

# **Part 3 - WS-XACML: Authorization and Privacy Policies for Web Services**

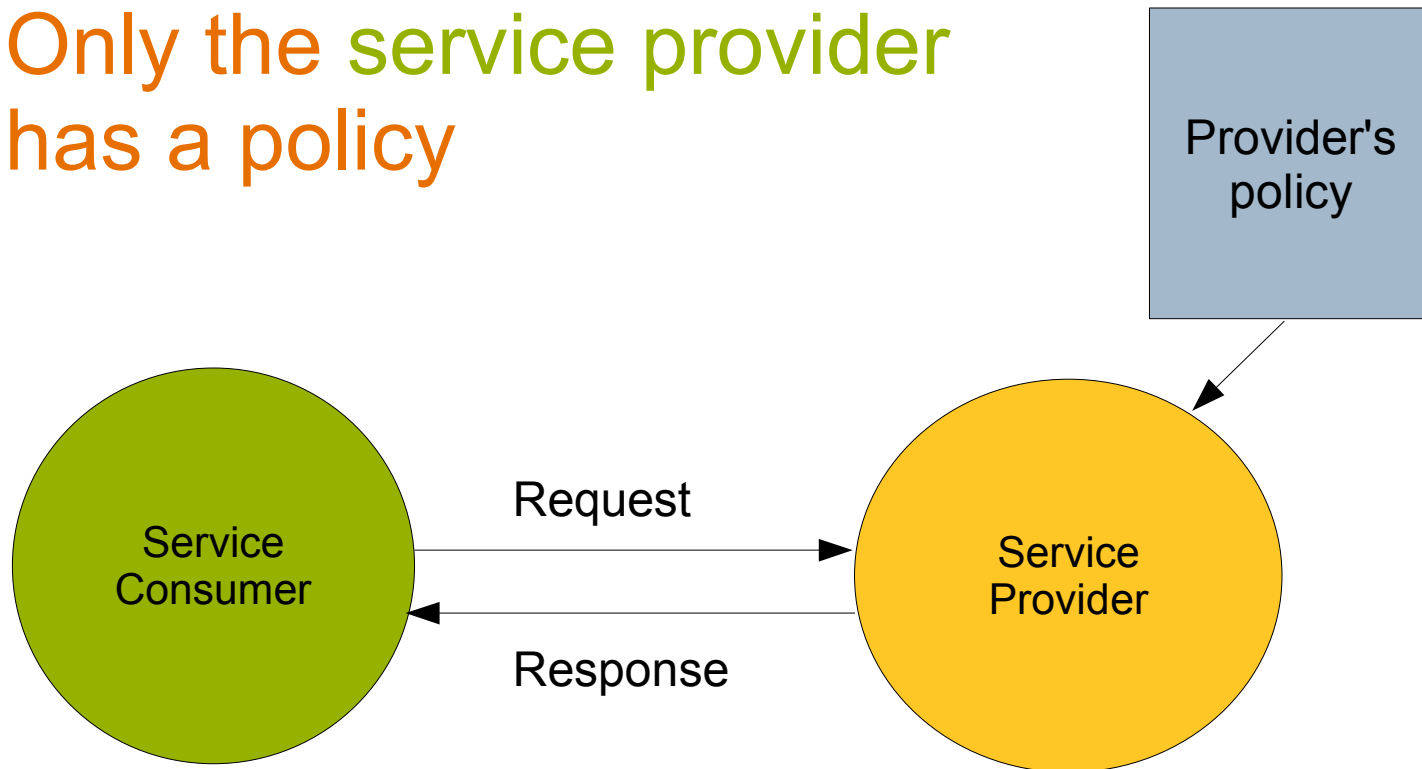
**Anne Anderson, Sun Microsystems**

# Outline

- **Web Services policies are different!**
- **XACML policies for Web Services**
  - WS-XACML policy assertions in general
  - XACMLAuthzAssertion
  - XACMLPrivacyAssertion

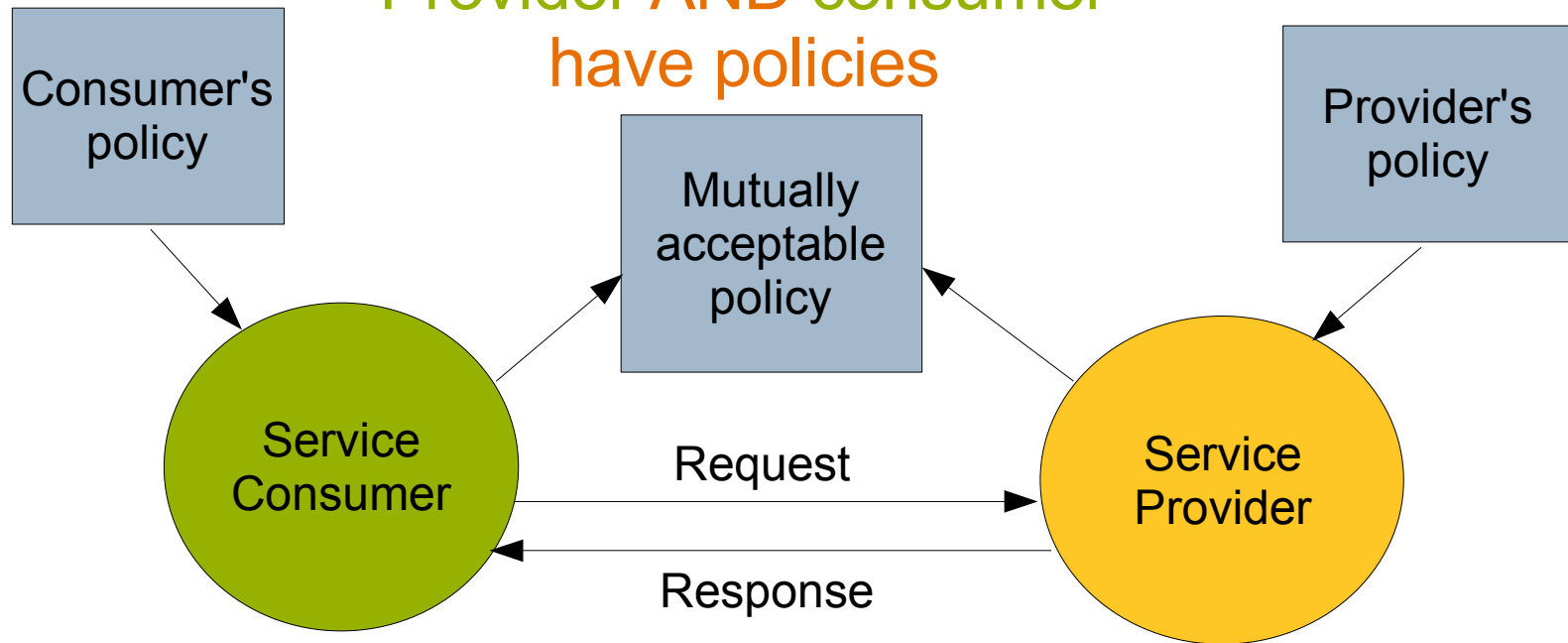
# Typical XACML policy usage

Only the service provider has a policy



# Typical Web Services policy usage

Provider AND consumer  
have policies



They agree on a mutually acceptable policy  
before interacting

# Web Services Policy (WS-Policy)

<Policy>

Reliable messaging assertion

Atomic transactions assertion

Endpoint addressing assertion

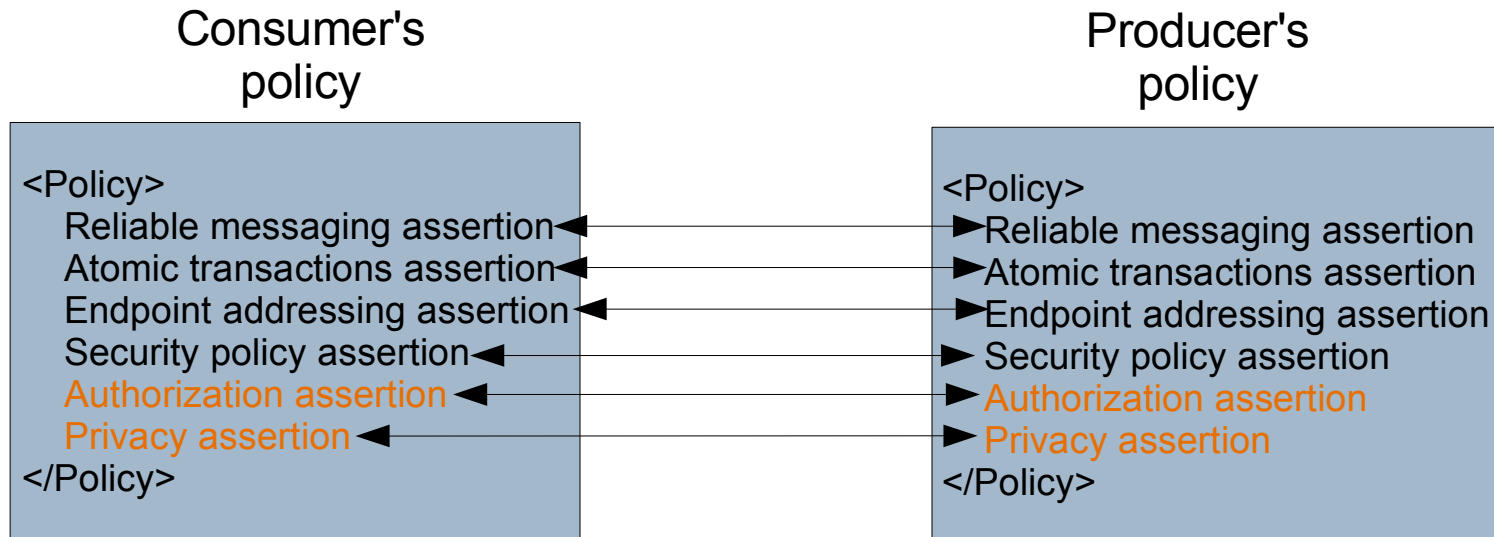
Security policy assertion

Authorization assertion

Privacy assertion

</Policy>

# Web Services Policy (WS-Policy)

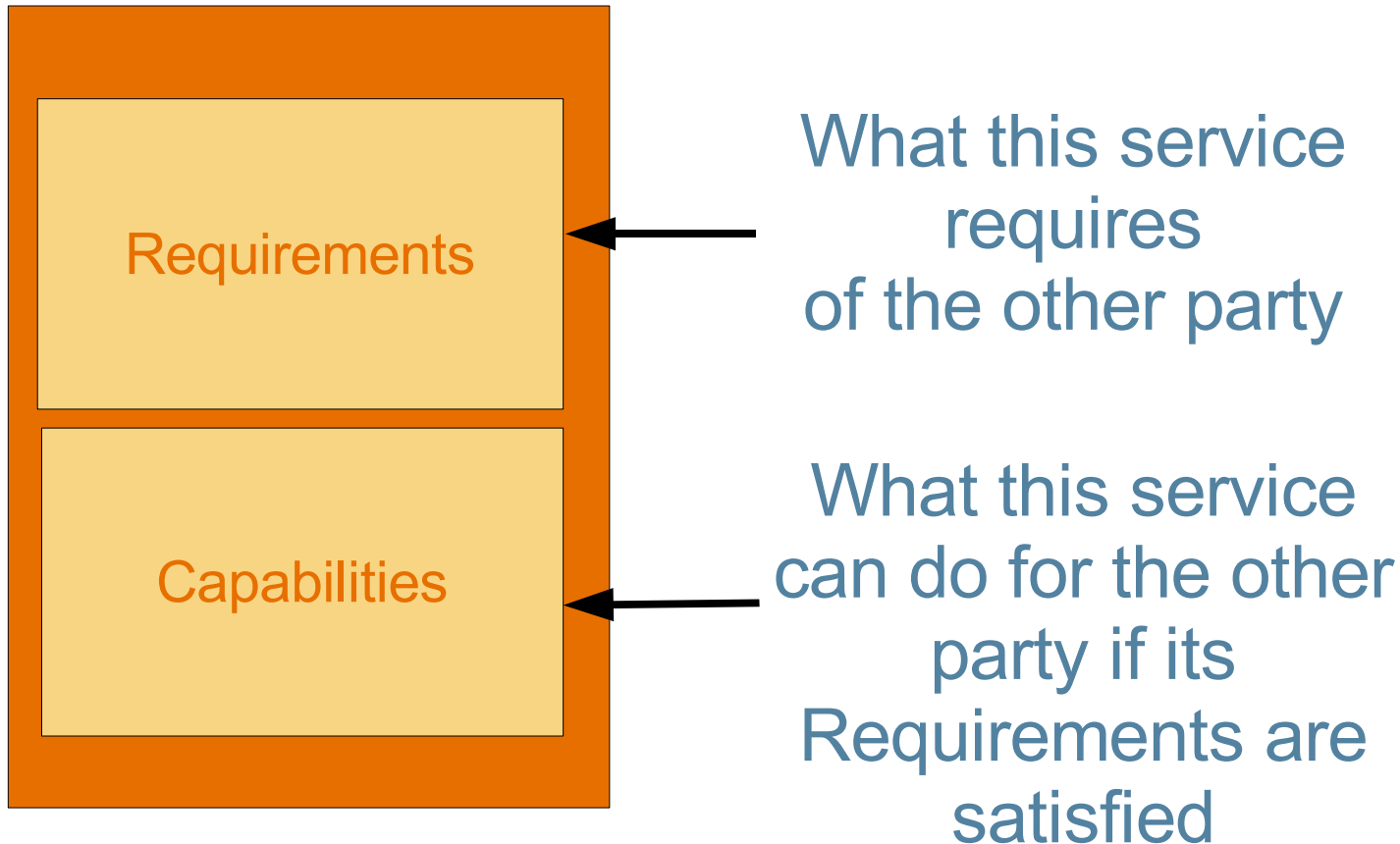


Mutually Acceptable Policy if all assertions match

# Outline

- Web Services policies are different!
- XACML policies for Web Services
  - WS-XACML policy assertions in general
  - XACMLAuthzAssertion
  - XACMLPrivacyAssertion

# WS-XACML assertion format

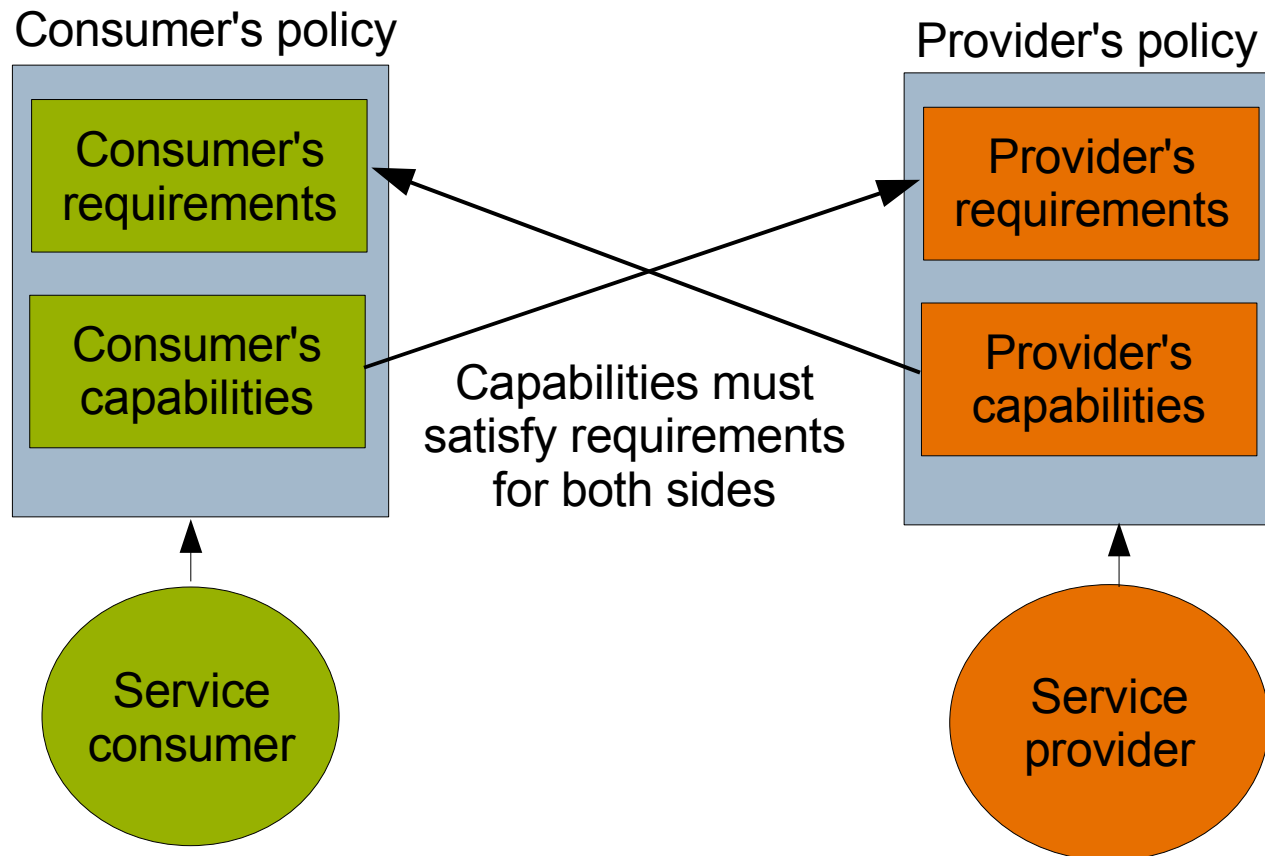




# WS-XACML assertion formats

- Requirements
  - XACML Policy or PolicySet
  - List of XACML “predicates”
- Capabilities
  - XACML Request
  - List of XACML “predicates”
  - XML document
    - Example: W3C P3P policy statement

# WS-XACML assertion matching



# Outline

- Web Services policies are different!
- XACML policies for Web Services
  - WS-XACML policy assertions in general
  - XACMLAuthzAssertion
  - XACMLPrivacyAssertion

# XACMLAuthzAssertion

- Authorization requirements
  - You must have the role of “Manager”,*
  - You must be an OASIS member,*
  - Your attributes must be signed by “TrustyCerts”*
- Capabilities for providing authorization information
  - I can provide attributes signed by “Example Corp.” or “TrustyCerts”*

# XACMLPrivacyAssertion

- Privacy and confidentiality requirements
  - You must not release my personal information to any 3<sup>rd</sup> party,*
  - You may keep my information  $\leq$  30 days*
- Capabilities for providing or protecting private information
  - I can provide my name, and address,*
  - I will not release your price list to any 3<sup>rd</sup> party*

# Frequently Asked Questions

- How is XACMLAuthzAssertion different from WS-SecurityPolicy?
  - *WS-SecurityPolicy: protocol-level security requirements - authentication tokens, encryption, digital signature*
  - *XACMLAuthzAssertion: authorization requirements for accessing the Web Services interface and its associated resources*

# Frequently Asked Questions

- Isn't publication of a service's authorization policy an invitation to security attacks?
  - *A service can publish just a subset of its authorization policy*
  - *Many Web Services WANT clients to know their authorization requirements*
    - *Clients can obtain necessary Attributes*
    - *Incompatible clients can go elsewhere*

# Frequently Asked Questions

- How is XACMLPrivacyAssertion different from W3C's P3P?
  - *P3P: allows a service to publish its user-level privacy policy in a standard format*
  - *XACMLPrivacyAssertion: fits into WS-Policy; can use P3P inside; supports policy agreement, privacy/confidentiality requirements for PII, specific resources or parts of XML documents, data retention limits*



## For more information

- **OASIS XACML TC Web Page**  
[www.oasis-open.org/committees/tc\\_home.php?wg\\_abbrev=xacml](http://www.oasis-open.org/committees/tc_home.php?wg_abbrev=xacml)
- **XACML 2.0 Standard**  
[www.oasis-open.org/committees/tc\\_home.php?wg\\_abbrev=xacml#XACML20](http://www.oasis-open.org/committees/tc_home.php?wg_abbrev=xacml#XACML20)
- ***XACML 3.0 Core, XACML 3.0 Administrative Policy, and XACML Web Services Profile (WS-XACML) Working Drafts***  
[www.oasis-open.org/committees/tc\\_home.php?wg\\_abbrev=xacml#CURRENT](http://www.oasis-open.org/committees/tc_home.php?wg_abbrev=xacml#CURRENT)