eXtensible Access Control Markup Language (XACML)

Anne Anderson

Sun Microsystems, Inc.

GSA Identity Workshop 27 Feb 2007

Outline

- **Introduction to XACML**
- XACML 3.0: Coming soon!
  - Administrative Policy and Delegation
  - XACML policy assertions

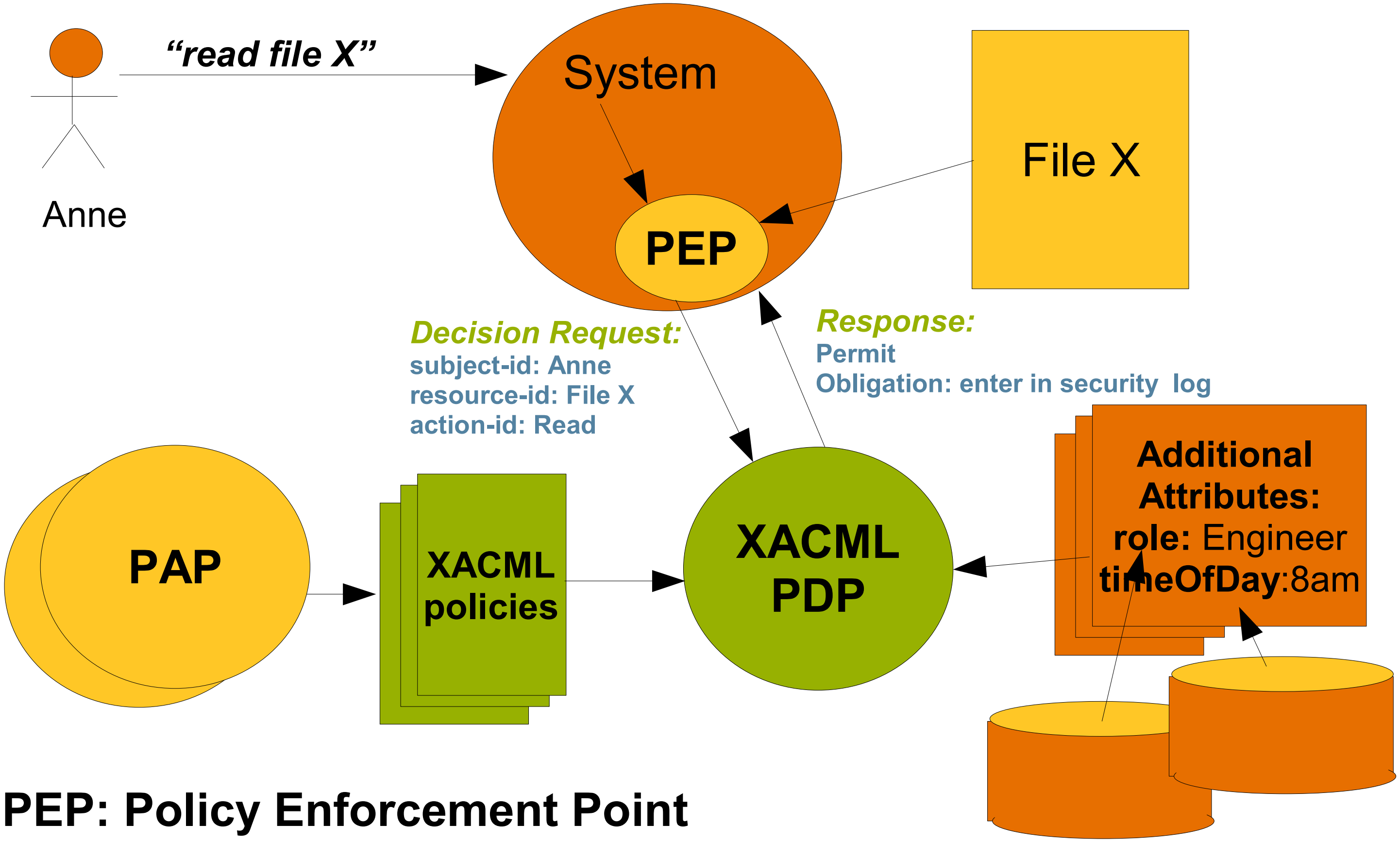
What is XACML?

- “eXtensible Access Control Markup Language”
  - Pronounced “X-akamull”, “X-A-C-M-L”, “zakamull”
- Language for describing authorization and privacy policies in XML
  - Once identity is authenticated, what can the identity do?
  - WHO
    can have access to WHAT,
    under which CONDITIONS,
    for which PURPOSES
- OASIS and ITU-T Standard

Why use XACML?

- Standard policy format
  - Share highly expressive policies across applications
  - Ease of use; common policy authoring and management tools
  - Maintain policy consistency
  - Auditing
- XML document access control
  - “Permit read if user is the patient named in the record”
- Control access to any type of resource
  - Not just for XML documents

How Does XACML Work?



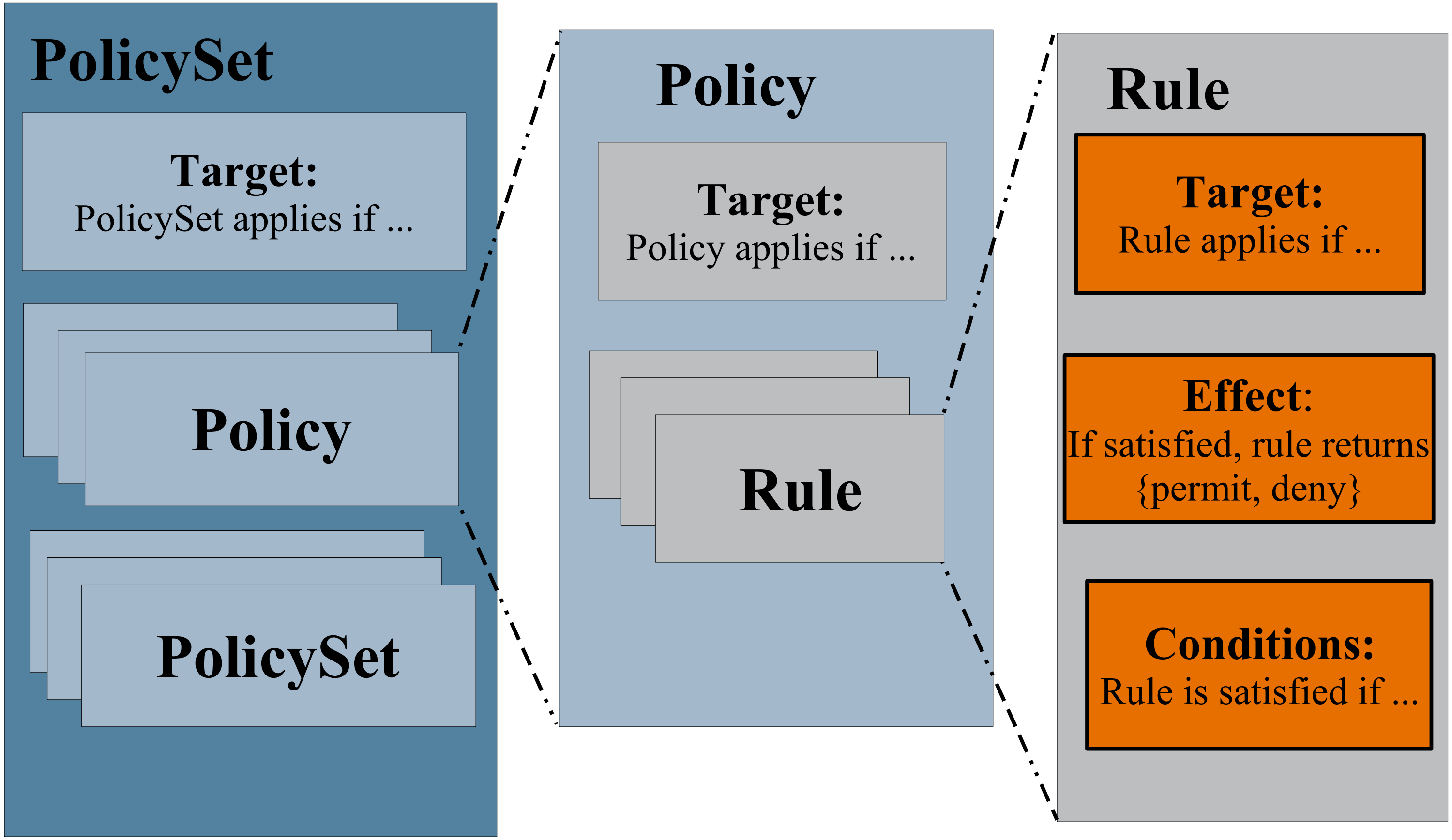
Decision Request:
subject-id: Anne
resource-id: File X
action-id: Read

Response:
Permit
Obligation: enter in security log

Repositories, Attribute Authorities, etc.

PEP: Policy Enforcement Point
PDP: Policy Decision Point
PAP: Policy Administration Point

XACML Policy Structure



PolicySet

Target:
PolicySet applies if ...

Policy

PolicySet

Policy

Target:
Policy applies if ...

Rule

Rule

Target:
Rule applies if ...

Effect:
If satisfied, rule returns {permit, deny}

Conditions:
Rule is satisfied if ...

A Simple XACML Rule

```
<Rule   Effect ="Permit">

    <Target>
           File X
    </Target>

    <Condition>
        <Apply FunctionId="AND">
           Role="Engineer",
           Action="Read",
           Time ≥ 8am,
           Time ≤ 5pm
        </Apply>
  </Condition>

</Rule>
```

Target can depend on Subject, Resource, Action, ...

Condition can use ~100 std functions, may be nested

Outline

- Introduction to XACML
- XACML 3.0: Coming soon!
  - **Administrative Policy and Delegation**
  - XACML Policy Assertions

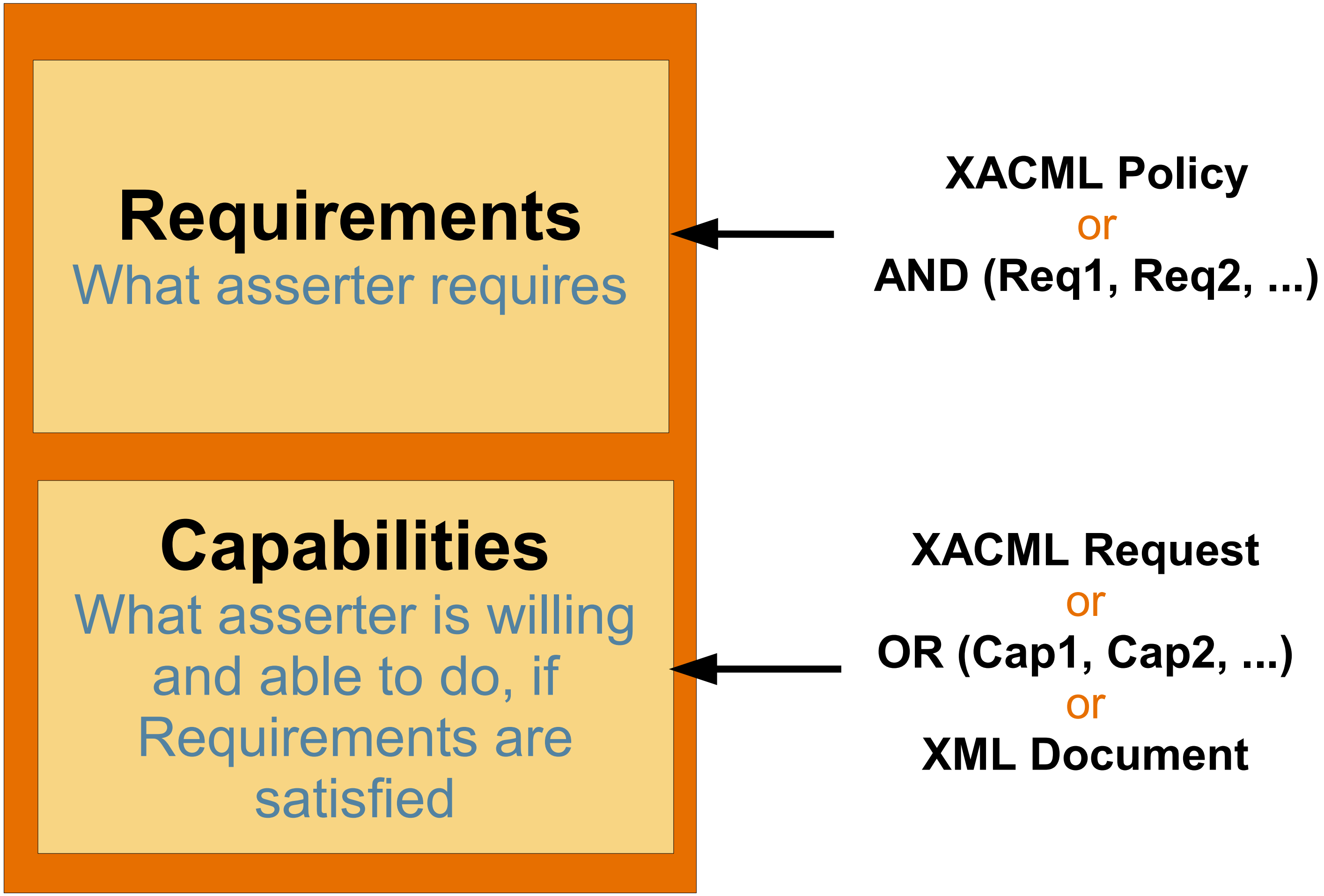
XACML 3.0:
Administrative Policy and Delegation

- Administrative Policy
  - > Who is allowed to write policies about what
- Delegation
  - > Allowing someone else to do something you are allowed to do

XACML 3.0:
XACML Policy Assertions (WS-XACML)

- Format for “published” Web Services XACML policies
- Consumers can match against their Assertions
- Can be used in a W3C WS-Policy
- Current XACML Assertion Types:
  - XACMLAuthzAssertion: Authorization policies
  - XACMLPrivacyAssertion: Privacy policies

XACMLAssertionAbstractType



Requirements

What asserter requires

Capabilities

What asserter is willing and able to do, if Requirements are satisfied

XACML Policy

or

AND (Req1, Req2, ...)

XACML Request

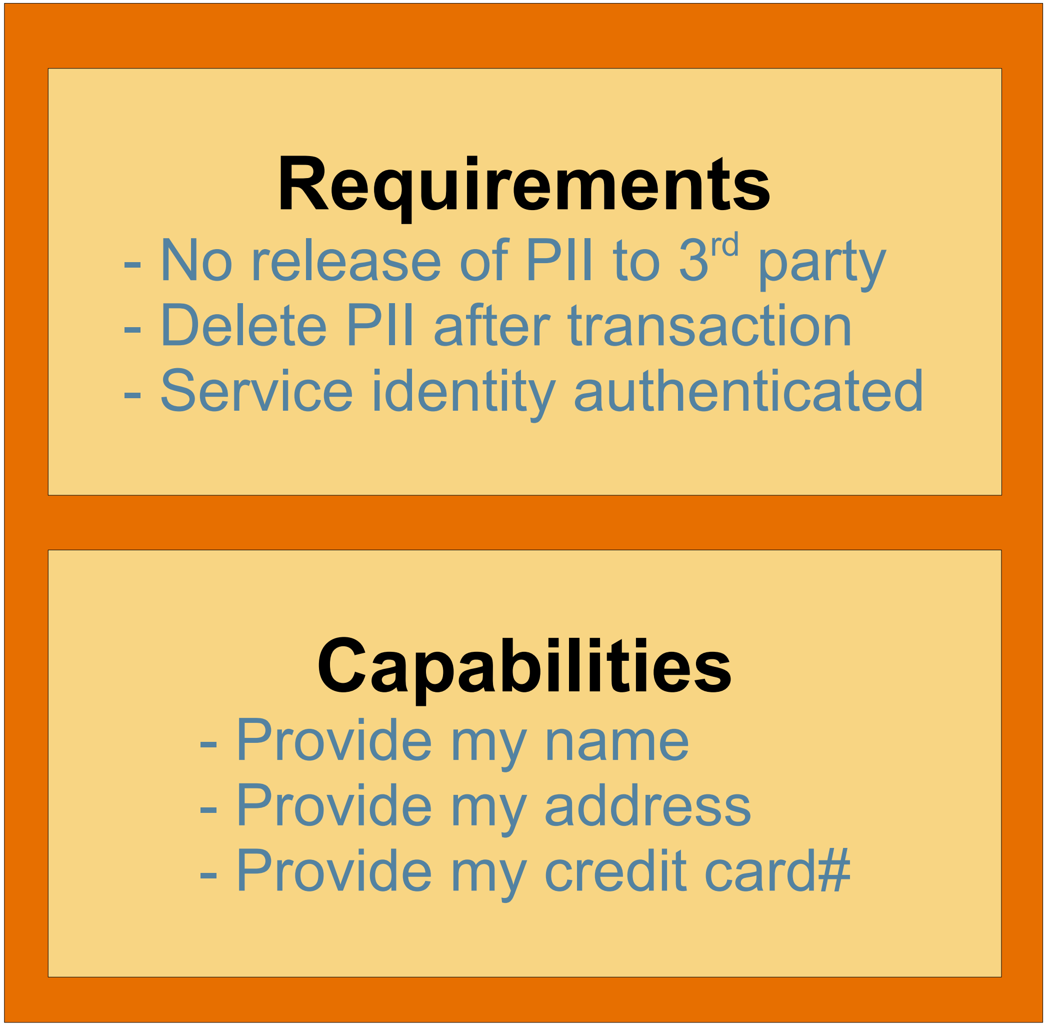
or

OR (Cap1, Cap2, ...)

or

XML Document

XACMLPrivacyAssertion Example



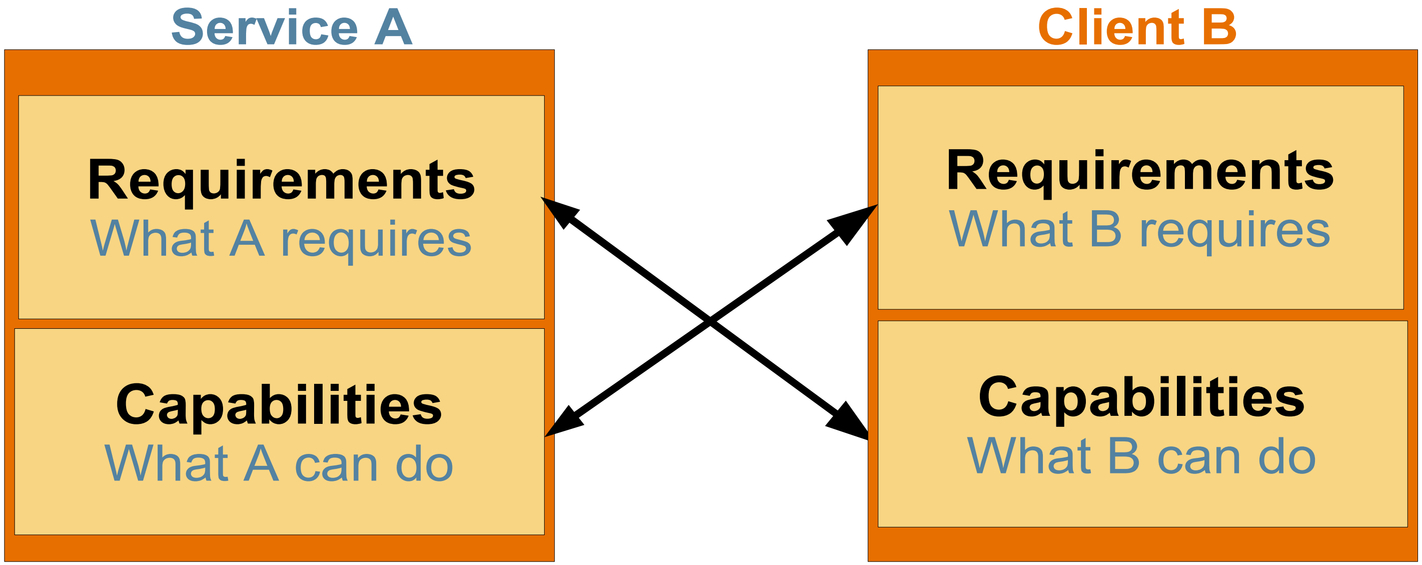
Requirements

- No release of PII to 3rd party
- Delete PII after transaction
- Service identity authenticated

Capabilities

- Provide my name
- Provide my address
- Provide my credit card#

XACML Assertion Matching



Service A is satisfied if B's Capabilities satisfy A's Requirements.
Client B is satisfied if A's Capabilities satisfy B's Requirements.

Each can supply only the minimum necessary Capabilities.

XACML

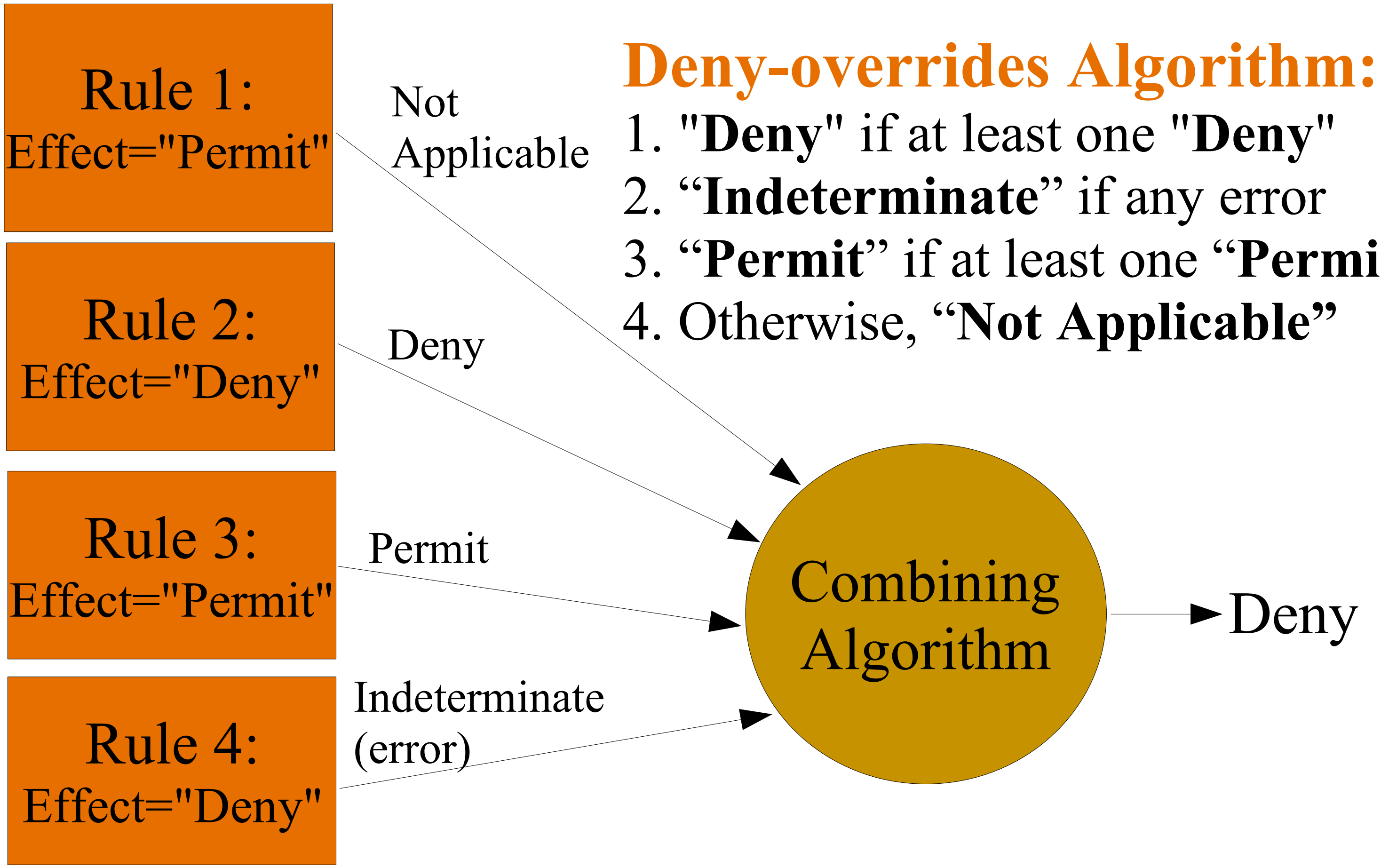
Questions?

XACML References

[1] *eXtensible Access Control Markup Language (XACML)*, OASIS XACML Technical Committee, all versions and profiles, http://www.oasis-open.org/committees/xacml

[2] *Web Services Profile of XACML (WS-XACML) Version 1.0*, Working Draft 8, 12 December 2006, OASIS XACML Technical Committee, http://www.oasis-open.org/committees/download.php/21490/xacml-3.0-profile-webservices-spec-v1.0-wd-8-en.pdf

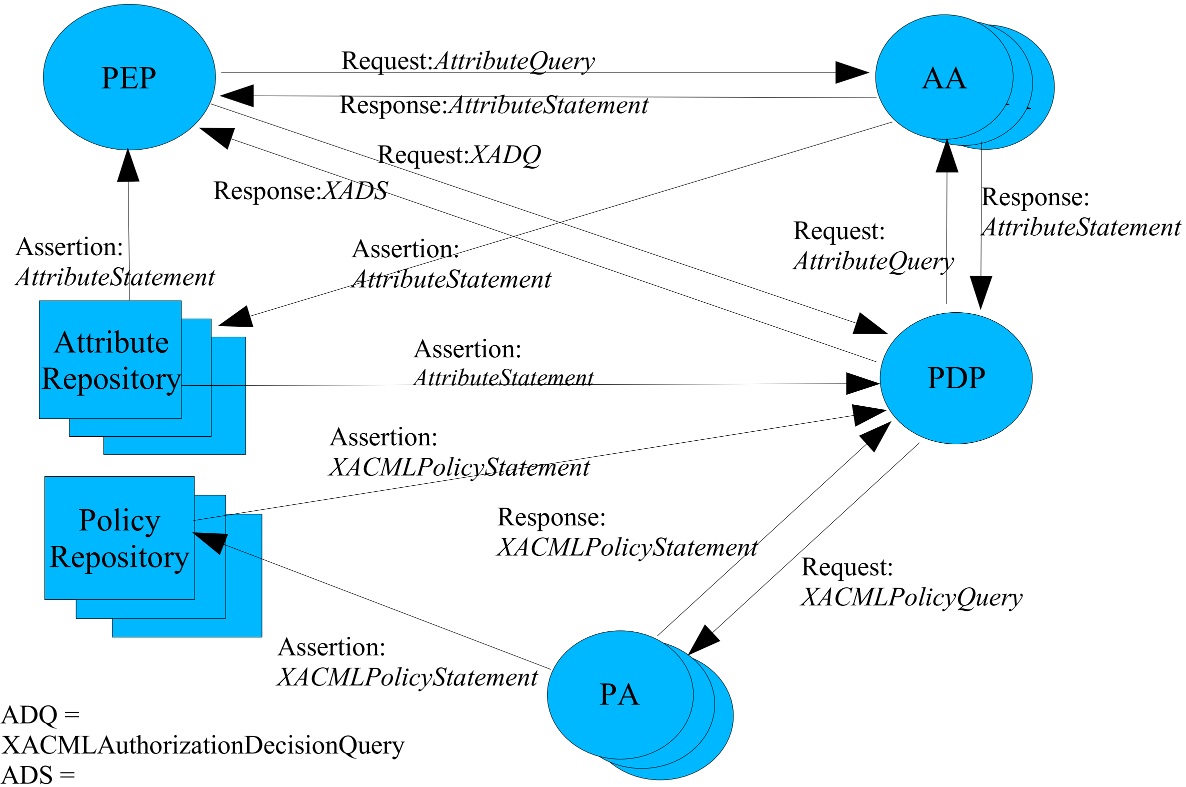
Combining Algorithm Example



Deny-overrides Algorithm:

1. "**Deny**" if at least one "**Deny**"
2. “**Indeterminate**” if any error
3. “**Permit**” if at least one “**Permit**”
4. Otherwise, “**Not Applicable**”

XACML and SAML



XADQ =
XACMLAuthorizationDecisionQuery
XADS =
XACMLAuthorizationDecisionStatement

eXtensible Access Control Markup Language (XACML)

Anne Anderson

anne.anderson@sun.com