IBM Software Group

# WS-Policy

## WS-SecurityPolicy Overview

e business on demand software

# Agenda

- WS-SecurityPolicy
  - Introduction
  - Assertion types
  - Token assertions
  - Binding assertions
  - Protocol assertions

# WS-SecurityPolicy

- Builds on WS-Policy
  - Uses nested policy to provide scope
- Defines various groups of policy assertions
- Expressed in WSDL per WS-PolicyAttachment

# WS-SecurityPolicy

- Designed for expressing security requirements
  - What needs to be protected
  - What tokens to use
  - Algorithms, reference types, etc.
- Constrains content and layout of wsse:Securityheader

# WS-SecurityPolicy

- Uses assertions to define exchange pattern in use
- A given pattern has fixed and variable aspects
- Variable aspects modelled as properties
  - Policy assertions populate properties

# Assertion Types

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

# Protection Assertions

- Specify what needs to be protected
  - Integrity protection
  - Confidentiality
- Part and element based assertions defined

# Protection Assertions Examples

```
<sp:SignedParts>
 <sp:Body />
 <sp:Header
  Namespace='http://schemas.xmlsoap.org/ws/2004/09/addressing' />
</sp:SignedParts>
```

```
<sp:SignedElements>
 <sp:XPath>/soap:Envelope/soap:Body</sp:XPath>
 <sp:XPath>
 /soap:Envelope/soap:Header/*[namespace-uri()=
'http://schemas.xmlsoap.org/ws/2004/09/addressing']</sp:XPath>
</sp:SignedElements>
```

# Token Assertions

- Specify the type of token to be used
- Take the form of token type and nested version assertion
  - Other nested assertions also allowed
- Carry an inclusion attribute
  - Specifies which messages token appears in

# Token Assertions Examples

```
<sp:X509Token sp:IncludeToken='.../IncludeToken/AlwaysToRecipient' >
 <wsp:Policy>
  <sp:WssX509V3Token10 />
 </wsp:Policy>
</sp:X509Token>
```

```
<sp:SamlToken
  sp:IncludeToken='.../IncludeToken/Always' >
 <wsp:Policy>
  <sp:WssSamlV11Token11 />
 </wsp:Policy>
</sp:SamlToken>
```

# Security Bindings

- Collections of properties
  - Tokens
  - Algorithms
  - Processing order et.al.
- Properties populated by assertions
  - Some have default values
- Spec defines three broad types

# Security Bindings Properties

- [AlgorithmSuite]
  - Populated by sp:AlgorithmSuiteand nested assertions
- [Timestamp]
  - Defaults to false
  - sp:IncludeTimestampsets property to true
- [Protection Order]
  - Defaults to SignBeforeEncrypting
  - sp:EncryptBeforeSigningsets property to EncryptBeforeSigning

# Security Bindings Properties

- [Signature Protection]
  - Defaults to false
  - sp:EncryptSignaturesets property to true
- [Token Protection]
  - Defaults to false
  - sp:ProtectTokenssets property to true
- [Entire Header and Body Signatures]
  - Defaults to false
  - sp:OnlySignEntireHeadersAndBodysets property to true.

# Security Bindings Properties

- •[Security Header Layout]
  - Populated by sp:Layoutassertion and nested assertions
  - Defaults to ‘Lax’

# Transport Bindings

- Indicates that the transport layer is used to satisfy the security requirements
- Allows specification of such things as
  - Security header layout
  - Timestamp presence
  - Supporting tokens

# Transport Bindings Examples

```
<sp:TransportBinding>
 <wsp:Policy>
  <sp:TransportToken>
   <wsp:Policy>
    <sp:HttpsToken />
   </wsp:Policy>
  </sp:TransportToken>
  <sp:AlgorithmSuite><sp:Basic256Rsa15 /></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 Examples

```
<sp:SymmetricBinding>
 <wsp:Policy>
  <sp:ProtectionToken>
   <wsp:Policy>
    <wsp:KerberosToken sp:IncludeToken='.../IncludeToken/Once' />
   </wsp:Policy>
  </sp:ProtectionToken>
  <sp:AlgorithmSuite><sp:Basic128Rsa15/></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 Examples

```
<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:Basic128Rsa15/></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

# Supporting Tokens Types

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

# Supporting Tokens Example

```
<sp:TransportBinding>
 <wsp:Policy>
  <sp:TransportToken>
   <wsp:Policy>
    <sp:HttpsToken />
   </wsp:Policy>
  </sp:TransportToken>
  <sp:AlgorithmSuite><sp:Basic256Rsa15 /></sp:AlgorithmSuite>
  <sp:IncludeTimestamp />
  <sp:SupportingTokens>
   <wsp:Policy>
    <sp:UsernameToken sp:IncludeToken='.../IncludeToken/Once' />
   </wsp:Policy>
  </sp:SupportingTokens>
 </wsp:Policy>
</sp:TransportBinding>
```

# WSS Assertions

- •Specify supported version of WSS
  - sp:Wss10
  - sp:Wss11
- Specify supported token reference mechanisms via Boolean properties
- Specify Signature Confirmation requirements for WSS 1.1

# WSS10 Properties

| Property Name | Default Value | Assertion |
|---|---|---|
| [Direct References] | True | None |
| [Key Identifier References] | False | sp:MustSupportKeyIdentifierReferences |
| [Issuer Serial References] | False | sp:MustSupportIssuerSerialReferences |
| [External URI References] | False | sp:MustSupportExternalURIReferences |
| [Embedded Token References] | False | sp:MustSupportEmbeddedTokenReferences |

79

# WSS11 Properties

| Property Name | Default Value | Assertion |
|---|---|---|
| [Thumbprint References] | False | sp:MustSupportThumbprintReferences |
| [Encrypted Key References] | False | sp:MustSupportEncryptedKeyReferences |
| [Signature Confirmation] | False | sp:MustSupportExternalURIReferences |
| [Embedded Token References] | False | sp:RequireSignatureConfirmation |

# 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

# Trust Properties

| Property Name | Default Value | Assertion |
|---|---|---|
| [Client Challenge] | False | sp:MustSupportClientChallenge |
| [Server Challenge] | False | sp:MustSupportServerChallenge |
| [Client Entropy] | False | sp:RequireClientEntropy |
| [Server Entropy] | False | sp:RequireServerEntropy |
| [Issued Tokens] | False | sp:MustSupportIssuedTokens |

# Trust Assertion Example

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

# Where are we ?

- WS-Trust provides flexible framework for building token processing protocols
- WS-SecureConversation provides secure sessions
- WS-SecurityPolicy describes security configuration
  - WSS, WS-Trust, WS-SecureConversation