

Requirements for policy- management in distributed systems

Policy workshop
Sun Microsystems
21 Feb 2003

Types of policy

- Authorization
 - Is this request properly authorized?
- Cryptographic security
 - Does this request have the required security attributes?
- Privacy
 - Is the requested disclosure properly authorized?
- Trust
 - Is this key acceptable for this purpose?
- Others

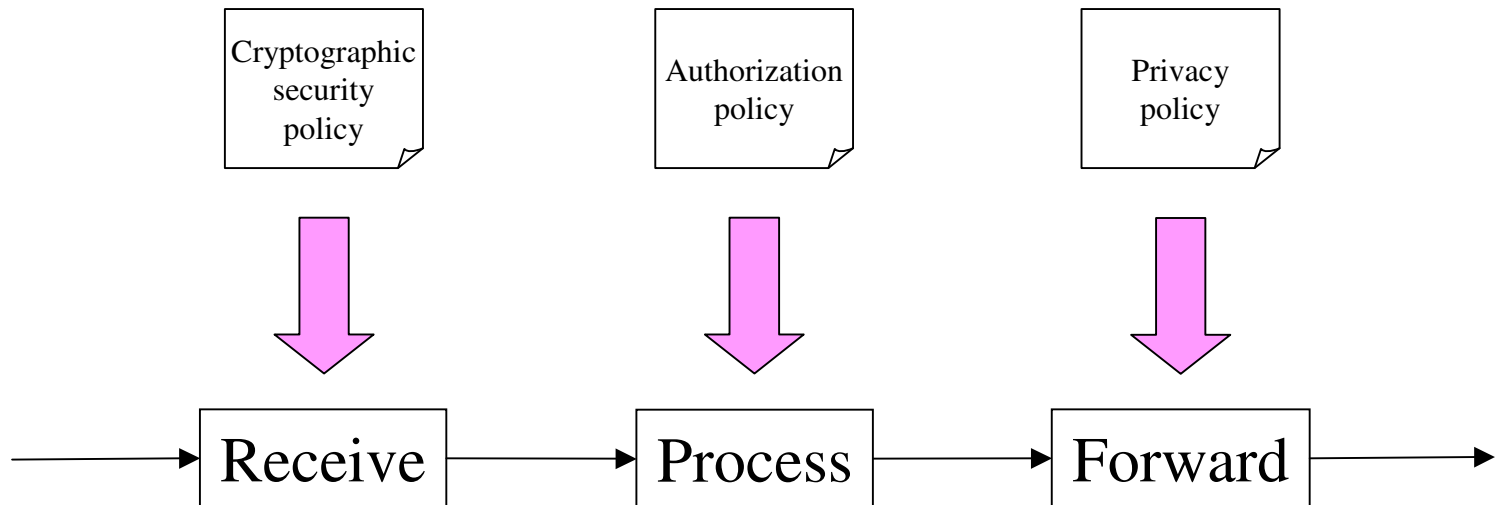
XAMPL

```
<Apply FunctionId="urn:oasis:names:tc:xacml:1.0:function:and">  
  <Apply FunctionId="urn:oasis:names:tc:xacml:1.0:function:anyURI-equal">  
    <ResourceAttributeDesignator AttributeId="wssqop:key-management-algorithm"  
      DataType="http://www.w3.org/2001/XMLSchema#anyURI"/>  
    <AttributeValue DataType="http://www.w3.org/2001/XMLSchema#anyURI">  
      Ds#rsa-sha1  
    </AttributeValue>  
  </Apply>  
  <Apply FunctionId="urn:oasis:names:tc:xacml:1.0:function:integer-greater-than-or-equal">  
    <ResourceAttributeDesignator AttributeId="wssqop:key-size"  
      DataType="http://www.w3.org/2001/XMLSchema#integer"/>  
    <AttributeValue DataType="http://www.w3.org/2001/XMLSchema#integer">  
      1024  
    </AttributeValue>  
  </Apply>  
</Apply>
```

Alternative view

- Policy instances contain data:-
 - Requirements
 - Capabilities
 - Preferences
 - Properties
 - Features
- “This service supports English” \equiv “Is this request in English?”

Application points



Questions a service-consumer may ask

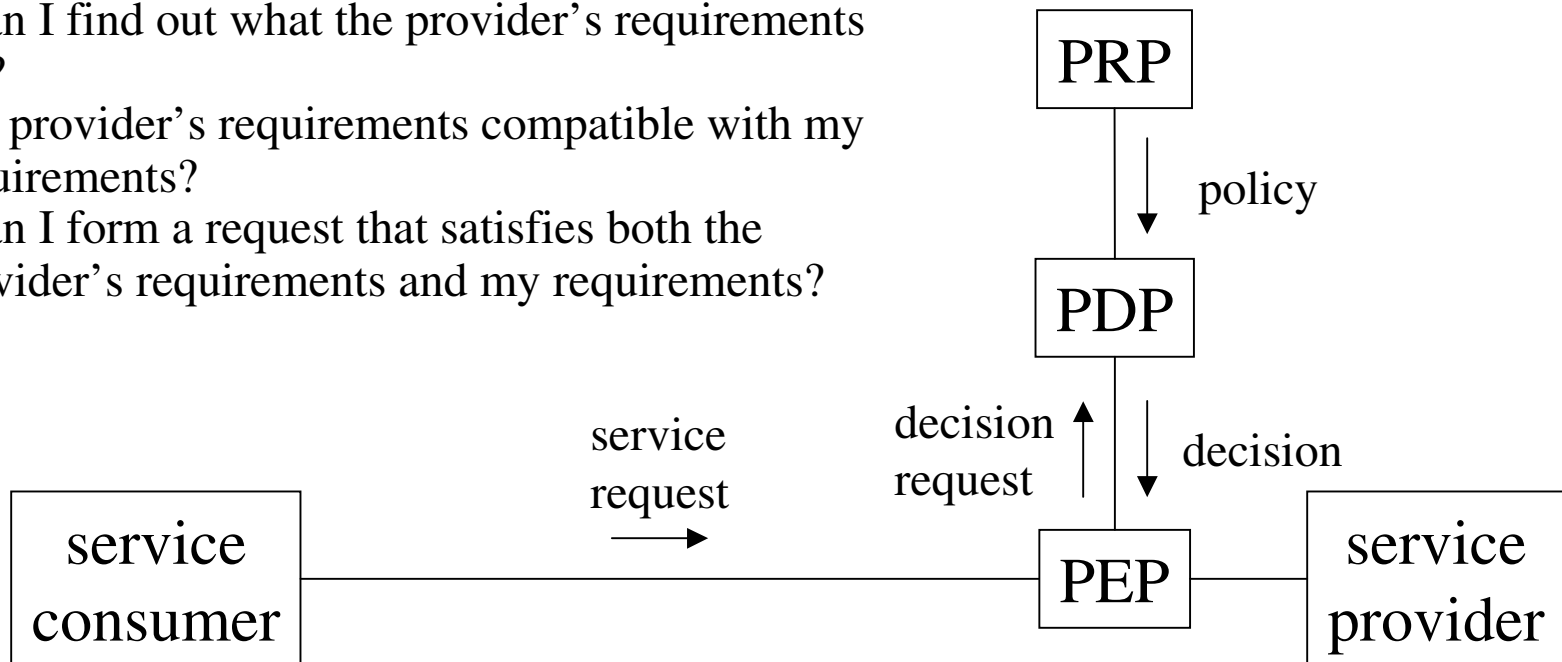
Does my request satisfy the provider's requirements?

How can I form a request that satisfies the provider's requirements?

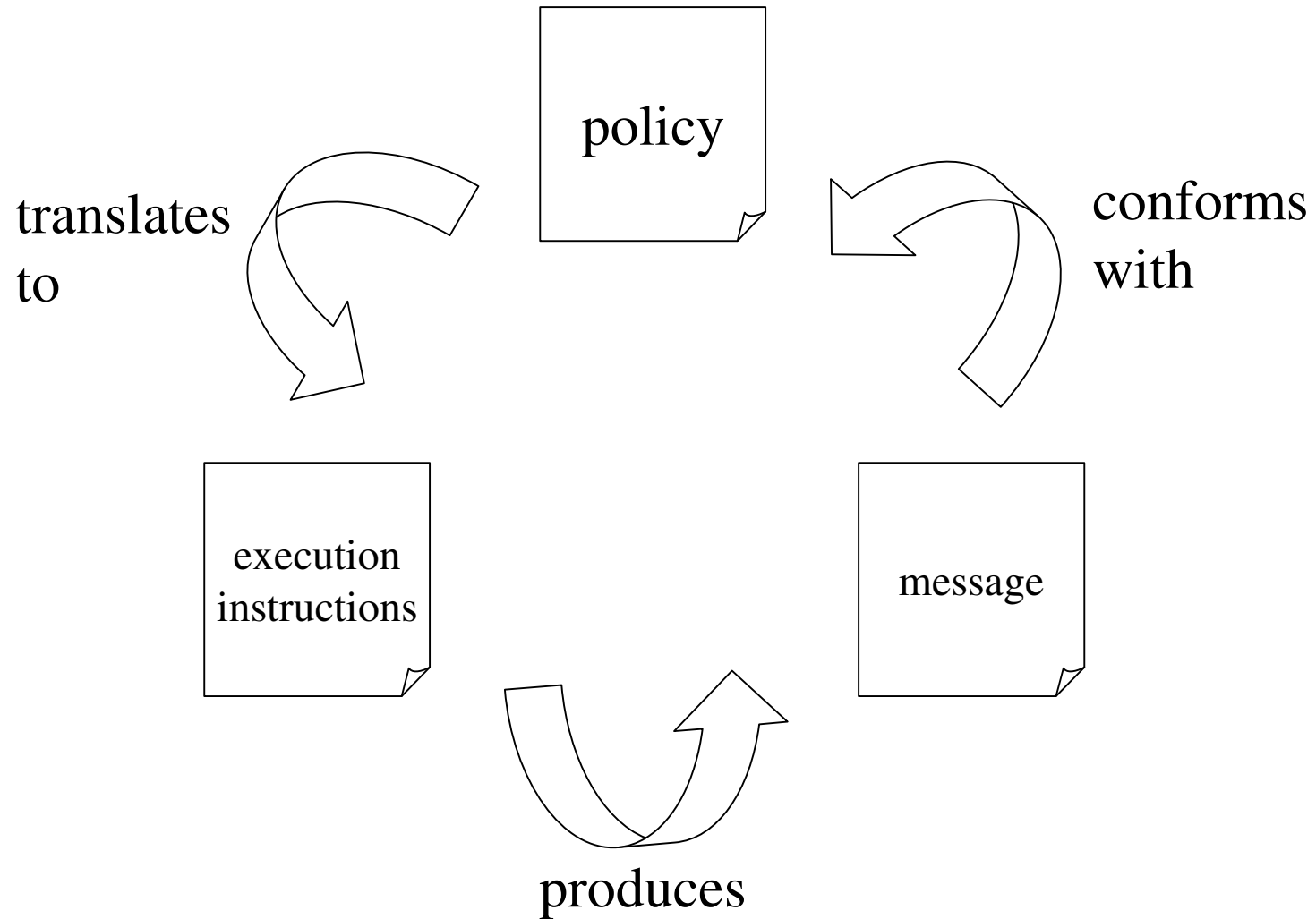
How can I find out what the provider's requirements are?

Are the provider's requirements compatible with my requirements?

How can I form a request that satisfies both the provider's requirements and my requirements?



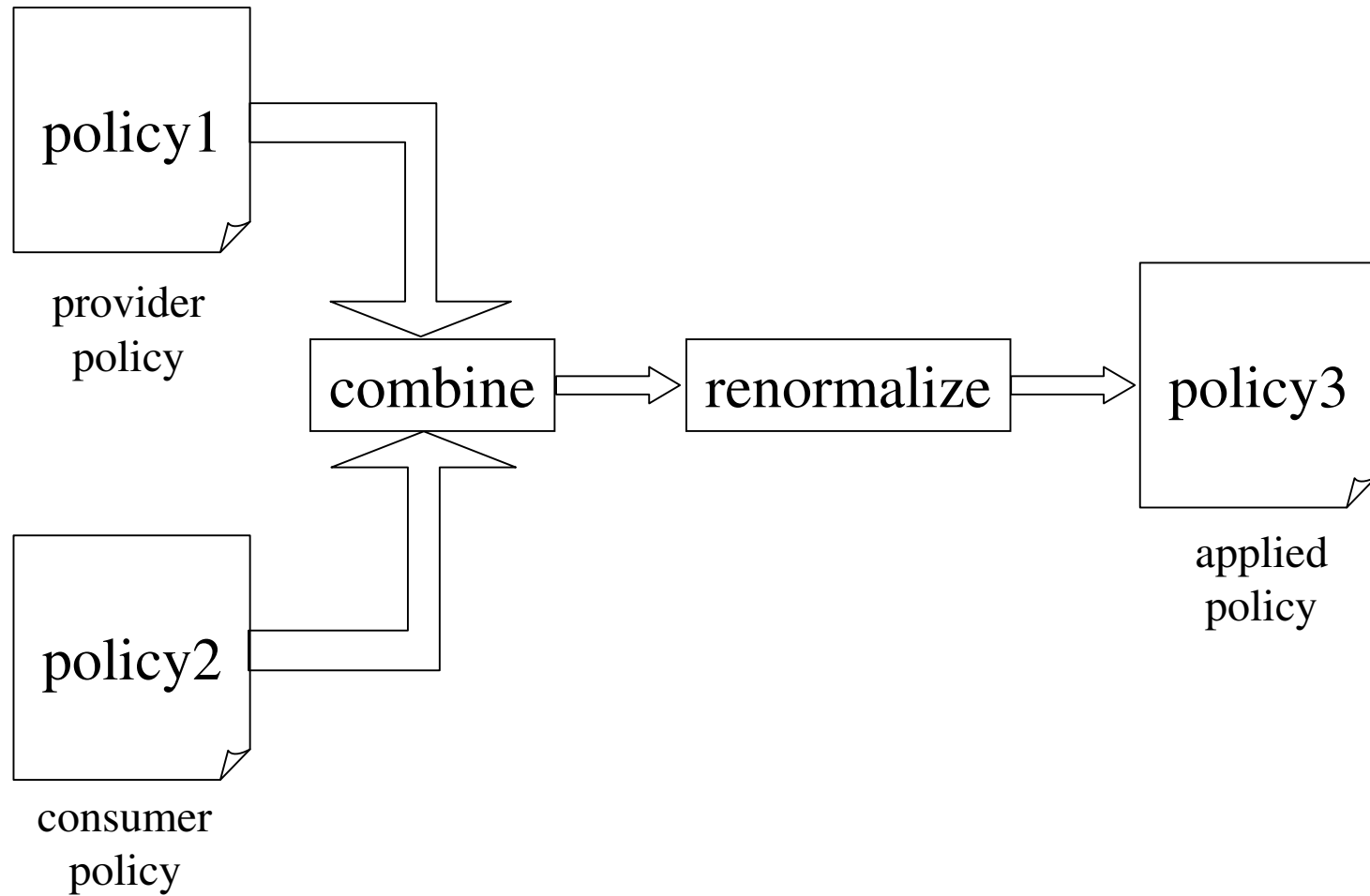
Solving policy



XAMPL

WSPF	XACML	BPEL4WS
<All>	<Apply and>	<sequence>
<OneOrMore>	<Apply or>	<switch>

Combining consumer and provider policies



Combining policies

- All component policies **MUST** be satisfied

<and>

<policy1/>

<policy2/>

</and>

- Any one component policy **MUST** be satisfied

<or>

<policy1/>

<policy2/>

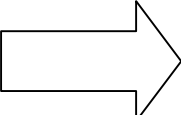
</or>

Renormalization

- Sample rules
 - Collapse identical adjacent operators
 - Reorder a sequence
 - Combine identical set operators
 - Combine identical inequality operators

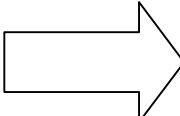
XAMPL

```
<and>  
  <and>  
  ...  
</and>  
<and>  
  ...  
</and>  
</and>
```



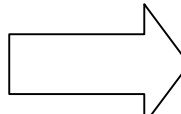
```
  <and>  
  ...  
  ...  
</and>
```

```
<superset a>  
  b  
  c  
</superset>  
<superset a>  
  c  
  d  
</superset>
```



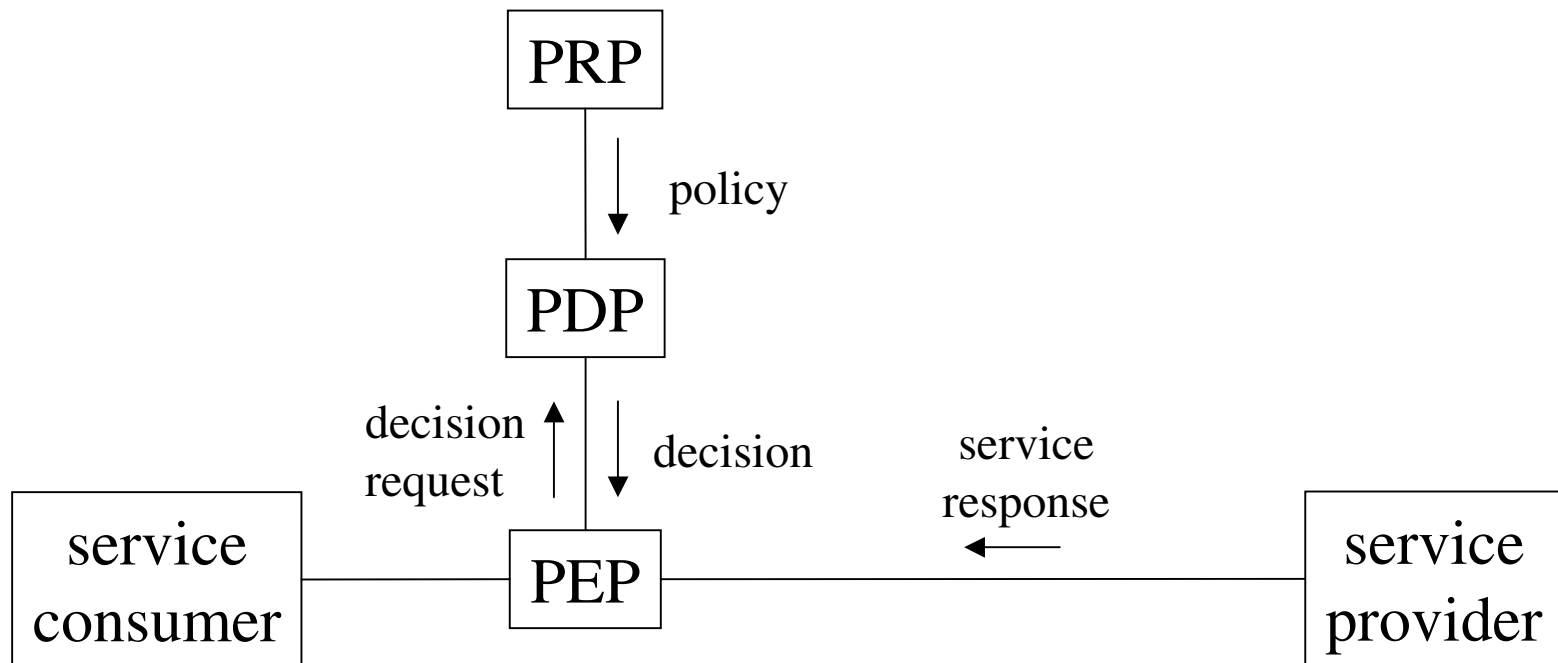
```
<superset a>  
  union{b,c,c,d}  
</superset>
```

```
<greater-than a>  
  b  
</greater-than>  
<greater-than a>  
  c  
</greater-than>
```



```
<greater-than a>  
  max{b,c}  
</greater-than>
```

Policy for responses



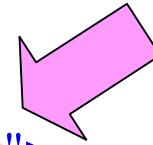
Policy distribution

- WSDL
 - Provider policy
 - <wsdl:operation> element
- SOAP
 - Consumer policy
 - <wsse:security> header element
- LDAP
 - Attribute of target entry
- HTTP
 - ?

Requirements and capabilities

	Form of message prevents processing	Form of message permits processing
Provider returns Fault	REQUIRE	REJECT
Provider processes message	SUPPORT	SUPPORT

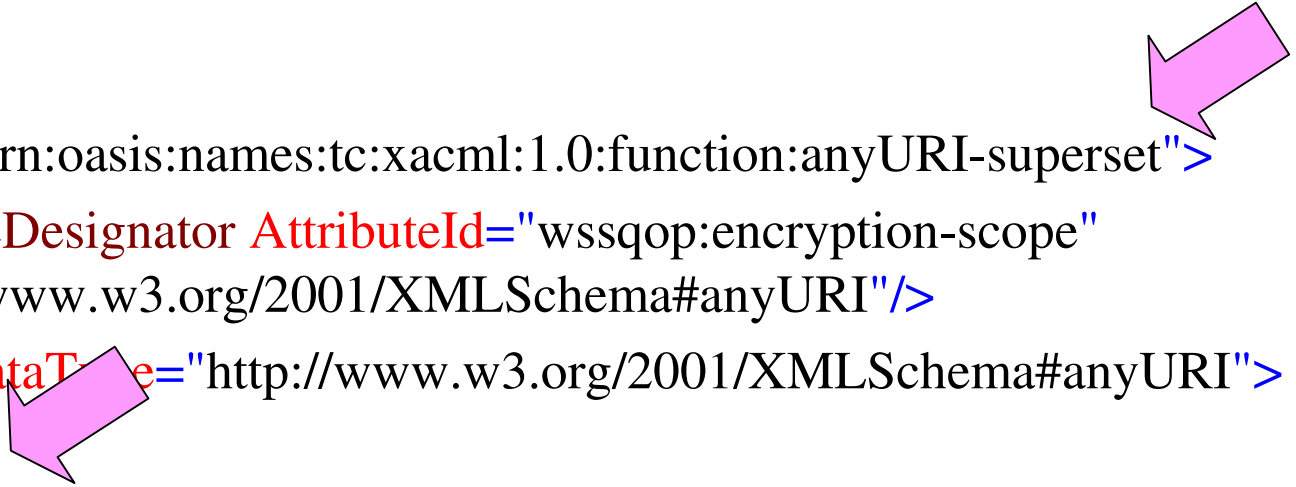
REJECT



```
<Apply FunctionId="urn:oasis:names:tc:xacml:1.0:function:not">  
  <Apply FunctionId="urn:oasis:names:tc:xacml:1.0:function:anyURI-superset">  
    <ResourceAttributeDesignator AttributeId="wssqop:encryption-scope"  
      DataType="http://www.w3.org/2001/XMLSchema#anyURI"/>  
    <AttributeValue  
      DataType="http://www.w3.org/2001/XMLSchema#anyURI">  
      //record/patient/patient-number  
    </AttributeValue>  
  </Apply>  
</Apply>
```


OPTIONAL

```
<Apply FunctionId="urn:oasis:names:tc:xacml:1.0:function:anyURI-superset">  
  <ResourceAttributeDesignator AttributeId="wssqop:encryption-scope"  
    DataType="http://www.w3.org/2001/XMLSchema#anyURI"/>  
  <AttributeValue DataType="http://www.w3.org/2001/XMLSchema#anyURI">  
  
    </AttributeValue>  
  </Apply>
```



Preferences

- Some alternatives may be preferable to others
 - E.g. lower processing cost
- List options in order of preference?

Miscellaneous

- Sequential application of requirements
 - E.g. sign then encrypt the data plus signature
- Attributes identified by name or location
- Policy specifies behaviour in event of unavailable attributes
- Mechanisms for locating and retrieving policies

Summary

- Publish provider-policy for request
- Transfer consumer-policy for response
- Combine provider and consumer policies
- Translate to execution instructions
- Express capabilities as well as requirements
- Express preferences
- Identify result of an execution step
- Use single formal logic system
 - Aids combining, renormalization and analysis