WS-Policy and WS-SecurityPolicy

Overview

- Introduction
- Policy assertions
- Main security bindings
- RampartConfig Assertion

WS-Policy

- General framework for endpoints to express requirements
- Basic operators
  - wsp:All
  - wsp:ExactlyOne
- Domain assertions
  - WS-SecurityPolicy Language
  - Just XML elements

Basic operators example

```
<wsp:Policy>
    <wsp:ExactlyOne>
        <wsp:All>
            <A/>
            <B/>
        </wsp:All>
        <wsp:All>
            <A/>
            <C/>
        </wsp:All>
    </wsp:ExactlyOne>
</wsp:Policy>
```

WS-SecurityPolicy

- Based on WS-Policy
- Various groups of policy assertions
- Can be embedded into WSDL or referenced

WS-SecurityPolicy

- To express security requirements of a Web service according to the WS-Policy spec
  - What needs to be protected
  - What tokens to use
  - Algorithms, reference types, etc..
- Covers all WS-Sec* specifications

Assertion Types

- Protection assertions
- Token assertions
- Binding assertions
- Supporting token assertions
- Protocol assertions

Protection Assertions

- Specify what needs to be protected
  - Integrity
  - Confidentiality
- Signed/EncryptedParts
- Signed/EncryptedElements
- RequiredElements

Signed/Encrypted Parts

- Headers
  - name / namespace
  - namespace
- Body
- Protect when present

Example

```
<sp:SignedParts xmlns:sp="http://...securitypolicy">
    <sp:Body/>
    <sp:Header Name="To" Namespace="http://.../ws/
2004/08/addressing"/>
    <sp:Header Name="From" Namespace="http://.../ws/
2004/08/addressing"/>
</sp:SignedParts>

<sp:EncryptedParts xmlns:sp="http://...securitypolicy">
    <sp:Body/>
</sp:EncryptedParts>
```

Signed/Encrypted elements

- arbitrary elements in the SOAP envelope
- configured using XPATH

Example

```
<sp:EncryptedElements xmlns:sp="http://../
securitypolicy">
   <sp:XPath
      xmlns:ns1="http://InteropBaseAddress/interop"
      xmlns:ns2="http://xmlsoap.org/Ping">
        /soapenv:Envelope/soapenv:Body/
                        ns1:PingResponse/ns2:scenario
    </sp:XPath>
</sp:EncryptedElements>
```

Required Elements

- arbitrary elements in the SOAP envelope
- configured using XPATH

Example

```
<sp:RequiredElements xmlns:sp="http://../
securitypolicy">
    <sp:XPath
            xmlns:a="http://xmlsoap.org/Ping">
                /soapenv:Envelope/soapenv:Body/
ns1:PingResponse/ns2:scenario/a:scenario
    </sp:XPath>
</sp:RequiredElements>
```

Token Assertions

- Specifying token types to use
  - UsernameToken
  - X. 509
  - IssuedToken
  - SecureConversation
  - Kerberos
- Token Inclusion
  - Never
  - Always
  - AlwaysToRecipient
  - Once

Token Assertion Examples

```
<sp:X509Token sp:IncludeToken="http://.../IncludeToken/
Never">
    <wsp:Policy>
        <sp:WssX509V3Token10/>
    </wsp:Policy>
</sp:X509Token>

<sp:UsernameToken sp:IncludeToken="http://.../
AlwaysToRecipient" />
```

Bindings

- Collections of security properties (values populated by assertions)
  - Tokens
  - Algorithms
  - Processing order
  - Inclusion of timestamp

Bindings

- Three main types:
  - TransportBinding
  - AsymmetricBinding
  - SymmetricBinding
- Security Binding properties

Algorithm Suite

- Defines values algorithms to be used
  - [Sym Sig] Symmetric Key Signature
  - [Asym Sig] Signature with an asymmetric key
  - [Dig] Digest
  - [Enc] Encryption
  - [Sym KW] Symmetric Key Wrap
  - [Asym KW] Asymmetric Key Wrap
  - [Comp Key] Computed key
  - [Enc KD] Encryption key derivation
  - [Sig KD] Signature key derivation
  - [Min SKL] Minimum symmetric key length
  - [Max SKL] Maximum symmetric key length
  - [Min AKL] Minimum asymmetric key length
  - [Max AKL] Maximum asymmetric key length
- Pre defined set of a algorithm suites
  - eg. Basic256, Basic192

Algorithm Suite	[Dig]	[Enc]	[Sym KW]	[Asym KW]	[Enc KD]	[Sig KD]	[Min SKL]
Basic256	Sha1	Aes256	KwAes256	KwRsaOaep	PSha1L256	PSha1L192	256
Basic192	Sha1	Aes192	KwAes192	KwRsaOaep	PSha1L192	PSha1L192	192

Security Binding Properties

- Timestamp
  - Default : false
  - sp:IncludeTimestamp sets property to true
- Protection Order
  - Default : Sign before encryption
  - sp:EncryptBeforeSigning to change it

Security Binding Properties

- Signature Protection
  - Default: false
  - sp:EncryptSignature sets property to true
  - signature should be encrypted
- Token Protection
  - Default: false
  - sp:ProtectTokens sets property to true
  - Token used to generate the signature must aslo be covered by the signature

Security Binding Properties

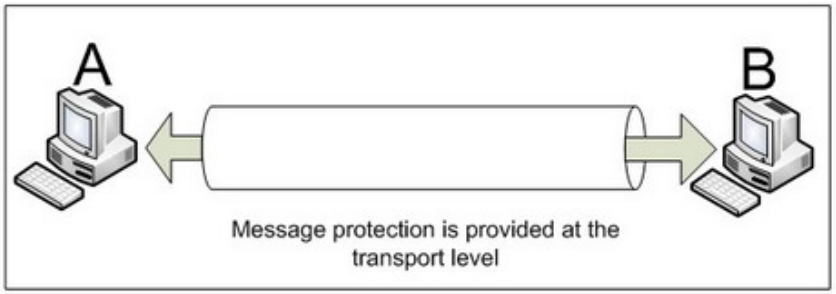
- Entire Header and Body Signatures
  - Default: false
  - sp:OnlySignEntireHeadersAndBody sets property to true.

Security Binding Properties

- Security Header Layout
  - Strict
  - Lax
  - LaxTimestampFirst
  - LaxTimestampLast
- Declare before use principle
- Default: Lax

Transport Binding

- Indicates that the transport layer is used to satisfy the security requirements



Transport Binding

- Allows specification of :
  - Transport tokens
  - Security header layout
  - Timestamp presence
  - Supporting tokens

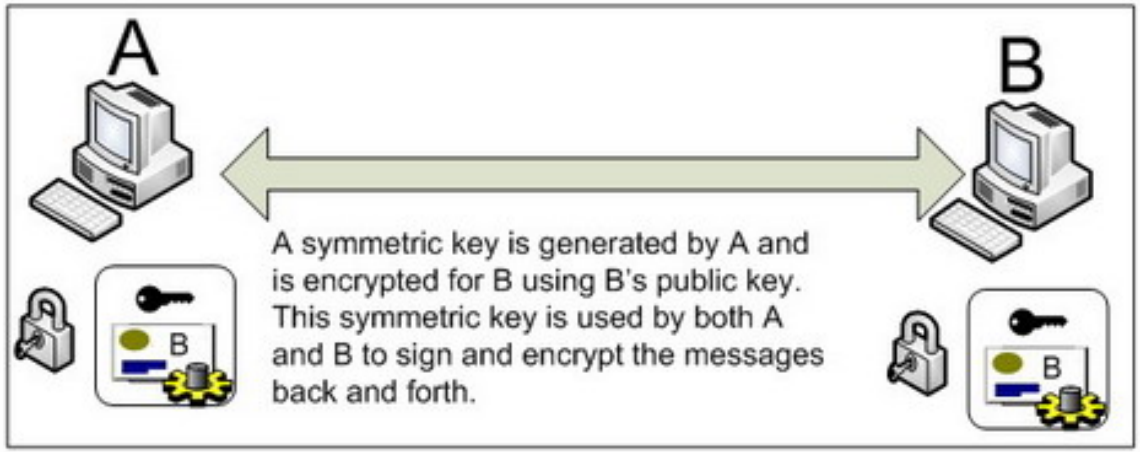
Transport Binding example

```
<sp:TransportBinding>
 <wsp:Policy>
  <sp:TransportToken>
   <wsp:Policy>
    <sp:HttpsToken />
   </wsp:Policy>
  </sp:TransportToken>
  <sp:AlgorithmSuite>...</sp:AlgorithmSuite>
  <sp:IncludeTimestamp />
 </wsp:Policy>
</sp:TransportBinding>
```

Symmetric Binding

- Indicates that the message layer is used to satisfy the security requirements
- Defines "Encryption Token" and "Signature Token" properties
- Where multiple messages are exchanged the tokens perform the same functions for all messages

Symmetric Binding



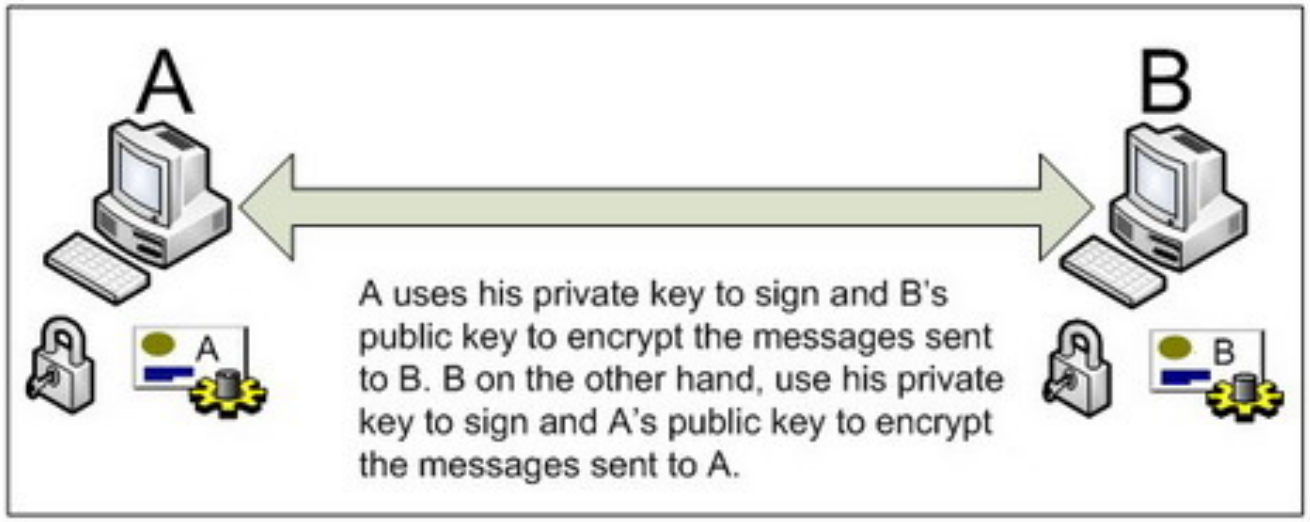
SymmetricBinding Example

```
<sp:SymmetricBinding>
 <wsp:Policy>
  <sp:ProtectionToken>
   <wsp:Policy>
    <sp:X509Token
    sp:IncludeToken="http://.../IncludeToken/Never"/>
   </wsp:Policy>
  </sp:ProtectionToken>
  <sp:AlgorithmSuite><sp:Basic256/></sp:AlgorithmSuite>
  <sp:EncryptBeforeSigning />
 </wsp:Policy>
</sp:SymmetricBinding>
```

Asymmetric Binding

- Indicates that the message layer is used to satisfy the security requirements
- Defines “Initiator Token” and “Recipient Token” properties
- Where multiple messages are exchanged the tokens perform different functions

Asymmetric Binding



Asymmetric Binding Example

```
<sp:AsymmetricBinding>
 <wsp:Policy>
  <sp:InitiatorToken>
   <wsp:Policy>
    <wsp:X509Token sp:IncludeToken='.../IncludeToken/AlwaysToRecipient' />
   </wsp:Policy>
  </sp:InitiatorToken>
  <sp:RecipientToken>
   <wsp:Policy>
    <wsp:X509Token sp:IncludeToken='.../IncludeToken/Never' />
   </wsp:Policy>
  </sp:RecipientToken>
  <sp:AlgorithmSuite><sp:Basic128/></sp:AlgorithmSuite>
  <sp:EncryptBeforeSigning />
 </wsp:Policy>
</sp:AsymmetricBinding>
```

Supporting Tokens

- Services may require multiple sets of claims to be presented
- Corresponds to additional tokens in a message
  - eg. Symmetric binding + Username token

Supporting Tokens Example

```
<sp:SupportingTokens>
 <wsp:Policy>
  <sp:UsernameToken sp:IncludeToken=‘.../
IncludeToken/Once’ />
 </wsp:Policy>
</sp:SupportingTokens>
```

Supporting Token types

Type	Sign main signature?	Signed by main token?
Supporting	No	No
Endorsing	Yes	No
Signed	No	Yes
Signed Endorsing	Yes	Yes

WSS Assertions

- WSS10
- <sp:MustSupportRefKeyIdentifier ... />
  <sp:MustSupportRefIssuerSerial ... />
  <sp:MustSupportRefExternalURI ... />
  <sp:MustSupportRefEmbeddedToken ... />

- WSS11
- <sp:MustSupportRefKeyIdentifier ... />
  <sp:MustSupportRefIssuerSerial ... />
  <sp:MustSupportRefExternalURI ... />
  <sp:MustSupportRefEmbeddedToken ... />
  <sp:MustSupportRefThumbprint ... />
  <sp:MustSupportRefEncryptedKey ... />
  <sp:RequireSignatureConfirmation ... />

WSS Assertions

- Should be able to process any of the key referencing mechanisms

```
<sp:X509Token sp:IncludeToken="http://../
  IncludeToken/Never">
      <wsp:Policy>
        <sp:RequireThumbprintReference/>
        <sp:WssX509V3Token10/>
      </wsp:Policy>
</sp:X509Token>
```

WSS Assertion Examples

```
<sp:Wss10>
 <wsp:Policy>
  <sp:MustSupportRefKeyIdentifier />
  <sp:MustSupportRefExternalURI />
 </wsp:Policy>
</sp:Wss10>

<sp:Wss11>
 <wsp:Policy>
  <sp:MustSupportRefExternalURI />
  <sp:MustSupportRefThumbprint />
  <sp:RequireSignatureConfirmation />
 </wsp:Policy>
</sp:Wss11>
```

Trust Assertions

- Specify supported version of WS-Trust and associated properties
  - sp:Trust10
- Example :

```
<sp:Trust10>
 <wsp:Policy>
  <sp:RequireClientEntropy />
  <sp:RequireServerEntropy />
 </wsp:Policy>
</sp:Trust10>
```

Policy Subjects

- Message Policy Subject
  - wsdl:binding/wsdl:operation/wsdl:input,
  - wsdl:binding/wsdl:operation/wsdl:output
- Operation Policy Subject
  - wsdl:binding/wsdl:operation
- Endpoint Policy Subject
  - wsdl:binding

Policy Subjects

- MUST NOT attach to
- Message Policy Subject
  - wsdl:message
  - wsdl:portType/wsdl:operation/wsdl:input
- Operation Policy Subject
  - wsdl:portType/wsdl:operation
- Endpoint Policy Subject
  - wsdl:portType

Applying Security Policies

services.xml

```
<service>
<wsp:Policy/>
   <operation name="echo">
      <wsp:Policy/>
       <message label="In">
          <wsp:Policy/>
       </message>
       <message label="Out">
          <wsp:Policy/>
       </message>
   </operation>
<service>
```

Applying Security Policies

```
<service>
   <wsp:PolicyAttachment
                  xmlns:wsp="http://../policy">
    <wsp:AppliesTo>
     <policy-subject identifier="binding:soap11" />
     <policy-subject identifier="binding:soap12" />
    </wsp:AppliesTo>
    <wsp:Policy/>
   </wsp:PolicyAttachment>
</service>
```

Applying Security Policies

```
<service>
   <wsp:PolicyAttachment
                  xmlns:wsp="http://../policy">
     <wsp:AppliesTo>
       <policy-subject  identifier="binding:soap11/
operation:echo" />
       <policy-subject identifier="binding:soap12/
operation:echo" />
     </wsp:AppliesTo>
     <wsp:Policy/>
   </wsp:PolicyAttachment>
</service>
```

Applying Security Policies

```
<service>
   <wsp:PolicyAttachment
                  xmlns:wsp="http://../policy">
     <wsp:AppliesTo>
       <policy-subject  identifier="binding:soap11/
operation:echo/in" />
       <policy-subject identifier="binding:soap12/
operation:echo/in" />
     </wsp:AppliesTo>
     <wsp:Policy/>
   </wsp:PolicyAttachment>
</service>
```