Privacy & Access control

2024/25 Q2

Jaime Delgado

DAC - UPC

DMAG
DISTRIBUTED MULTIMEDIA APPLICATIONS GROUP

Security in Internet Applications

- Security in application layer protocols
- XML and security
- Specific security protocols for the Web
- Privacy and access control

Security in Internet Applications

- ~~Security in application layer protocols~~
- ~~XML and security~~
- ~~Specific security protocols for the Web~~
- **Privacy and access control**

Privacy and Access Control

- Privacy basic concepts
- Access Control mechanisms
- Privacy policies expresssion: XACML

Privacy and Access Control

- **Privacy basic concepts**
- Access Control mechanisms
- Privacy policies expresssion: XACML

Privacy

- Personally Identifiable Information (PII) in digital form
  - Social Networks
  - Public Institutions (i.e. health organizations, etc.)
  - …
- How to control access to this information?
  - Privacy policies/rules, XACML
  - Privacy controls (organizational, physical and technical measures) to treat risks
  - Enforcement, Protection, Access control
  - → *PETs (Privacy Enhancing Technologies)*

Datos que vulneran la privacidad de la persona, que sea identificable

nos centraremos en este, ayuda a proteger la privacidad.

PET (Privacy Enhancing Technology)

(definition in ISO/IEC 29100)

Privacy control, consisting of information and communication technology (ICT) measures, products, or services that protect privacy by eliminating or reducing **personally identifiable information (PII)** or by preventing unnecessary and/or undesired processing of PII, all without losing the functionality of the ICT system

NOTE 1. Examples of PETs include, but are not limited to, anonymization and pseudonymization tools that eliminate, reduce, mask or de-identify PII or that prevent unnecessary, unauthorized and/or undesirable processing of PII.

NOTE 2. Masking is the process of obscuring elements of PII.

Privacy actors: Scenarios

a) Principal provides PII to controller, *e.g. service registration*

b) Controller provides PII to processor, which processes it on behalf of controller, *e.g. outsourcing agreement*

c) Principal provides PII to processor, which processes it on behalf of controller

d) Controller provides PII to principal, as this PII is related to the principal, *e.g. on principal request*

e) Processor provides PII to principal, *e.g. directed by controller*

f) Processor provides PII to controller, *e.g. after performing a requested service*

g) Controller provides PII to a third party, *e.g. related to a business agreement*

h) Processor provides PII to a third party, *e.g. directed by controller*

From ISO/IEC 29100

Privacy actors: Interactions

Scenario/ actor	Principal	Controller	Processor	Third party
a	Provider	Recipient		
b		Provider	Recipient	
c	Provider		Recipient	
d	Recipient	Provider		
e	Recipient		Provider	
f		Recipient	Provider	
g		Provider		Recipient
h			Provider	Recipient

From ISO/IEC 29100

Privacy standards (1/2)

- ISO/IEC **29100**:2011 Information technology — Security techniques — Privacy framework (*withdrawn*)

- Edition 2 available (ISO/IEC 29100:2024): ISO/IEC 29100:2024 Information technology — Security techniques — **Privacy framework**

ISO/IEC 29100 - Privacy principles

- Consent and Choice
- Purpose legitimacy and specification
- Collection limitation
- Data minimization
- Use, retention and disclosure limitation
- Accuracy and quality
- Openness, transparency and notice
- Individual participation and access
- Accountability
- Information Security
- Privacy compliance

Privacy standards (2/2)

- ISO/IEC **27701**:2019 Security techniques — Extension to ISO/IEC 27001 and ISO/IEC 27002 for privacy information management — Requirements and guidelines

  Published (Edition 1, 2019)

- Edition 2 coming in 2024:

  Information security, cybersecurity and privacy protection — Privacy information management systems — **Requirements and guidance**

Privacy standards - ISO/IEC 27701

Implementation guidance for PII Controllers and PII processors

- Implementation guidance for PII controllers
- Implementation guidance for PII processors
- Implementation guidance for PII controllers and PII processors

Privacy standards - ISO/IEC 27701

Implementation guidance for PII controllers

- Conditions for collection and processing
- Obligations to PII principals
- Privacy by design and by privacy default
- PII sharing, transfer and disclosure

…

Privacy

- Protect PII (*Personally Identifiable Information*)
- Follow Legislation (GDPR, …), Guidelines, Risk analysis, …
- Specify Policies / Rules
- Expression mechanisms: XACML, …
- Enforcement (protocols and formats)

→ ACCESS CONTROL

Privacy and Access Control

- ~~Privacy basic concepts~~
- **Access Control mechanisms**
- Privacy policies expresssion: XACML

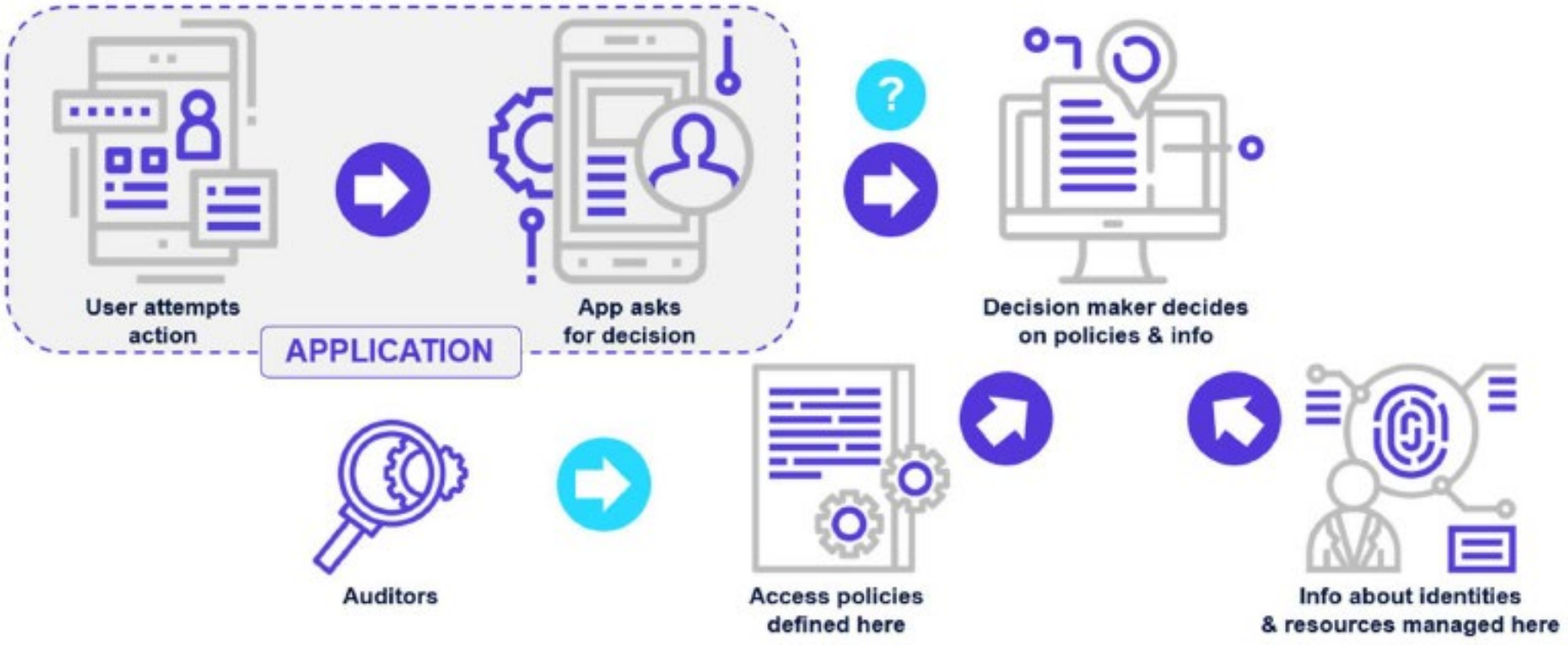
Access control

- Decision Making Process of applications
- Types of Access Control systems
- RBAC
- ABAC
- Others

Decision Making Process of applications (locally)

From "A Guide to Authorization" WHITEPAPER | MARCH 2021, Patrick Parker, CEO EmpowerID

Decision Making Process of applications (external)



From "A Guide to Authorization" WHITEPAPER | MARCH 2021, Patrick Parker, CEO EmpowerID

Decision Making Process of applications (model)

From "A Guide to Authorization" WHITEPAPER | MARCH 2021, Patrick Parker, CEO EmpowerID

Decision Making Process of applications (model)

From “A Guide to Authorization” WHITEPAPER | MARCH 2021, Patrick Parker, CEO EmpowerID

Types of Access Control systems

- Discretionary Access Control (DAC)
- Mandatory Access Control (MAC)
- Role-Based Access Control (RBAC)
- Attribute Based Access Control (ABAC)
- Policy-Based Access Control (PBAC)

Types of Access Control systems

- Discretionary Access Control (DAC)
  - Restricting access to objects based on the identity of the subject (the user or the group to which the user belongs)
  - Implemented using access control lists
  - It is discretionary in the sense that subjects can manipulate it, because the owner of a resource, in addition to the security administrator, can identify who can access the resource and with what authority

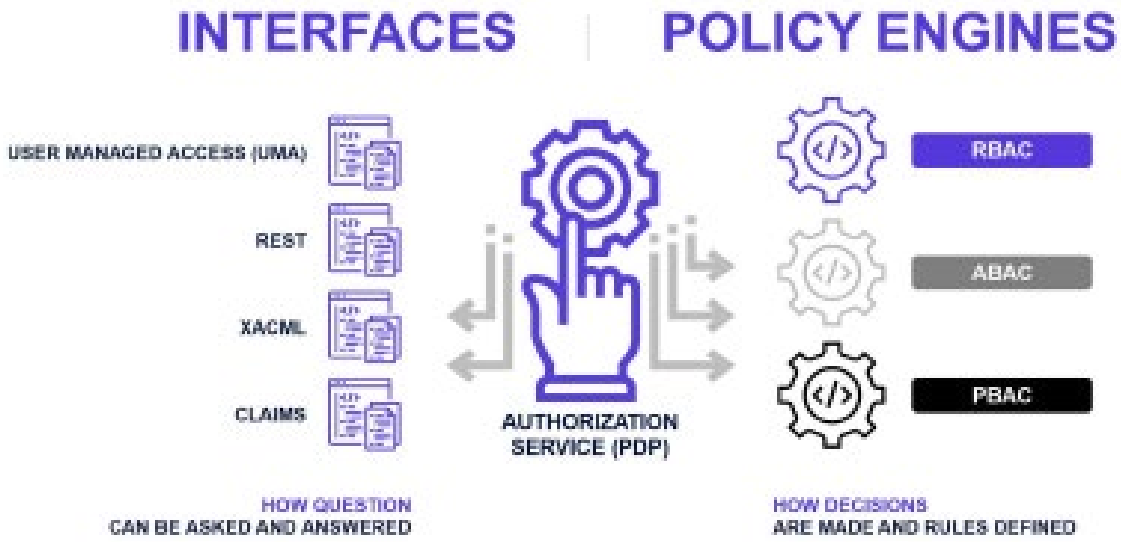
Types of Access Control systems

- Mandatory Access Control (MAC)
  - Method of limiting access to resources based on sensitivity of the information and authorization of the user to access information with that level of sensitivity. (*https://www.ibm.com/docs/en/zos*)
  - Sensitivity defined with a **security label**:
    - security level (level or hierarchical classification, f.e. *Restricted, Confidential, Internal*)
    - security categories (to which the information belongs). Users can access only the information in a resource to which their security labels entitle them.

Types of Access Control systems

- Discretionary Access Control (DAC)
- Mandatory Access Control (MAC)
- Role-Based Access Control (RBAC)
- Attribute Based Access Control (ABAC)
- Policy-Based Access Control (PBAC)

Query interfaces vs. PDP policy models



From "A Guide to Authorization" WHITEPAPER | MARCH 2021, Patrick Parker, CEO EmpowerID

Decision Making Process of applications (model) - REPEATED

From “A Guide to Authorization” WHITEPAPER | MARCH 2021, Patrick Parker, CEO EmpowerID

RBAC

- Role-Based Access Control
- ANSI standard 2004 (model in 1992)
- **Current standard (2012)**
- INCITS 359-2012, **Information Technology -- Role-Based Access Control** (May 29, 2012)

- ***Subject – Role – Permission*** model

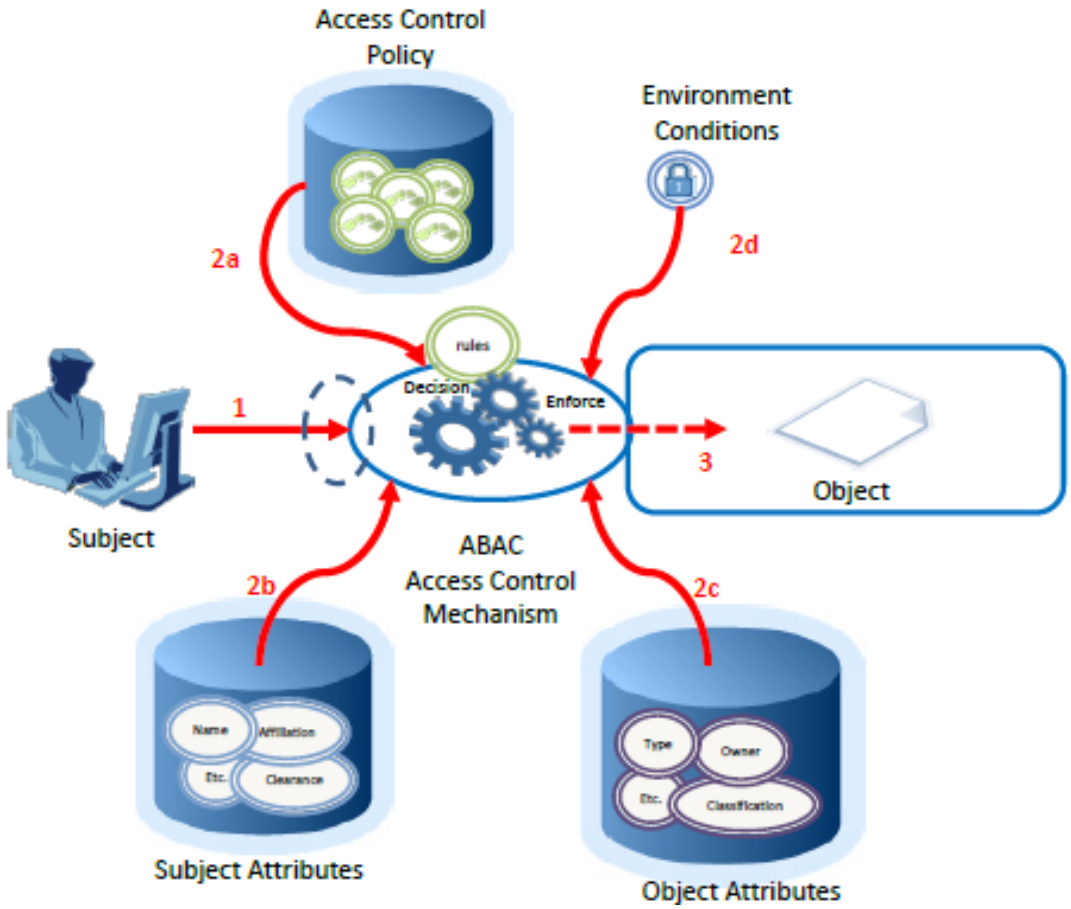
RBAC

- Assigns permissions to users based on their role within the organization
- A role is assigned to the user and that role has a set of permissions
- Roles should be engineered based on the principle of least privileged
- Easier to audit (visibility)
- Can result in an enormous number of roles to accomplish fine-grained authorization.

ABAC

- Rule-based approach.
- Can be easy to set up but complex to manage.
- Evaluates attributes (characteristics), rather than roles, to determine access.
- Policies/rules based on (sets of attributes):
  - Subject (person or actor evaluated)
  - Resource (target or object being affected)
  - Action (to be performed on the Resource)
  - Environment (others: time of day, IP subnet, …)

Basic ABAC Scenario

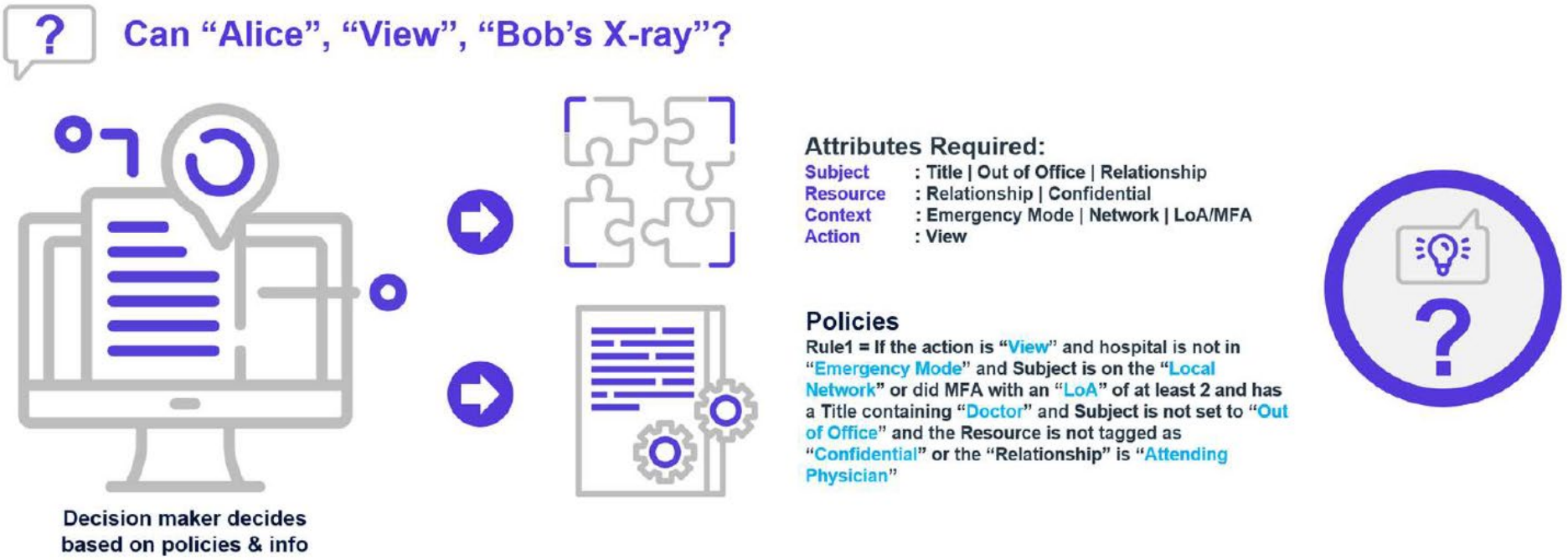


From "Guide to Attribute Based Access Control (ABAC) Definition and Considerations", NIST Special Publication 800-162, 2014

Basic ABAC Scenario

1. Subject requests access to object
2. Access Control Mechanism evaluates
   a) Rules
   b) Subject Attributes
   c) Object Attributes
   d) Environment Conditions to compute a decision
3. Subject is given access to object if authorized

ABAC authorization (external)



From “A Guide to Authorization” WHITEPAPER | MARCH 2021, Patrick Parker, CEO EmpowerID

PBAC

Policy-Based Access Control

- Authorization model combining RBAC & ABAC
- Example:
  Next Generation Access Control (NGAC) *(NIST)*
- Solve some of the complexities and limitations in ***XACML*** standard while maintaining its flexible and expressive nature

NGAC – Functional Architecture (NGAC-FA)

From "A Guide to Authorization" WHITEPAPER | MARCH 2021, Patrick Parker, CEO EmpowerID

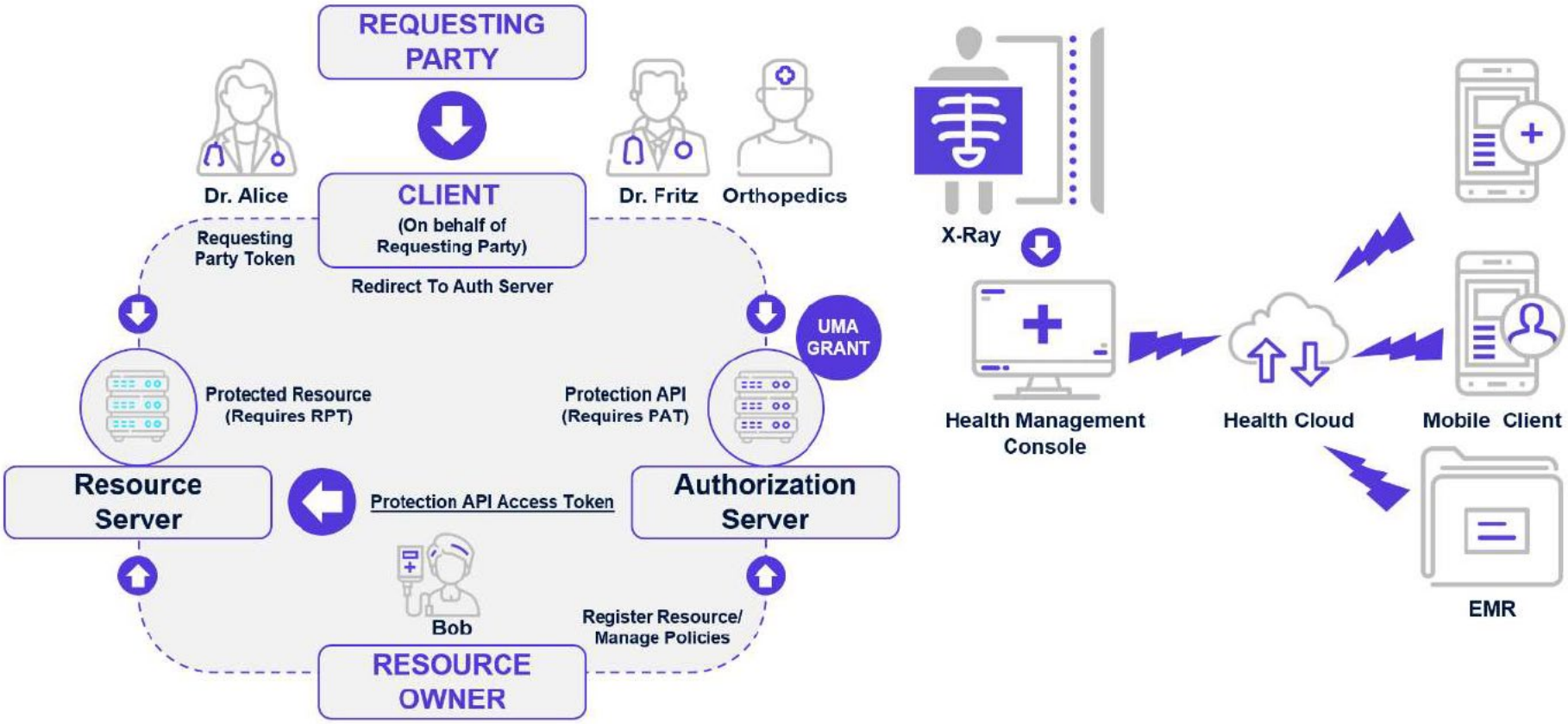
Example of a PBAC Get Permissions decision

From "A Guide to Authorization" WHITEPAPER | MARCH 2021, Patrick Parker, CEO EmpowerID

Example of Full PBAC Access Check

From "A Guide to Authorization" WHITEPAPER | MARCH 2021, Patrick Parker, CEO EmpowerID

User Managed Access (UMA)



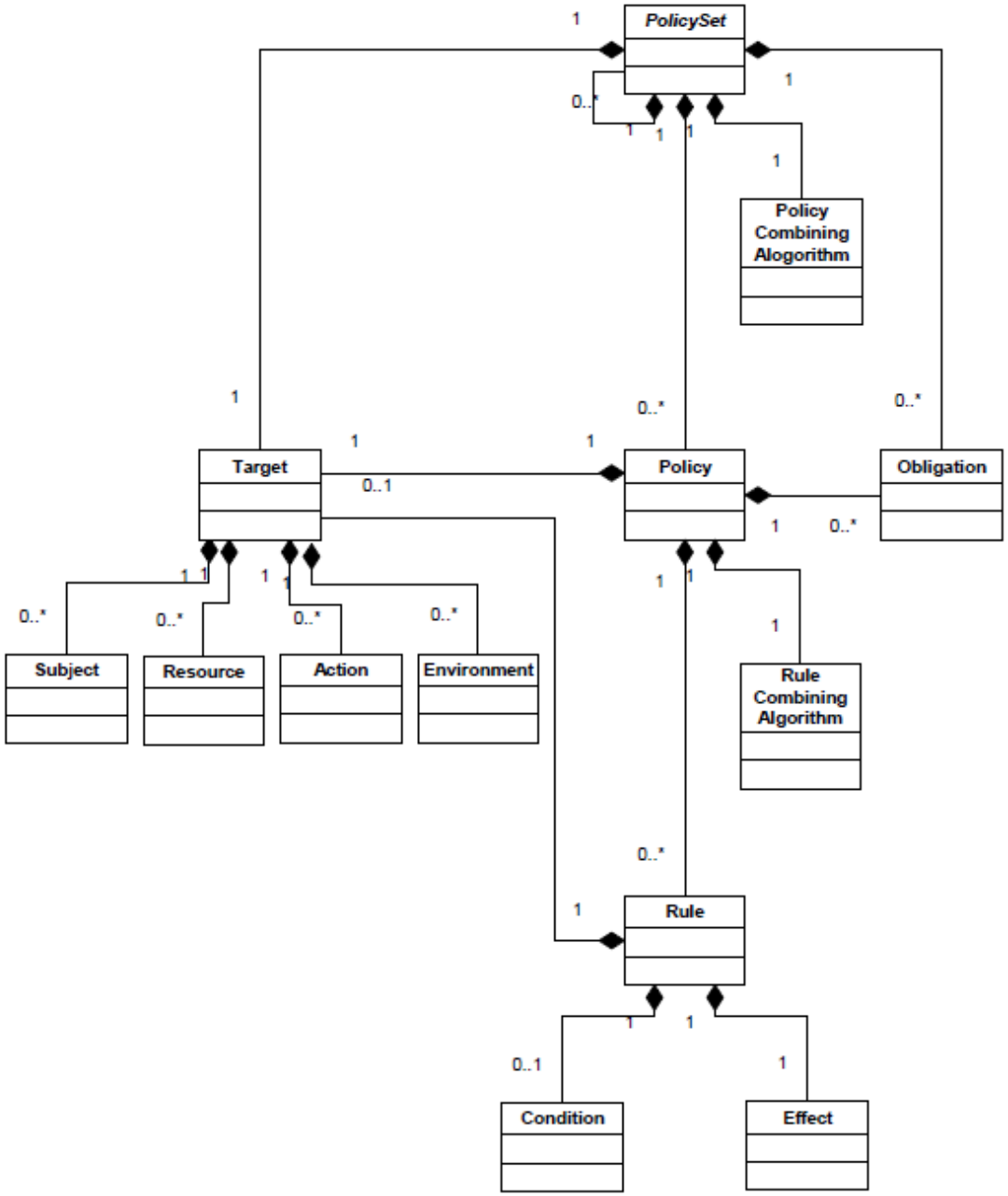
Privacy and Access Control

- ~~Privacy basic concepts~~
- ~~Access Control mechanisms~~
- **Privacy policies expresssion: XACML**

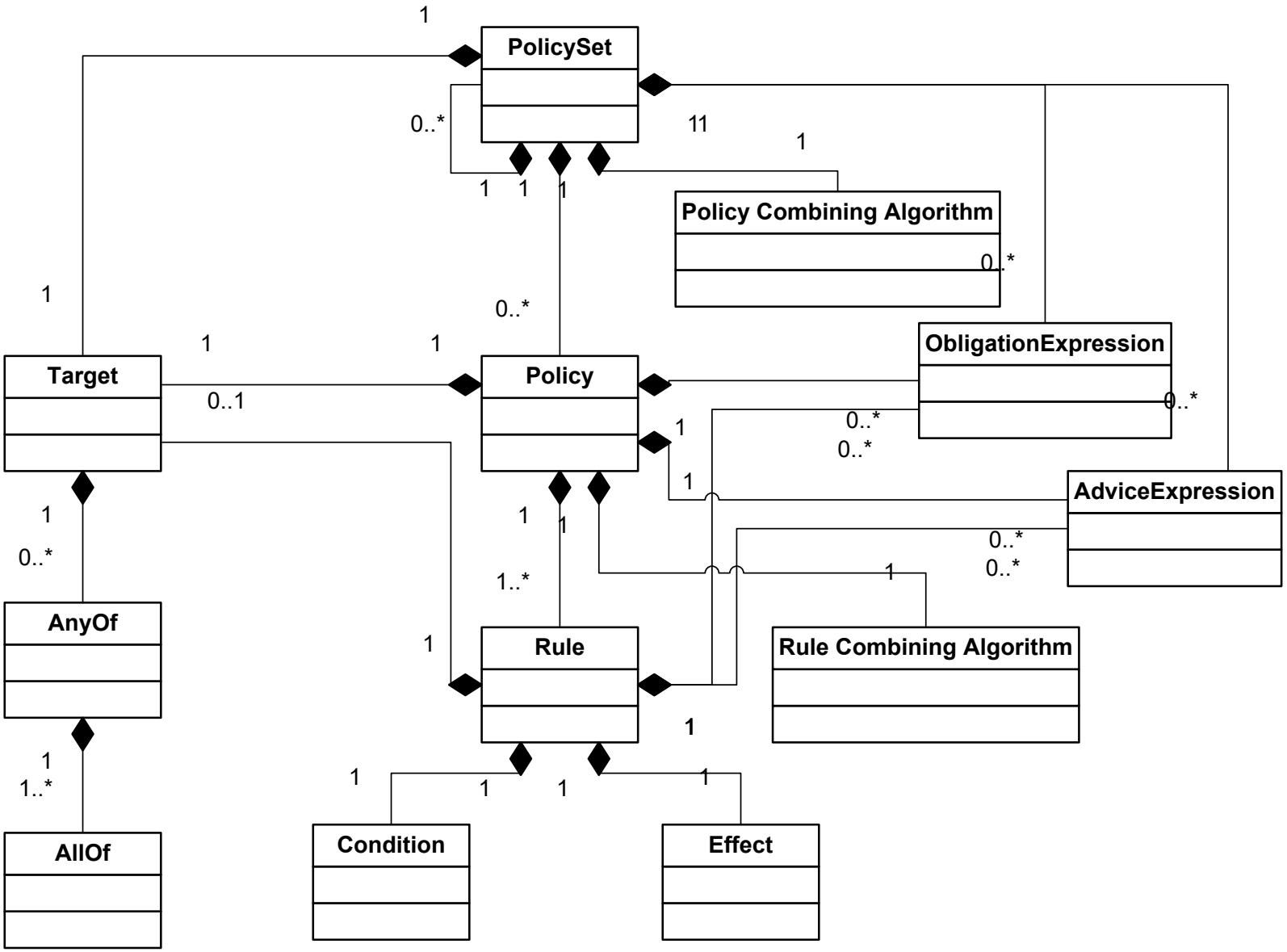
Privacy policies expression

- **XACML (eXtensible Access Control Markup Language)**
- OASIS Standard. Version 3.0, 22nd January 2013 (1st in 2010). Version 2.0 in 2005.
  http://docs.oasis-open.org/xacml/3.0/xacml-3.0-core-spec-os-en.pdf
  - Designed to express authorization policies in XML over objects identifiable in XML
  - Specifies a model for policies formed by 3 elements:
    - Rule
    - Policy
    - PolicySet

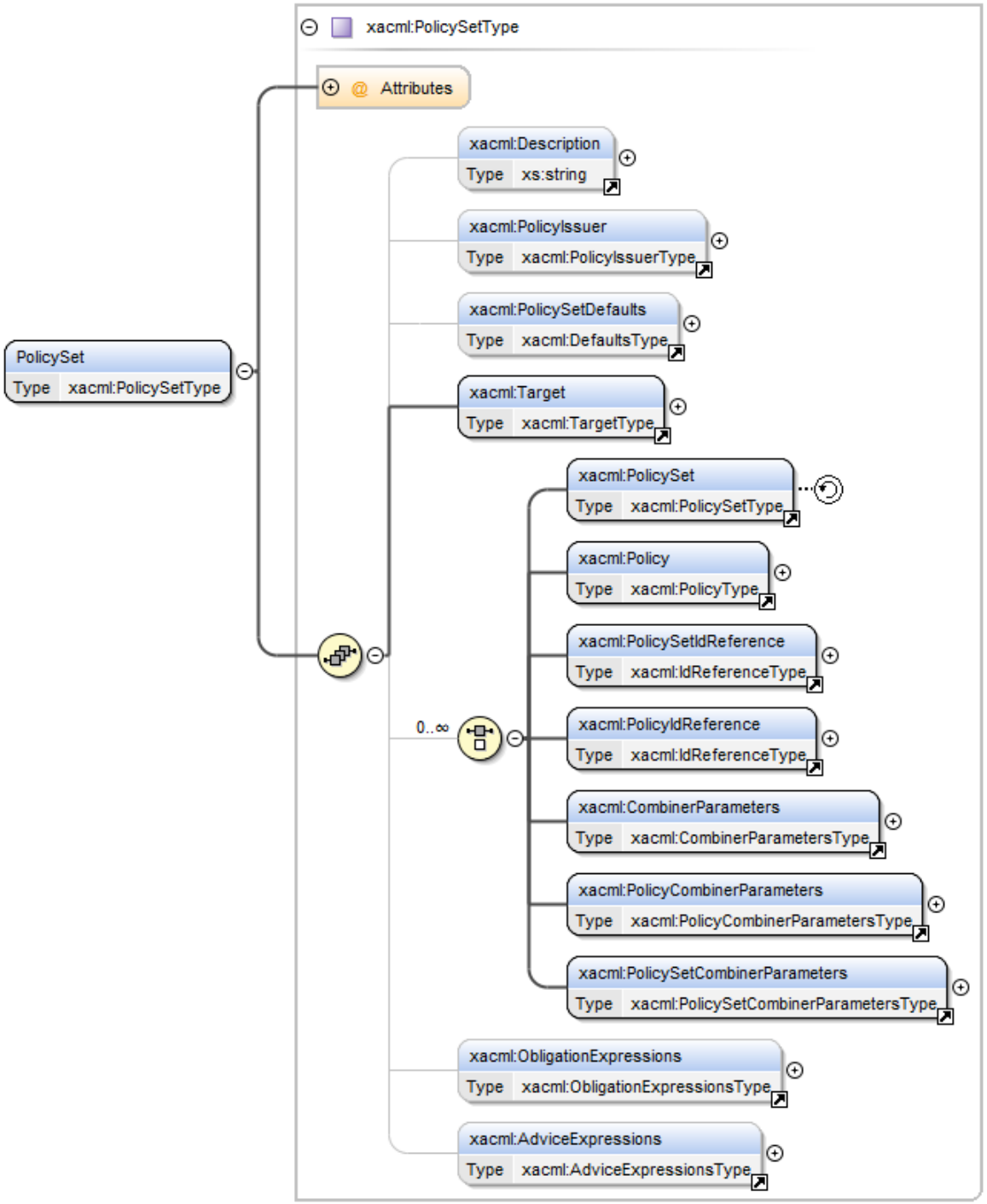
XACML 2.0 Policy Model



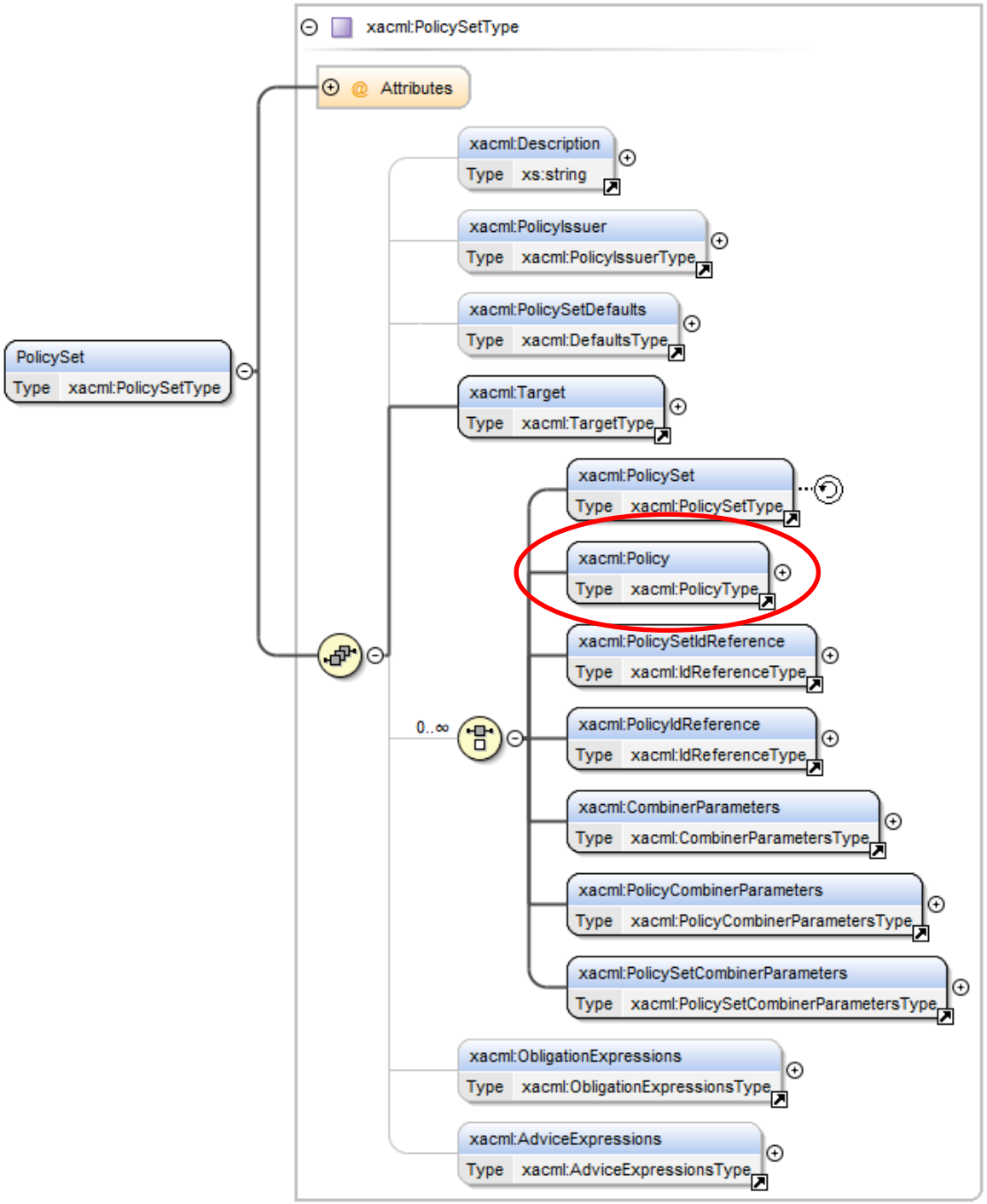
XACML 3.0 Policy Model



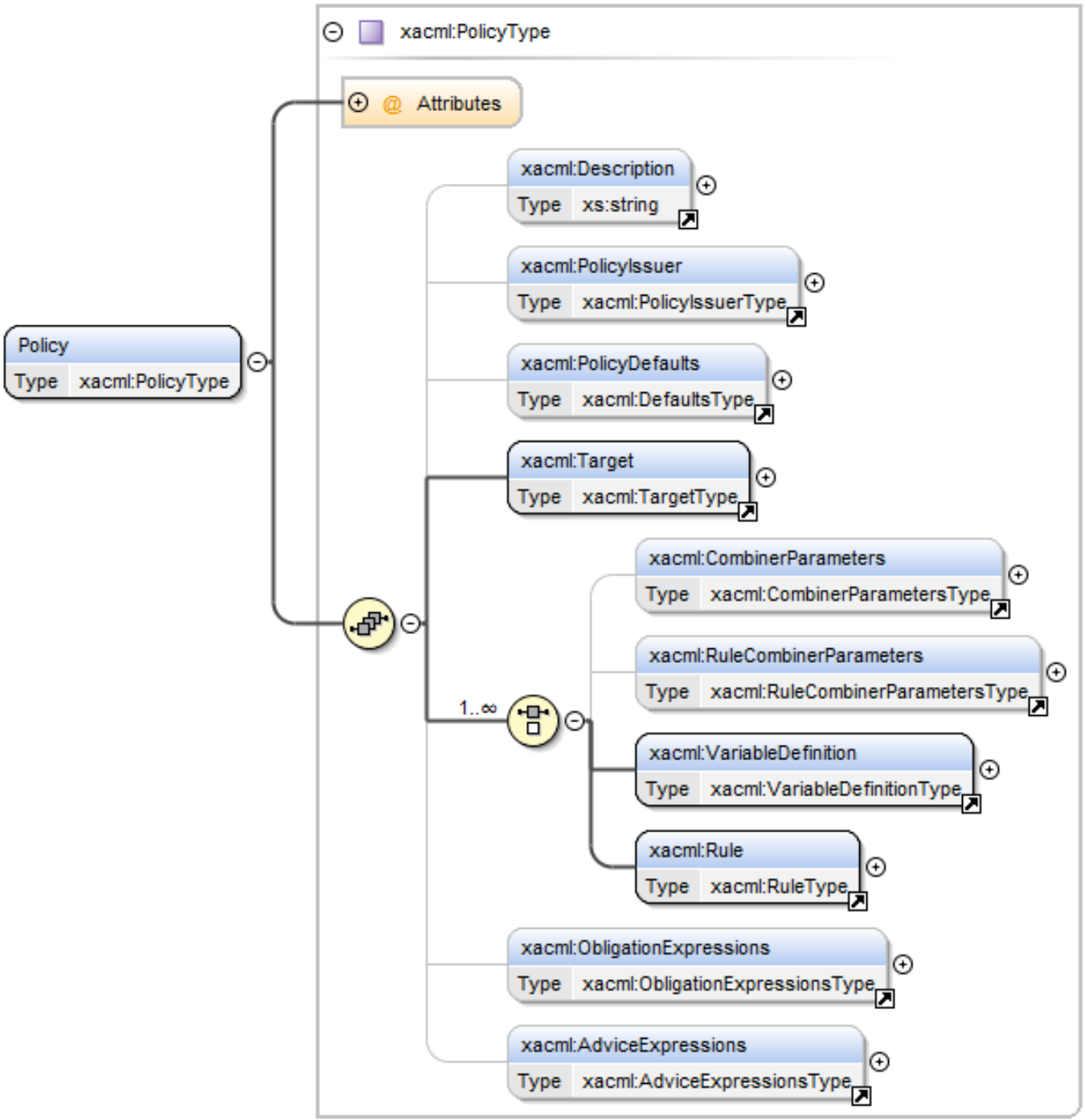
PolicySet Element



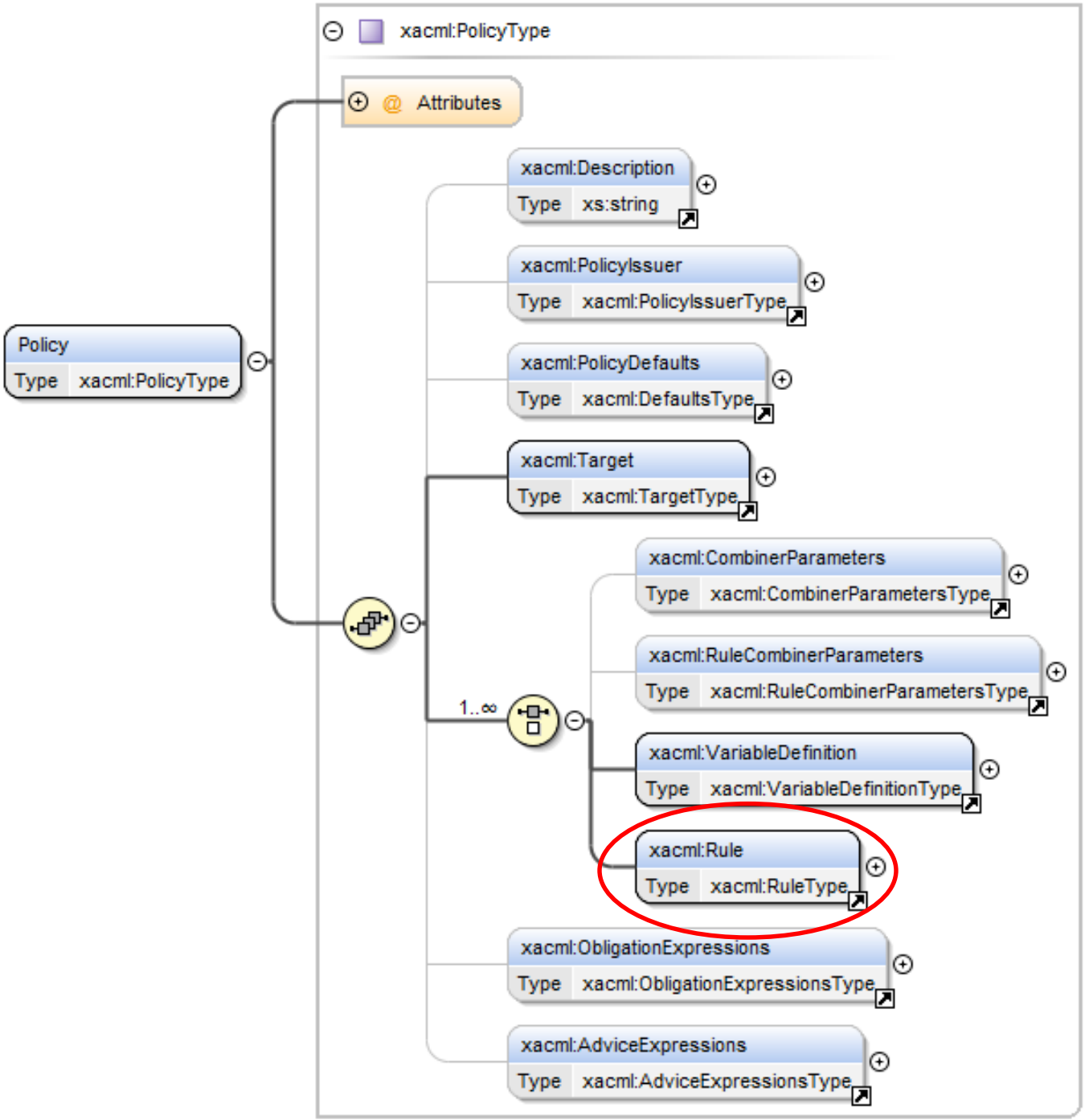
PolicySet Element



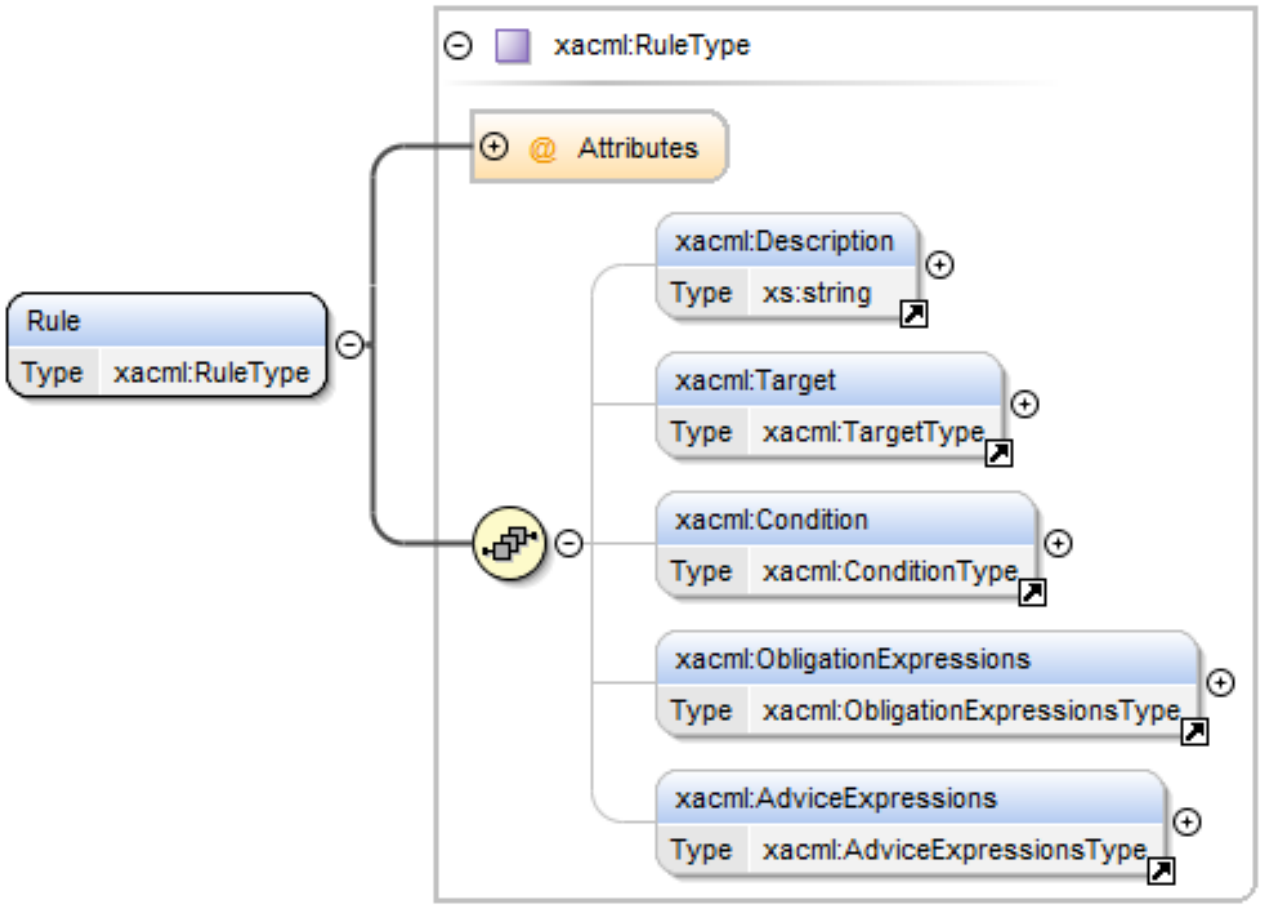
Policy Element



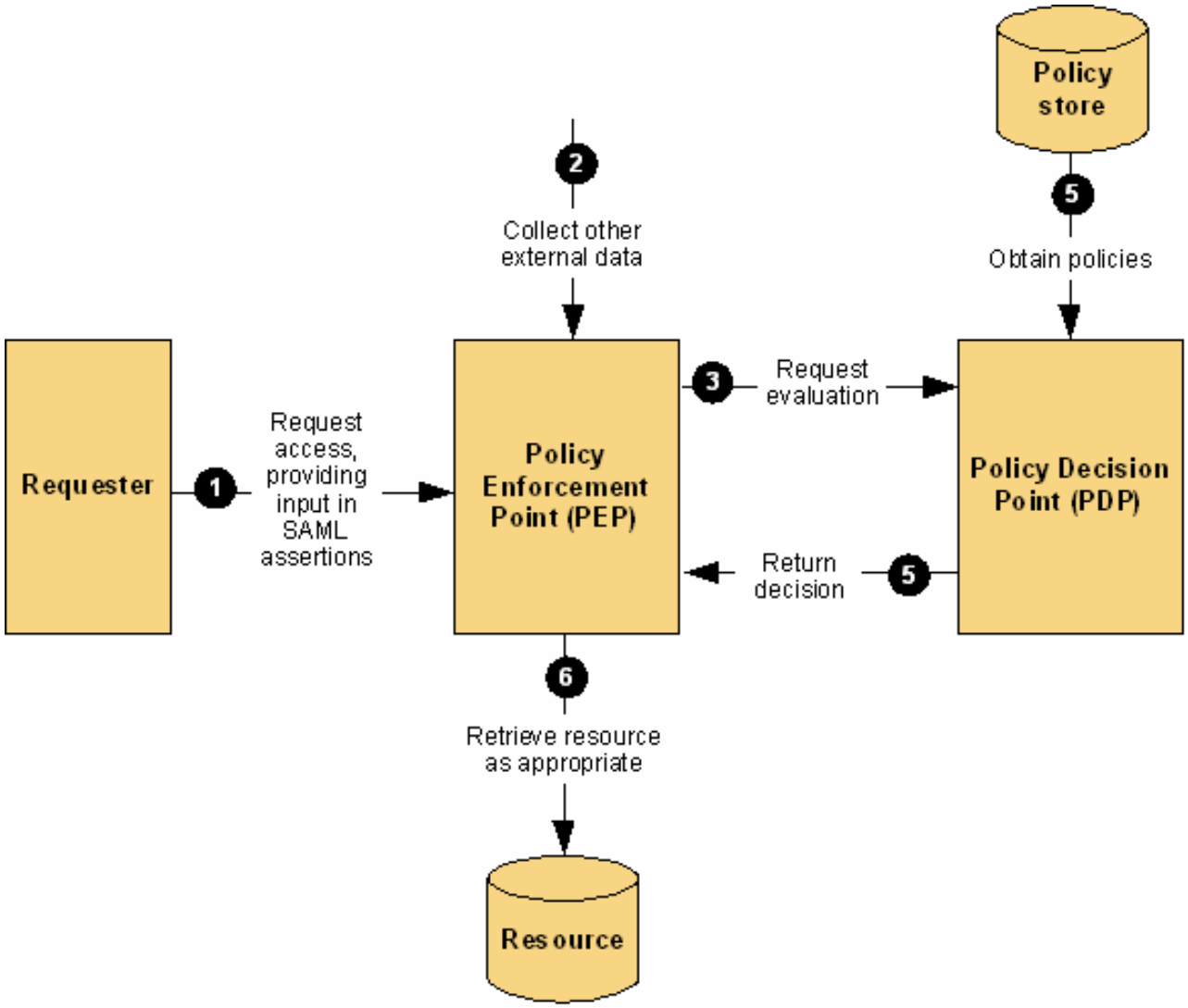
Policy Element



Rule element



SAML in XACML



Security in Internet Applications

- ~~Security in application layer protocols~~
- ~~XML and security~~
- ~~Specific security protocols for the Web~~
- ~~Privacy and access control~~

Security in Internet Applications

- ~~Security in application layer protocols~~
- ~~XML and security~~
- ~~Specific security protocols for the Web~~
- ~~Privacy and access control~~
- Security and privacy in eHealth