IEEE Policy 2004 Workshop
8 June 2004
Comparing WSPL and WS-Policy

Anne Anderson
Staff Engineer
Sun Labs, Burlington, MA
Anne.Anderson@sun.com

Sun microsystems
We make the net work.

“Web services policy”

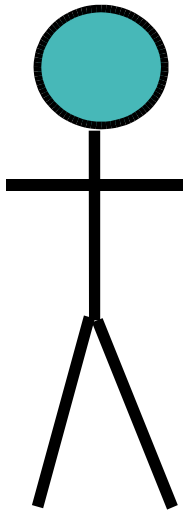
- Definition:

The requirements and abilities of a web service in its interactions with other web services or consumers.

Endpoints in a web services interaction must agree on one set of parameters from the intersection of their policies in order to interact successfully.

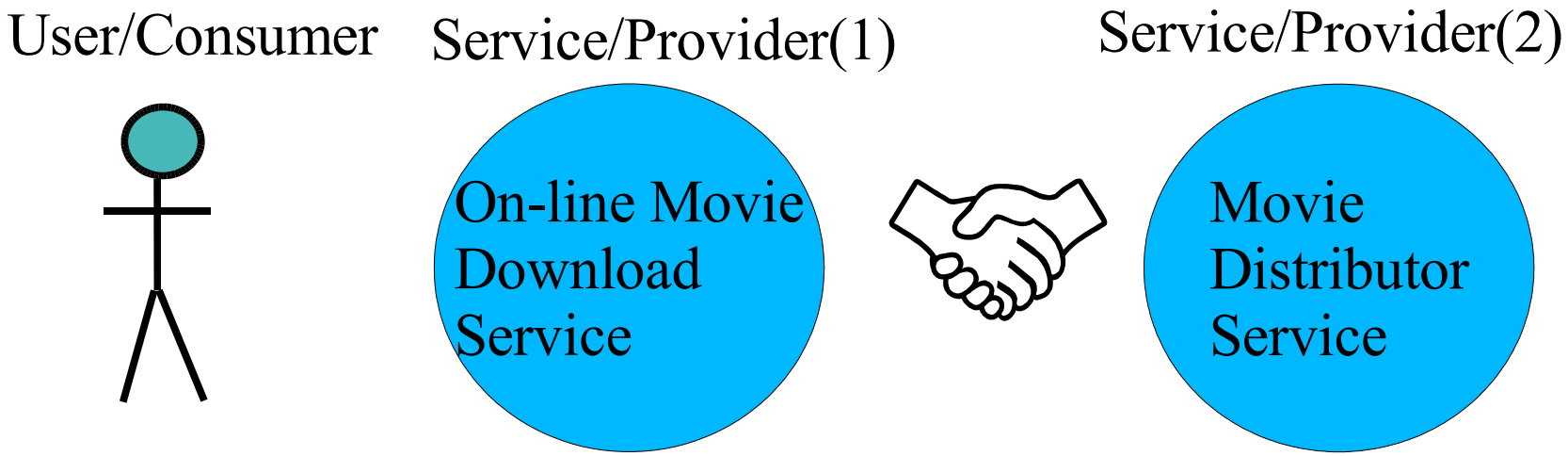
Interaction example

User/Consumer



Service/Provider

Another interaction example



Need to negotiate

Authentication:
- Method
- Algorithms and keys

Privacy:
- Share info?
- Store user info?
- Send ads?

Authorization to
- Subscribe/unsubscribe?
- Download?
- Manage?

Service options
- # of movies/month
- Bandwidth guarantees
- Fee

Possible types of web services policies

- Authentication
- Authorization
- Quality of Protection (QoP)
- Quality of Service (QoS)
- Privacy
- Reliable messaging
- Service-specific options
- …

Negotiation is KEY

- Needed when choices exist
- Both sides have preferences, capabilities, requirements
- Needed to automate service discovery and connection

WS-Policy background

- MS/IBM/BEA/SAP authored
- Actually 3 specifications
  - WS-Policy (Web Services Policy Framework)
  - WS-PolicyAssertions
  - WS-PolicyAttachment
  - Related: WS-SecurityPolicy (security assertions)
- Initial documents: 18 December 2002
- Most recent: 2 June 2003*

*all information as of 2 June 2004

WSPL background

- Based on the OASIS eXtensible Access Control Markup Language (XACML) Standard
- Working draft in the OASIS XACML Technical Committee

WSPL is related to XACML*

- Strict subset of XACML syntax: restricted to Distributive Normal Form
- Different evaluation engines
  - XACML: given a set of Attributes and a Policy, is the set acceptable or not?
  - WSPL: given two Policies, what are the mutually acceptable sets of Attributes?

* OASIS eXtensible Access Control Markup Language Standard

WS-Policy example*

```
<Policy>
    <ExactlyOne>
        <SecurityToken Usage="Required">
            <TokenType>Kerberosv5TGT</TokenType>
        </SecurityToken>
        <SecurityToken Usage="Required">
            <TokenType>X509v3</TokenType>
        </SecurityToken>
    </ExactlyOne>
</Policy>
```

*Based on example in WS-Policy specification v1.1

WS-Policy basic features*

- Operators (can be nested)
  - All, ExactlyOne, OneOrMore
- Assertions
  - Simple or complex XML schema elements
- Assertion “usage qualifiers”
  - Required, Optional, Rejected, Observed, Ignored
- Assertion “preference”
  - Preference weighting
  - Example: Preference=”100”

*All information as of 27 May 2004

Equivalent WSPL Example

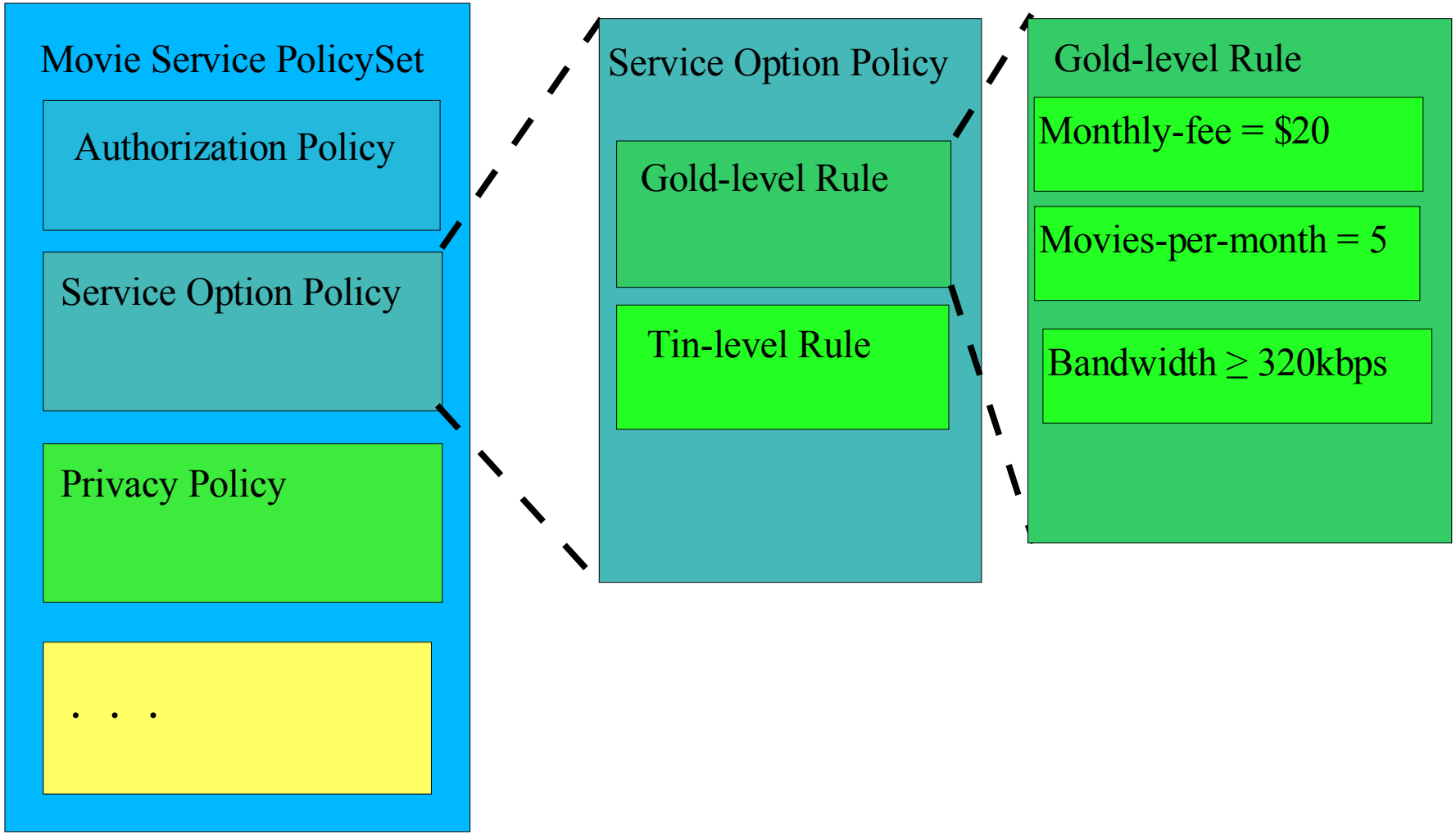
```
<Policy PolicyId="policy:1" RuleCombiningAlgorithm="&permit-overrides;">
  <Rule RuleId="rule:1" Effect="Permit">
    <Condition FunctionId="&function;string-is-in">
      <AttributeValue DataType="&string;">Kerberosv5TGT</AttributeValue>
      <ResourceAttributeDesignator AttributeId="&SecurityToken;"
                                   DataType="&string;"/>
    </Condition>
  </Rule>
  <Rule RuleId="rule:2" Effect="Permit">
    <Condition FunctionId="&function;string-is-in">
      <AttributeValue DataType="&string;">X509v3</AttributeValue>
      <ResourceAttributeDesignator AttributeId="&SecurityToken;"
                                   DataType="&string;"/>
    </Condition>
  </Rule>
</Policy>
```

*"&function;string-is-in" is defined in XACML; not currently included in WSPL working draft

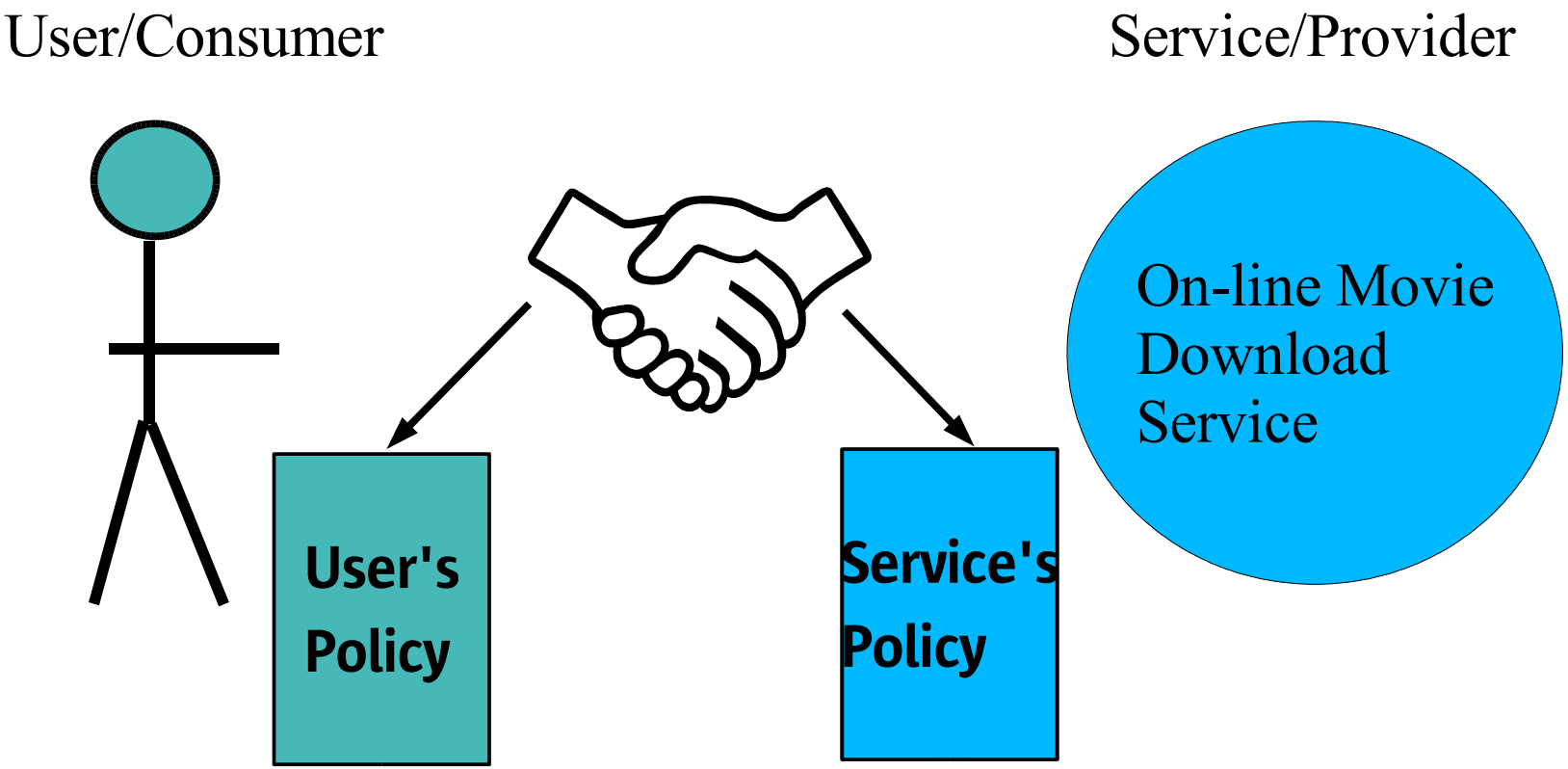
WSPL basic features

- Policy
  - Set of <Rule>s
  - <Rule> = One set of acceptable policy attribute values
  - Distributive Normal Form (“or” <Rule>s of “and” predicates)
- Operators
  - Comparison between an attribute of the policy and a value
  - Comparison between two attributes of the policy
  - -equal,-greater-than,-greater-than-or-equal,...,set-equals,subset
  - Primitive datatypes: integer, string, X500Name, date, ...
- Rule preferences
  - 1st <Rule> has highest preference, 2nd <Rule> has next highest...

WSPL policy diagram

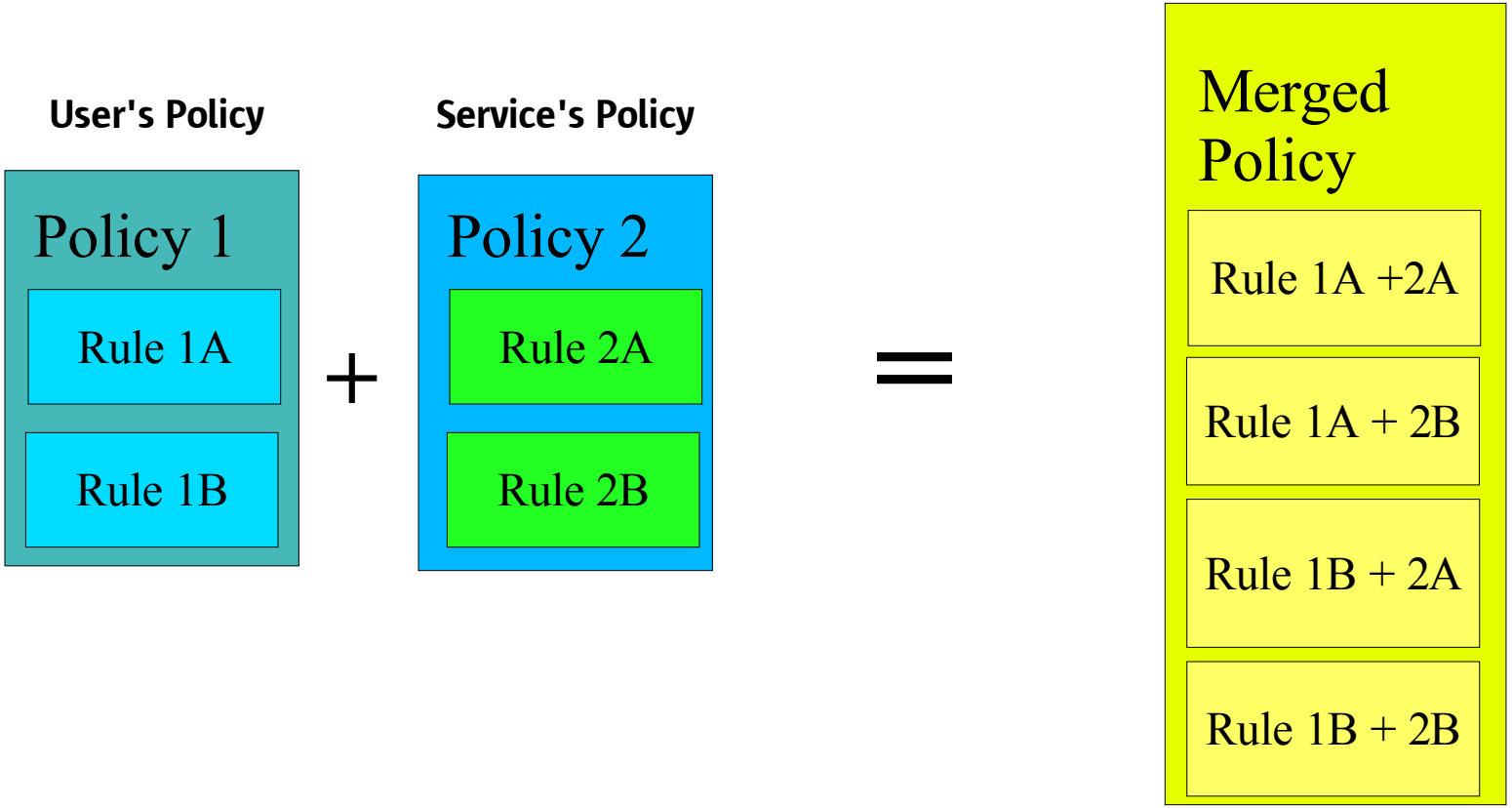


WSPL Policy Negotiation



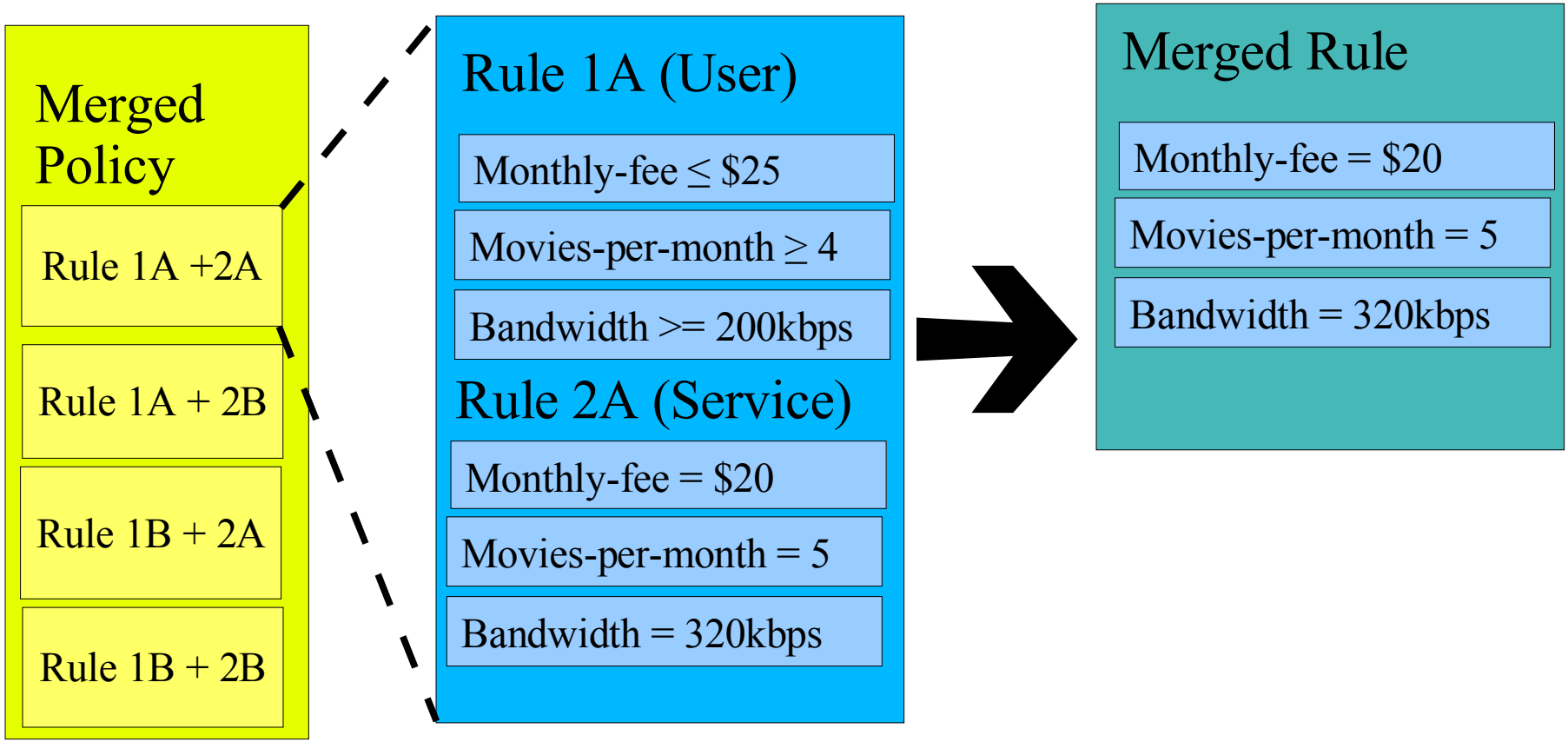
Policy negotiation (1)

- Pair rules in all possible combinations



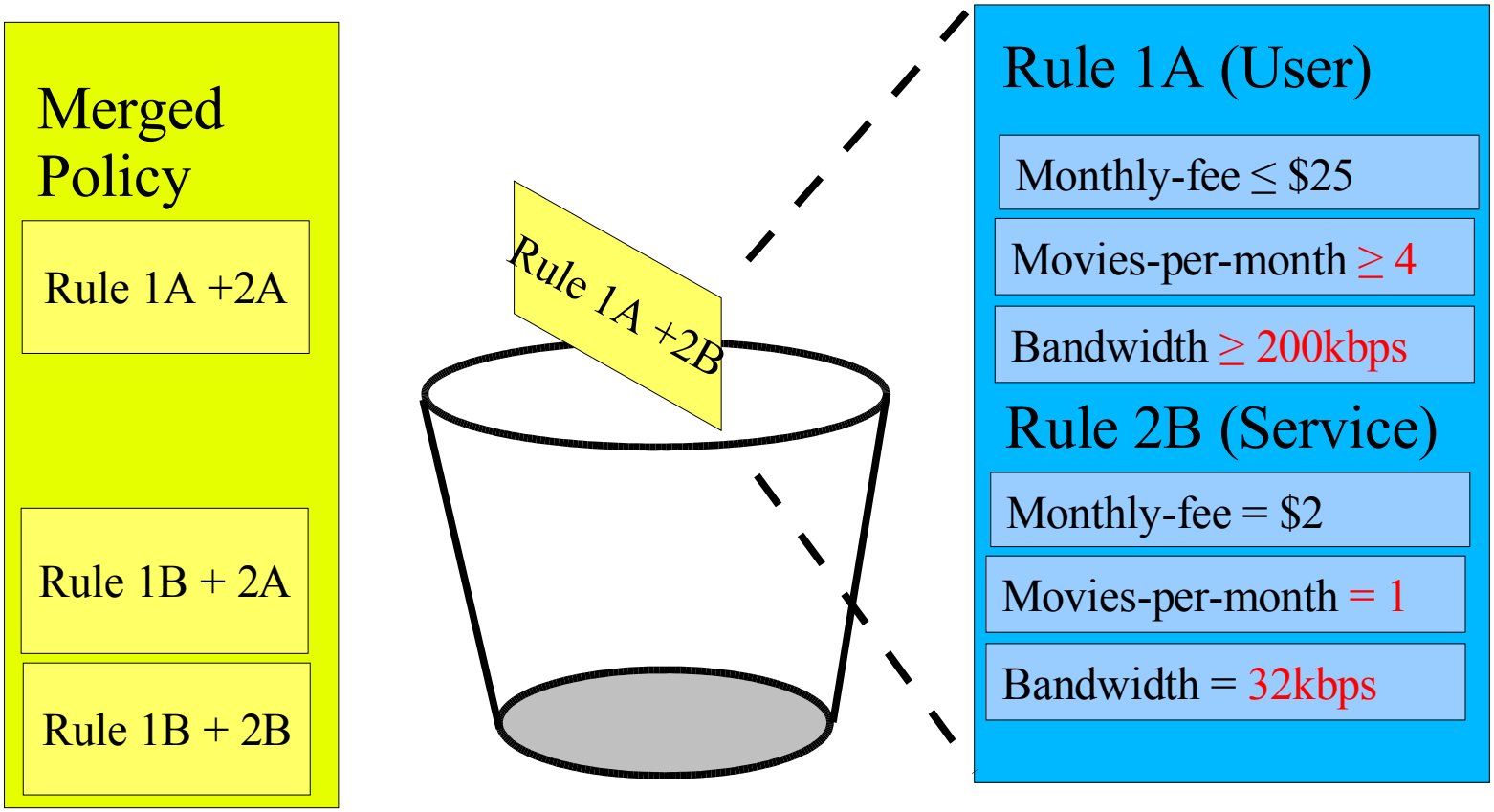
Policy negotiation (2)

- Merge rules



Policy merging (3)

- Eliminate incompatible rules



Policy merging (4)

- Eliminate unusable rules

Example:

Current time of day:

timeOfDay == 6pm

Rule says:

timeOfDay ≥ 9am

timeOfDay ≤ 5pm

WS-Policy issues: Technical

No support for negotiation*

- No merge algorithm specified, just flattening
- Only exact “match” of entire Assertion
- Negotiation of preferences not specified
- Canonicalization not specified

WSPL: negotiation fully supported

- Fully specified
- Exact matches or value-range matches
- Negotiation of preferences specified
- Canonicalization specified

*All information as of 2 June 2004

WS-Policy issues: Technical

Usage flags conflict with operators*

E.g. <ExactlyOne>
Value=A Usage="required",
Value=B Usage="required",
</ExactlyOne>

Puts policy into Assertions

WSPL: logically consistent

- Based on XACML, whose semantics have been formally analyzed
- Benefits from XACML usage experience

*All information as of 2 June 2004

WS-Policy issues: Technical

No assertion comparison functionality*

- Must specify every value for a fine-grained Assertion
- Examples: IP-Address, $, time of day

WSPL: rich set of comparison operators

- Examples: time of day > 9am, fee >= 25

*All information as of 2 June 2004

WS-Policy issues: Usage*

No licensing terms

- WSPL is Royalty Free

Completely dependent on extensions

- Could be proprietary, could have onerous license terms
- WSPL designed not to need extensions
- WSPL uses standard data types and operations
- WSPL can be extended via new names

Requires custom evaluation engines

- WSPL supports one standard engine

*All information as of 2 June 2004

WSPL issues: Usage*

Verbose

- But you get the comparison functionality
- Policy authoring tools could make this a non-issue

Access control terms like “Permit”

- But you can re-use most of an XACML implementation
- Policy authoring tools could make this a non-issue

*All information as of 2 June 2004

WS-Policy issues: standardization*

- Not submitted to any standards body
- Not developed in any standards group
- Not based on any approved standards
- No public requirements specification
- No public review and comment
- No license terms specified

*All information as of 2 June 2004

WSPL Standardization Status

- Working draft in OASIS XACML TC
- Based on OASIS XACML Standard
- Public review and comment
- Royalty free
- Requirements Specification developed with public input and review

WS-Policy + WSPL: best of both?

- Work in an open standards group
  - Incl. public requirements specification and review
- Add to WS-Policy
  - Comparison operators
  - Standard data types
  - Canonicalization algorithm
  - Procedure for negotiation
  - Specify negotiation of preferences
- Remove from WS-Policy
  - “Usage” attribute

References

- ***XACML profile for Web-services*** (also known as WSPL), Tim Moses, ed., OASIS XACML TC Working Draft 04, 29 Sep 2003 , http://www.oasis-open.org/committees/download.php/3661/draft-xacml-wspl-04.pdf
- ***Web-services policy language use-cases and requirements***, Tim Moses, ed., OASIS XACML TC Working Draft 04, 16 April 2003, http://www.oasis-open.org/committees/download.php/1608/wd-xacml-wspl-use-cases-04.pdf
- ***Web Services Policy Framework (WS-Policy)***, Maryann Hondo, Chris Kaler, eds., Version 1.01, 2 June 2003, http://www.ibm.com/developerworks/library/ws-polfram/
- ***Web Services Policy Attachment (WS-PolicyAttachment)***, Maryann Hondo, Chris Kaler, eds., Version 1.1, 28 May 2003, http://www.ibm.com/developerworks/library/ws-polat/
- ***Web Services Policy Assertions Language (WS-PolicyAssertions)***, Anthony Nadalin, ed., Version 1.01, 2 June 2003, http://www.ibm.com/developerworks/library/ws-polas

All references are to the most recent versions available as of 2 June 2004.

Further Information

Sun's open source XACML implementation

http://sunxacml.sourceforge.net/

Danfeng Yao's WSPL prototype and demo

http://www.cs.brown.edu/people/dyao/wspl.html

OASIS XACML Technical Committee web page

http://www.oasis-open.org/committees/xacml

Anne Anderson <Anne.Anderson@sun.com>