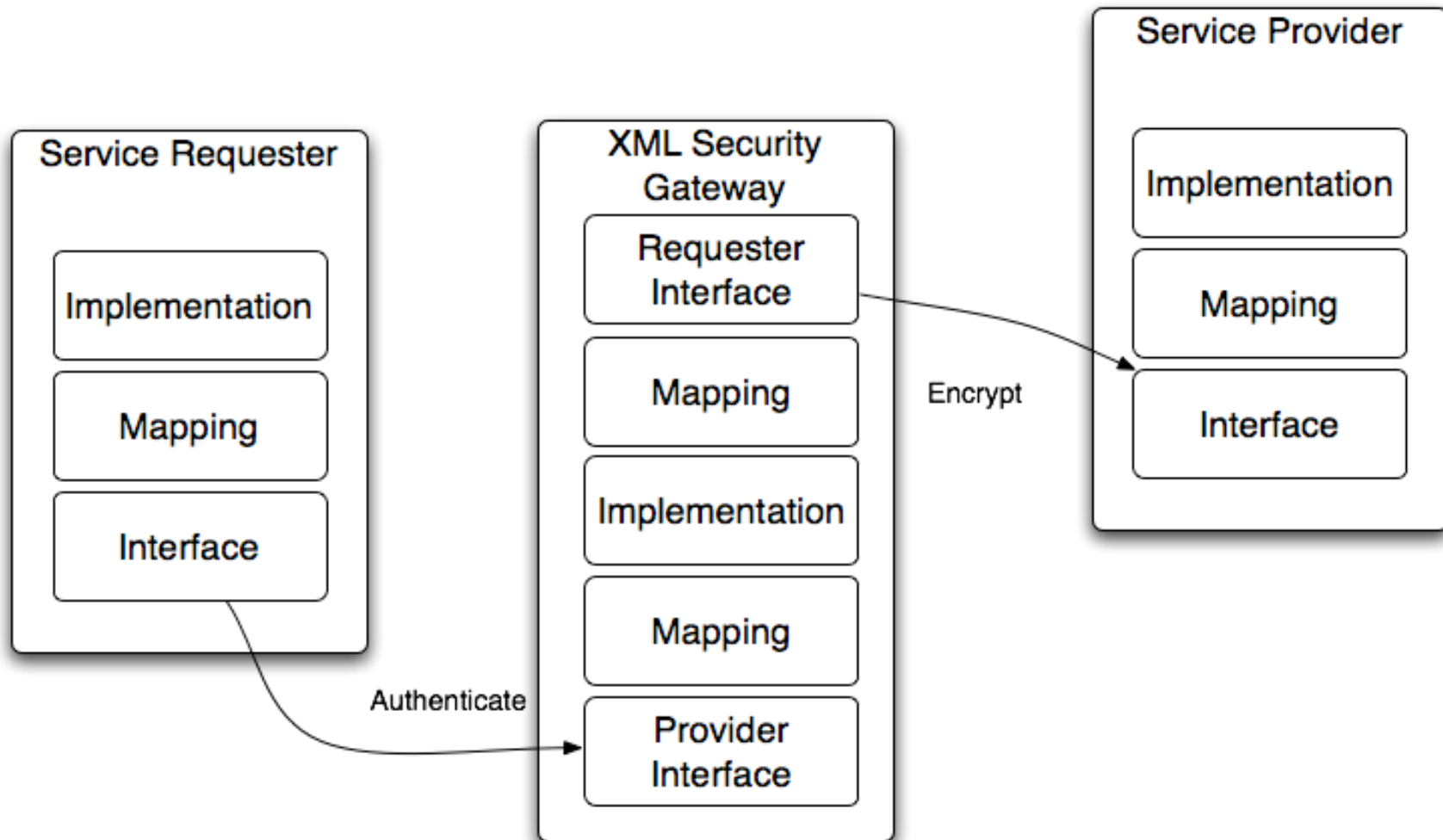


XSGEC Authorization Support

- Evaluate XSG's ability to
 - ▶ Assert that a specific policy has been applied by a XSG at a certain time for a given request, subject, condition, and action



Encrypt for Remote Hosts



XML Encryption

```
<soap:Body>
<ns0:getCustomerDetails xmlns:ns0="http://servicehost"/>

<enc:EncryptedData..>
  <enc:EncryptionMethod Algorithm="http://www.w3.org/2001/04/xmlenc#aes256-
cbc
"/>

    <enc:CipherData>

<enc:CipherValue>EjADnNmG1VK9wTiG+La+uHaDthMnSs1N6CXv0I1DIyVT/M1asHgM+
  </enc:CipherData>
  <enc:ReferenceList>
    <enc:DataReference URI="#Id-000001129355dbad-0000000000000009"/>
  </enc:ReferenceList>
  <enc:CarriedKeyName>Id-000001129355dbad-
0000000000000008</enc:CarriedKey
Name>

    <wsu:Timestamp
xmlns:wsu="http://schemas.xmlsoap.org/ws/2003/06/utility"
  wsu:Id="Id-000001129355dbb6-000000000000000d">
    <wsu:Created>2007-05-16T05:21:56Z</wsu:Created>
```

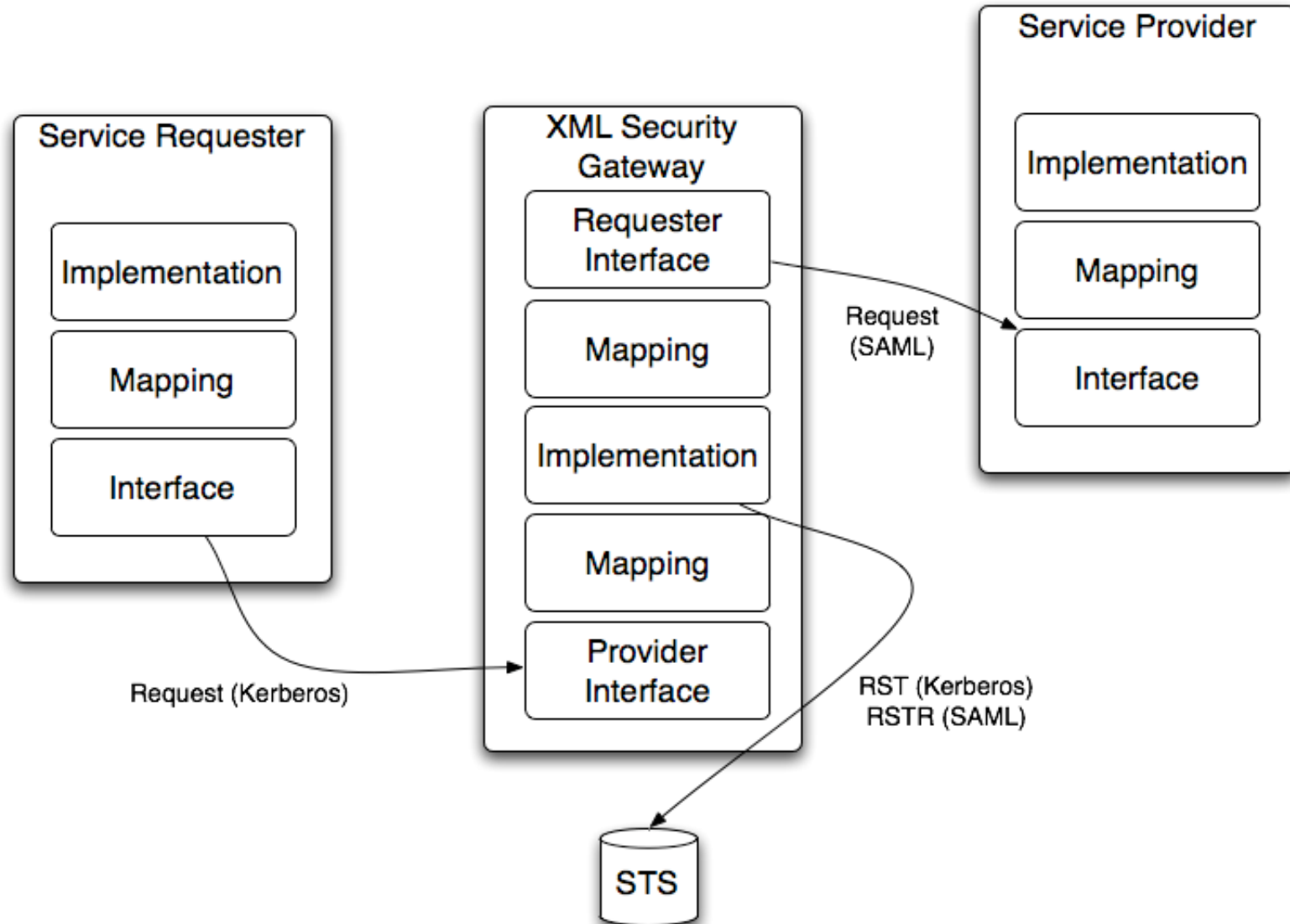


XSGEC

- Evaluate XSG's ability to
 - ▶ Protect/encrypt/sign outbound messages



STS - Attribute & Identity Mapping



XSGEC

- Evaluate XSG's ability to:
 - ▶ Map inbound/outbound security tokens
 - ▶ Map inbound/outbound attributes



XSG Metrics

■ Asset metrics

- ▶ Transactional throughput volume and performance

■ Threat metrics

- ▶ Malicious requests/responses

■ Vulnerability metrics

- ▶ Policy violations



XSGEC

■ Evaluate XSG's ability to:

- ▶ Provide historical, predictive, and real time metrics for
 - Assets
 - Threats
 - Vulnerabilities



XSGEC

Understand
key architecture tradeoffs
&
design considerations



XSGEC

- Interested in participating? More information:
- http://www.owasp.org/index.php/Category:OWASP_XML_Security_Gateway_Evaluation_Criteria_Project

