Lesson 20 – WS-Policy

Service Oriented Architectures Security

Module 1 - Basic technologies

Unit 1 – Introduction

Ernesto Damiani

Università di Milano

Agenda

Introduction

Domain Terminology

Policy Expressions

Policy Assertions

Policy Attachments

Conclusion

Policy In Action

Introduction to WS-Policy

Why?

- To integrate software systems with web services
- Need a way to express its characteristics
  - –When/Does it *require …*
    - WS-Security?
    - signed messages?
    - encryption?
  - –What security tokens is it *capable* of processing?
  - –What tokens does it *prefer*?
- Without this standard, developers need docs

Introduction to WS-Policy

What?

- Provides a flexible and extensible *grammar* for expressing the *capabilities*, *requirements*, and *general characteristics* of Web Service *entities*

How?

- Defines a model to express these properties as policies

Introduction to WS-Policy

Goal:

- Provide the mechanisms needed to enable Web Services applications to specify policies

WS-Policy specifies:

1. An XML-based structure called a policy expression containing policy information
2. Grammar elements to indicate how the contained policy assertions apply

Agenda

Introduction

Domain Terminology

Policy Expressions

Policy Assertions

Policy Attachments

Conclusion

Policy In Action

Terminology

Policy: refers to the set of information being expressed as *policy assertions*

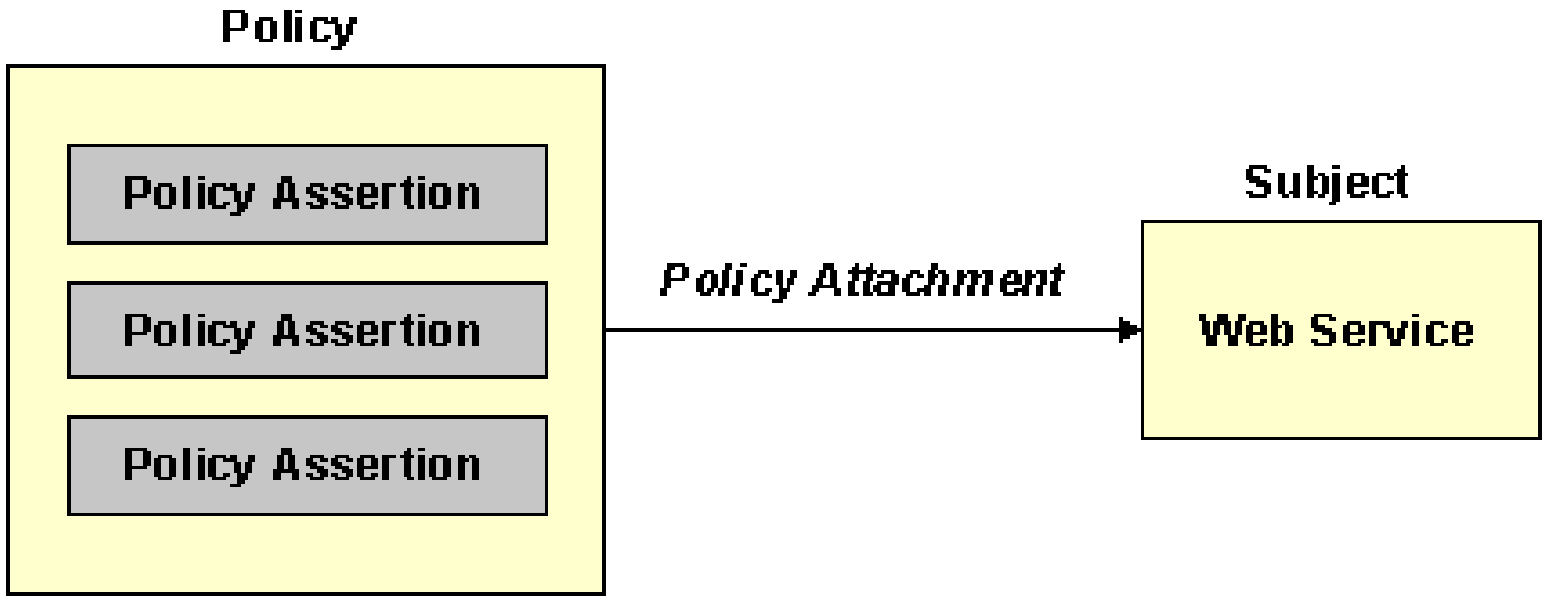
Policy Assertion: represents an individual preference, requirement, capability, etc.

Policy Expression: set of one or more *policy assertions*

Policy Subject: an entity to which a *policy expression* can be bound

Terminology

Policy Attachment: the mechanism for associating policy expressions with one or more subjects



Agenda

Introduction

Domain Terminology

Policy Expressions

Policy Assertions

Policy Attachments

Conclusion

Policy In Action

Policy Expressions

A Policy Expression is the XML representation of a policy

- XML facilitates interoperability between a heterogeneous platforms

We will look at how to name and identify them

Policy Namespaces

WS-Policy schema defines all constructs that can used in a *policy expression*

Prefix	Description	Namespace
wsp	WS-Policy, WS-PolicyAssertions, and WS-PolicyAttachment	http://schemas.xmlsoap.org/ws/2002/12/policy
wsse	WS-SecurityPolicy	http://schemas.xmlsoap.org/ws/2002/12/secext
wsu	WS utilty schema	http://schemas.xmlsoap.org/ws/2002/07/utility
msp	WSE 2.0 policy schema	http://schemas.microsoft.com/wse/2003/06/Policy

Policy Namespaces

wsp:Policy

- Representation of a *policy expression*
- Container for *policy assertions*

```
<wsp:Policy xmlns:wsp="..."
xmlns:wsu="..." wsu:Id="..."
   Name="..." TargetNamespace="...">
   <!-- policy assertions go here -->
</wsp:Policy>
```

- The wsu:Id attribute assigns the *policy expression* an ID value as a URI

Policy Expression Naming

A full ID is formed by:

<base URI>#<wsu:Id value>

Policy Expression:

```
<wsp:Policy xmlns:wsp="..."
    xmlns:wsu="..." wsu:Id="MyPolicies" >
    ...</wsp:Policy>
```

Policy Reference:

```
...
<wsp:PolicyReference xmlns:wsp="..."
  URI="http://virginia.edu/isis/policy.xml#MyPolicies"/>
...
```

Policy Expression Naming

Alternatively, use namespace-qualified name

- Add `Name` and `TargetNamespace`:

```
<wsp:Policy xmlns:wsp="..." Name="MyPolicies"
      TargetNamespace="http://virginia.edu/policies">
...</wsp:Policy>
```

Reference:

```
...
<wsp:PolicyReference xmlns:wsp="..."
      xmlns:p="http://virginia.edu/policies"
      Ref="p:MyPolicies"/>
...
```

Agenda

Introduction

Domain Terminology

Policy Expressions

Policy Assertions

Policy Attachments

Conclusion

Policy In Action

Policy Assertions

A policy assertion:

- represents an individual preference, requirement, capability, or other characteristic
- is the basic building block of a policy expression
- an XML element with a well-known name and meaning

```
<wsp:Policy xmlns:wsp="..." xmlns:wsu="..." wsu:Id="..."
      Name="..." TargetNamespace="..." >
      <Assertion wsp:Usage="..." wsp:Preference="..." />
      <Assertion wsp:Usage="..." wsp:Preference="..." />
... </wsp:Policy>
```

Types of Assertions

Two types:

1. Requirements and capabilities that are explicitly manifested on the wire
2. No wire manifestation, just provide information

The Usage Qualifier

wsp:Usage distinguishes between

- different types of assertions
- how assertions are processed

Value	Meaning
wsp:Required	The assertion must be applied, otherwise an error results
wsp:Rejected	The assertion is not supported and, if present, will cause failure
wsp:Optional	The assertion may be made of the subject, but is not required
wsp:Observed	The assertion will be applied to all subjects and requestors are told
wsp:Ignored	The assertion will be ignored if present and requestors are told

Assertion Example

What does this Assertion state?

```
<wsp:Policy xmlns:wsp="..." xmlns:wsse="...">
  <wsse:SecurityToken wsp:Usage="wsp:Required">
<wsse:TokenType>wsse:Kerberosv5ST</wsse:TokenType>
  </wsse:SecurityToken>
  <wsse:Integrity wsp:Usage="wsp:Required">
    <wsse:Algorithm Type="wsse:AlgSignature"
      URI="http://www.w3.org/2000/09/xmlenc#aes" />
  </wsse:Integrity>
</wsp:Policy>
```

Two policy assertions:

1. Security Token is required
2. Use of AES is required

Assertion Preference

wsp:Preference attribute:

- Used to specify the service's preference as an integer value
- Larger integer => higher preference
- Omitted preference attribute is interpreted as a 0

Assertion Preference Example

What does this Assertion state?

```
<wsp:Policy xmlns:wsp="..." xmlns:wsse="...">
  <wsse:SecurityToken wsp:Usage="wsp:Optional">

<wsse:TokenType>wsse:UsernameToken</wsse:TokenType>
  </wsse:SecurityToken>
  <wsse:SecurityToken wsp:Usage="wsp:Optional"
    wsp:Preference="1">
    <wsse:TokenType>wsse:x509v3</wsse:TokenType>
  </wsse:SecurityToken>
</wsp:Policy>
```

The subject prefers X.509 certificates over UsernameTokens

Standard Policy Assertions

WS-PolicyAssertions defines four general policy assertions for any subject

Policy Assertion	Description
wsp:TextEncoding	Specifies a character encoding
wsp:Language	Specifies a natural language (xml:Lang)
wsp:SpecVersion	Specifies a version of a particular specification
wsp:MessagePredicate	Specifies a predicate that can be tested against the message (XPath expressions by default)

General Assertion Example

What does this Assertion state?

```
<wsp:Policy xmlns:wsse="...">
  <wsp:TextEncoding wsp:Usage="wsp:Required"
Encoding="utf-8"/>
  <wsp:Language wsp:Usage="wsp:Required" Language="en"/>
  <wsp:SpecVersion wsp:Usage="wsp:Required"
    URI="http://www.w3.org/TR/2000/NOTE-SOAP-20000508/" />
  ...
</wsp:Policy>
```

The subject requires

1. The UTF-8 character encoding
2. Any form of the English language
3. SOAP version 1.1

General Assertion Example

What does this Assertion state?

```
<wsp:Policy xmlns:wsp="..." xmlns:wsse="...">
  <wsp:MessagePredicate wsp:Usage="wsp:Required">
    count(wsp:GetHeader(.)/wsse:Security) = 1
  </wsp:MessagePredicate>
  <wsp:MessagePredicate wsp:Usage="wsp:Required">
    count(wsp:GetBody(.)/*) = 1
  </wsp:MessagePredicate>
  ...
</wsp:Policy>
```

Must be:

1. Exactly one wsse:Security header element
2. Exactly one child within the soap:Body element

WS-SecurityPolicy

Defines a set of security-related assertions

Policy Assertion	Description
wsse:SecurityToken	Specifies a type of security token (defined by WS-Security)
wsse:Integrity	Specifies a signature format (defined by WS-Security)
wsse:Confidentiality	Specifies an encryption format (defined by WS-Security)
wsse:Visibility	Specifies portions of a message that MUST be able to be processed by an intermediary or endpoint
wsse:SecurityHeader	Specifies how to use the <Security> header defined in WS-Security
wsse:MessageAge	Specifies the acceptable time period before messages are declared "stale" and discarded

Combining Multiple Assertions

Policy operators are used to combine assertions

- Can nest operators

Policy Operator	Description
wsp:All	Requires that all of its child elements be satisfied
wsp:ExactlyOne	Requires that exactly one child to be satisfied
wsp:OneOrMore	Requires that at least one child be satisfied
wsp:Policy	Same as wsp:All

Assertion Combination Example

What does this Assertion state?

```
<wsp:Policy xmlns:wsp="..." xmlns:wsse="...">
  <wsp:ExactlyOne wsp:Usage="Required">
    <wsse:SecurityToken>
      <wsse:TokenType>wsse:UsernameToken</wsse:TokenType>
    </wsse:SecurityToken>
    <wsse:SecurityToken wsp:Preference="10">
      <wsse:TokenType>wsse:x509v3</wsse:TokenType>
    </wsse:SecurityToken>
    <wsse:SecurityToken wsp:Preference="1">
      <wsse:TokenType>wsse:Kerberosv5ST</wsse:TokenType>
    </wsse:SecurityToken>
  </wsp:ExactlyOne>
</wsp:Policy>
```

Exactly one child must be satisfied

Policy Reference

Mechanism to share policy assertions across policy expressions

Uses the naming conventions discussed above

```
<wsp:Policy xmlns:wsp="...">
  ...
  <wsp:PolicyReference URI="..."
                       Ref="..."
                       Digest="..."
                       DigestAlgorithm="..." />
  ...
</wsp:Policy>
```

Policy Reference Example

```
<wsp:Policy wsu:Id="tokens" xmlns:wsp="..." xmlns:wsse="...">
  <wsp:ExactlyOne wsp:Usage="Required">
    <wsse:SecurityToken>
      <wsse:TokenType>wsse:UsernameToken</wsse:TokenType>
    </wsse:SecurityToken>
    <wsse:SecurityToken wsp:Preference="10">
      <wsse:TokenType>wsse:x509v3</wsse:TokenType>
    </wsse:SecurityToken>
    <wsse:SecurityToken wsp:Preference="1">
      <wsse:TokenType>wsse:Kerberosv5ST</wsse:TokenType>
    </wsse:SecurityToken>
  </wsp:ExactlyOne>
</wsp:Policy>
```

Policy Reference Example

```
<wsp:Policy wsu:Id="tokensWithSignature"
  xmlns:wsp="..." xmlns:wsse="...">
  <wsp:PolicyReference URI="#tokens" />
  <wsse:Integrity wsp:Usage="wsp:Required">
    ...
  </wsse:Integrity>
</wsp:Policy>

<wsp:Policy wsu:Id="tokensWithEncryption"
  xmlns:wsp="..." xmlns:wsse="...">
  <wsp:PolicyReference URI="#tokens" />
  <wsse:Confidentiality wsp:Usage="Required">
  ...
  </wsse:Confidentiality>
</wsp:Policy>
```

Agenda

Introduction

Domain Terminology

Policy Expressions

Policy Assertions

Policy Attachments

Conclusion

Policy In Action

Policy Attachments

WS-PolicyAttachment defines mechanisms to associate expressions with subjects

Specifically defines mechanisms for:

- XML elements
- WSDL definitions
- UDDI entries

Uses attributes

1. wsp:PolicyURIs – list of URIs
2. wsp:PolicyPrefs – list of QNames

Policy Attachments

The attribute wsp:PolicyAttachment binds an endpoint to a policy expression

- Requires no change to the web service

```
<wsp:PolicyAttachment>
  <wsp:AppliesTo>
    <wsa:EndpointReference xmlns:s="...">
      <wsa:Address>http://virginia.edu/someendpoint</wsa:Address>
      <wsa:PortType>s:SomePortType</wsa:PortType>
      <wsa:ServiceName>s:SomeService</wsa:ServiceName>
    </wsa:EndpointReference>
  </wsp:AppliesTo>
  <wsp:PolicyReference URI="http://virginia.edu/policy.xml" />
  <wsse:Security>
    <ds:Signature> ... </ds:Signature>
  </wsse:Security>
</wsp:PolicyAttachment>
```

Agenda

Introduction

Domain Terminology

Policy Expressions

Policy Assertions

Policy Attachments

Conclusion

Policy In Action

Conclusion of WS-Policy

The policy specifications define a standard framework

Developers can:

- express requirements, capabilities, and preferences in an interoperable way
- select web services more meaningfully

Policies provide support for standard assertions

Primary References

http://msdn.microsoft.com/webservices/default.aspx?pull=/library/en-us/dnglobspec/html/ws-policy.asp#ws-policy__toc42483108

- Official document describing WS-Policy

http://msdn.microsoft.com/library/default.asp?url=/library/en-us/dnwebsrv/html/understwspol.asp

- "Understanding WS-Policy" – A great reference that I used a lot for this presentation. Provides a great, easy explanation of WS-Policy.

Secondary References

http://schemas.xmlsoap.org/ws/2002/12/Policy/

- This is the policy schema definition

http://msdn.microsoft.com/webservices/default.aspx?pull=/library/en-us/dnglobspec/html/ws-policyassertions.asp

- Provides a very detailed description of WS-PolicyAssertions

http://msdn.microsoft.com/webservices/default.aspx?pull=/library/en-us/dnglobspec/html/ws-policyattachment.asp

- Provides a very detailed description of WS-PolicyAttachment

http://msdn.microsoft.com/webservices/default.aspx?pull=/library/en-us/dnglobspec/html/ws-securitypolicy.asp

- Provides a detailed description of WS-SecurityPolicy

Policy In Action

- **Web Service Enhancements (WSE) 2.0 for .NET 2.0 provides basic support for WS-Policy**
- **Let's go!**