XACML

eXtensible Access Control Markup Language

Autor

Francisco Alexandre de Gouveia

Orientador

Doutor Diogo Gomes

Colaborador

Engenheiro Ricardo Azevedo

Universidade de Aveiro

Instituto de Telecomunicações

Portugal Telecom Inovação

XACML – O que é

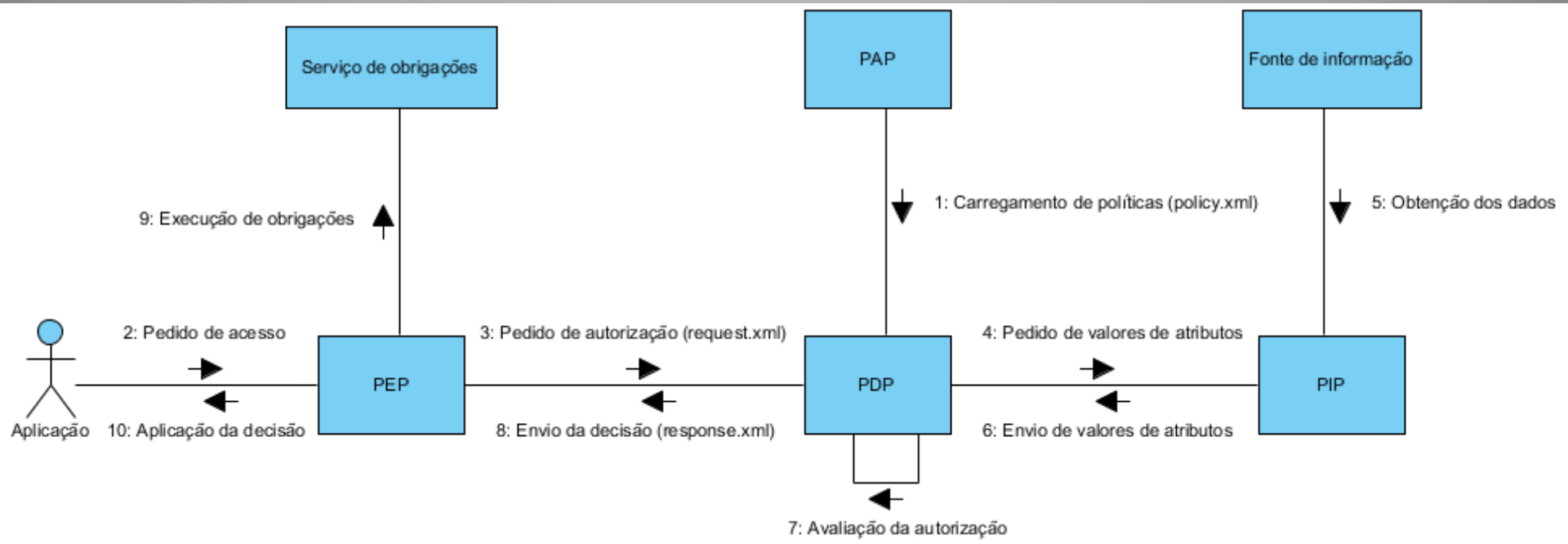
- Norma definida pela OASIS para controlo de acessos extensível e genérico
- Consiste em:
  - Linguagem extensível de políticas em xml
  - Linguagem extensível de pergunta-resposta em xml
  - Arquitectura distribuída baseada em:
    - Policy Enforcement Point
    - Policy Decision Point
    - Policy Information Point
    - Policy Administration Point

XACML – Para que serve

- Controlo de acessos
- Como é genérico e extensível, pode ser aplicado em qualquer contexto:
  - Controlo de acesso de portas
  - Controlo de acesso numa página web
  - Controlo de acesso de serviços
- Só toma decisões!
  - Não serve para saber que permissões uma determinada entidade tem

XACML – Como funciona

- Sistema de pergunta – resposta
- Arquitectura distribuída



XACML – Pergunta

- O **sujeito** pode realizar a **acção** no **recurso** num determinado **contexto**?
- Palavras chave:
  - **Sujeito** – Tanto pode ser uma pessoa como um equipamento
  - **Acção** – Predicado (aceder, ler, editar, abrir,…)
  - **Recurso** – O destino da acção (serviço, publicação, texto, porta, …)
  - **Contexto** – Tudo o que não se enquadre nos anteriores (espaço temporal, níveis de carga de processamento, nº de pessoas num local)

XACML – Pergunta

- O **sujeito** pode realizar a **acção** no **recurso** num determinado **contexto**?

Exemplo em XACMLv2

```
<Request>
    <Subject>
        <Attribute AttributeId="utilizador"
        DataType="http://www.w3.org/2001/XMLSchema#string">
            <AttributeValue>Anónimo</AttributeValue>
        </Attribute>
    </Subject>
    <Action>
        <Attribute AttributeId="urn:oasis:names:tc:xacml:1.0:action:action-id"
        DataType="http://www.w3.org/2001/XMLSchema#string">
            <AttributeValue>Ler</AttributeValue>
        </Attribute>
    </Action>
    <Resource>
        <Attribute AttributeId="tipo" DataType="http://www.w3.org/2001/XMLSchema#string">
            <AttributeValue>Tópico</AttributeValue>
        </Attribute>
    </Resource>
</Request>
```

Sujeito

Acção

Recurso

XACML – Pergunta

- O **sujeito** pode realizar a **acção** no **recurso** num determinado **contexto**?

```
<Subject>
        <Attribute AttributeId="utilizador" DataType="http://www.w3.org/2001/XMLSchema#string">
                <AttributeValue>Anónimo</AttributeValue>
        </Attribute>
</Subject>
```

Exemplo em XACMLv2

```
<xacml:Attributes Category="urn:oasis:names:tc:xacml:1.0:subject-category:access-subject">
        <xacml:Attribute AttributeId="utilizador“ IncludeInResult="false">
                <xacml:AttributeValue DataType="http://www.w3.org/2001/XMLSchema#string">
                        Anónimo
                </xacml:AttributeValue>
        </xacml:Attribute>
</xacml:Attributes>
```

Exemplo em XACMLv3

XACML – Resposta

- Tipos de resposta:
  - Permissão concedida (Permit)
  - Permissão negada (Deny)
  - Permissão indeterminada (Indeterminate)
  - Não existem políticas aplicáveis (Not applicable)
- Juntamente com:
  - Tarefas a serem executadas antes de ser permitido o acesso *

XACML – Resposta

- * Na versão 2 do XACML, existe o elemento *Obligation*
- O Policy Enforcement Point deve executar todas as tarefas descritas nos *Obligations*

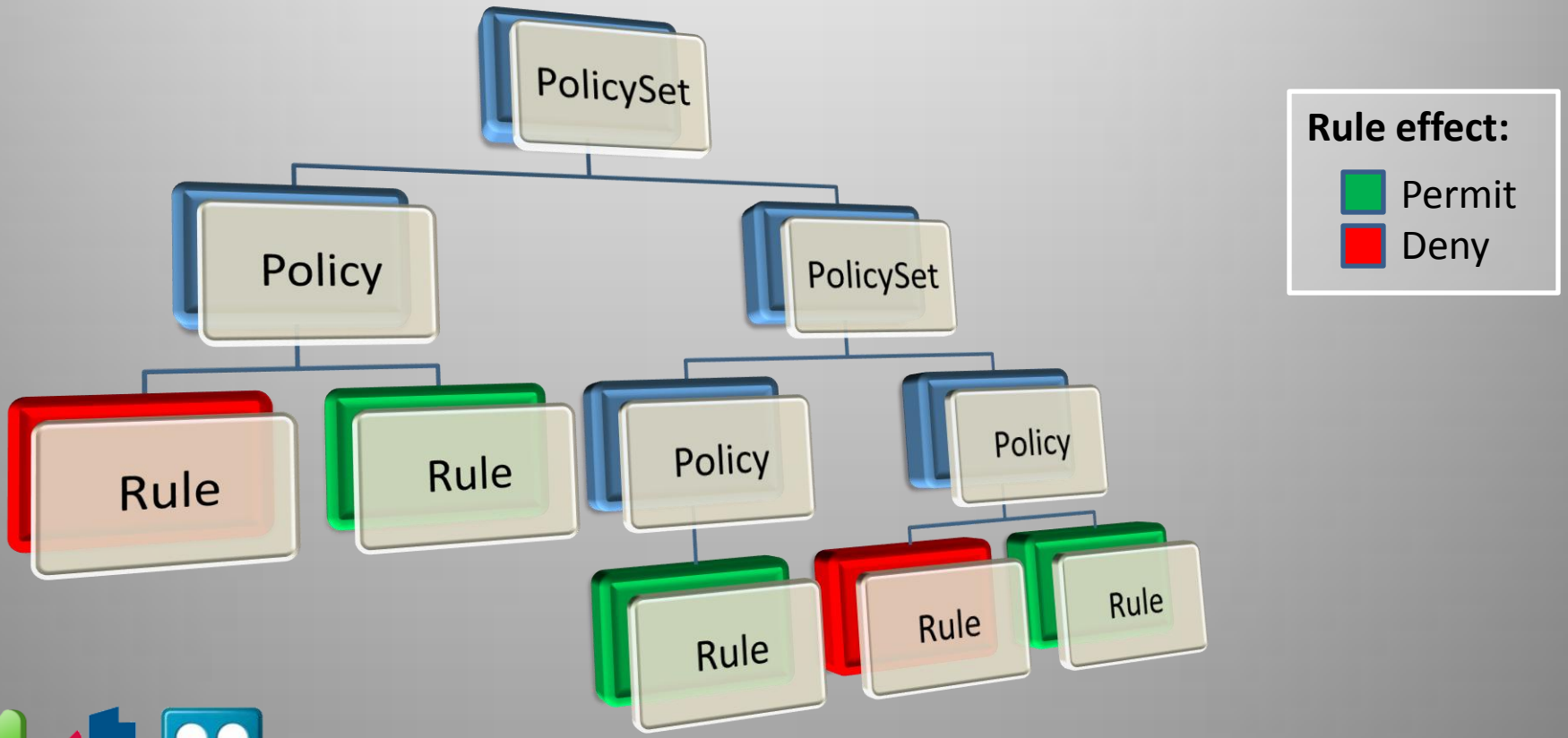
- *O que acontece quando a tarefa não é relevante e o Policy Enforcement Point não a consegue executar?*

XACML – Resposta

- * Na versão 3 do XACML, existem os elementos *Obligation e Advice*
- O Policy Enforcement Point :
  - Deve executar todas as tarefas descritas nos *Obligations*
  - Tentar executar as tarefas descritas nos Advices
- Se uma tarefa do elemento Advice falhar, a decisão não é alterada

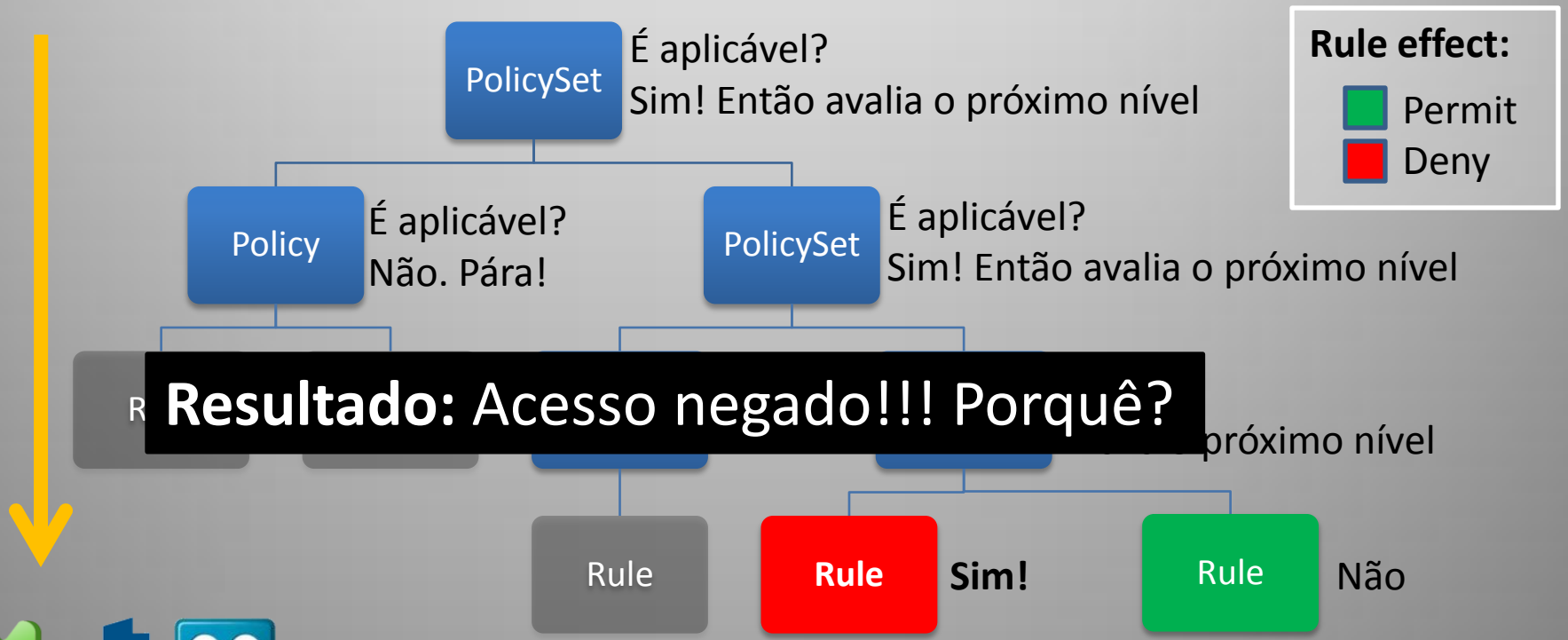
XACML – Avaliação

- Como são estruturadas as políticas?
- Existem 3 elementos principais



XACML – Avaliação

- Como são avaliados os elementos?
- Cada elemento tem um "*Target*"
- Avaliação feita a partir do topo

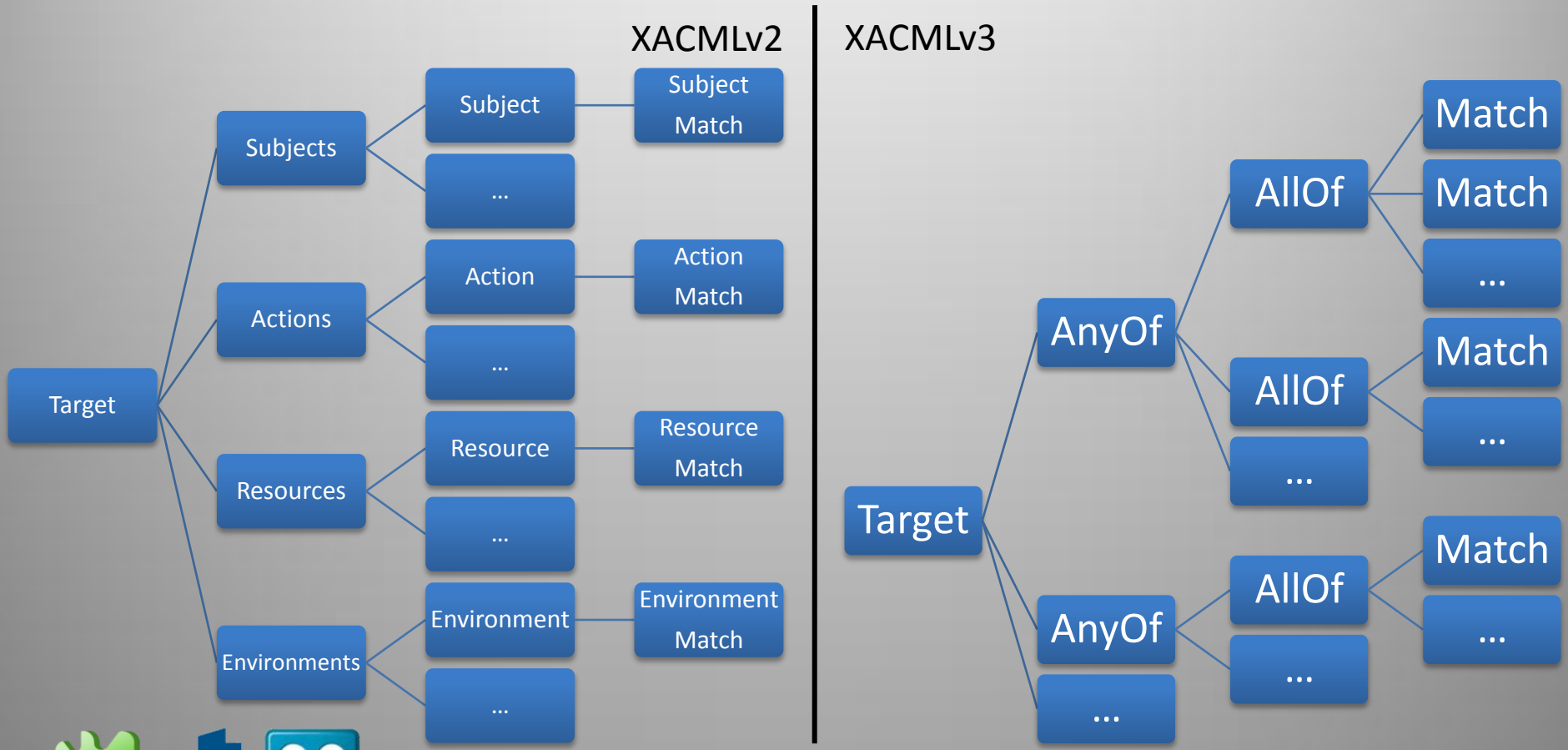


XACML – Avaliação

- E se mais do que uma **regra/política** for aplicável?
- Resposta: Algoritmos combinatórios
  - Permit-overrides
  - Deny-overrides
  - Only-one-applicable
  - First-applicable
  - … (podem ser criados outros)

XACML – Avaliação

- Como é constituído um *Target*?



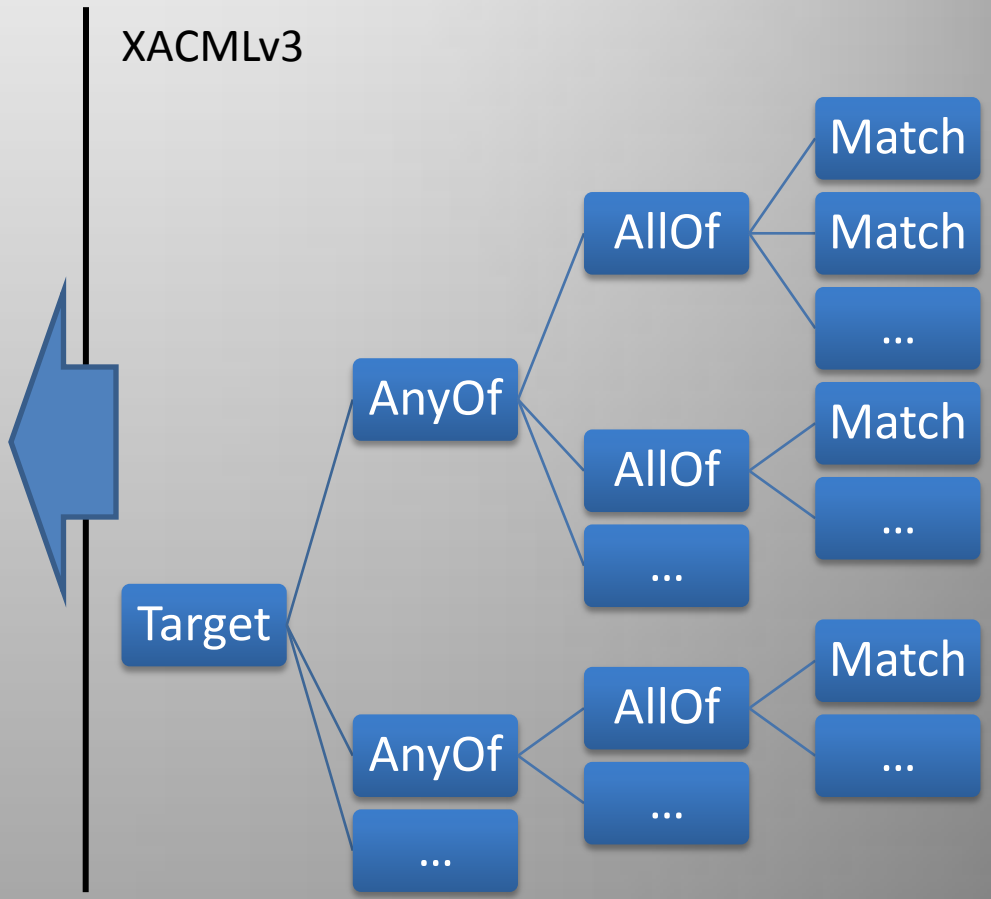
XACML – Avaliação

- Como é constituído um *Target*?

•Processo uniforme para todas as categorias
•Permite uniões e intersecções

Mas…

•Elementos AnyOf e AllOf não têm atributos identificadores
  •Na gestão de políticas implica analisar os valores contidos para saber qual editar/apagar e onde inserir
  •Ou recriar Target por cada alteração



PAP XACMLv3

Policy Administration Point

Autor

Francisco Alexandre de Gouveia

Orientador

Doutor Diogo Gomes

Colaborador

Engenheiro Ricardo Azevedo

Universidade de Aveiro

Instituto de Telecomunicações

Portugal Telecom Inovação

Policy Administration Point

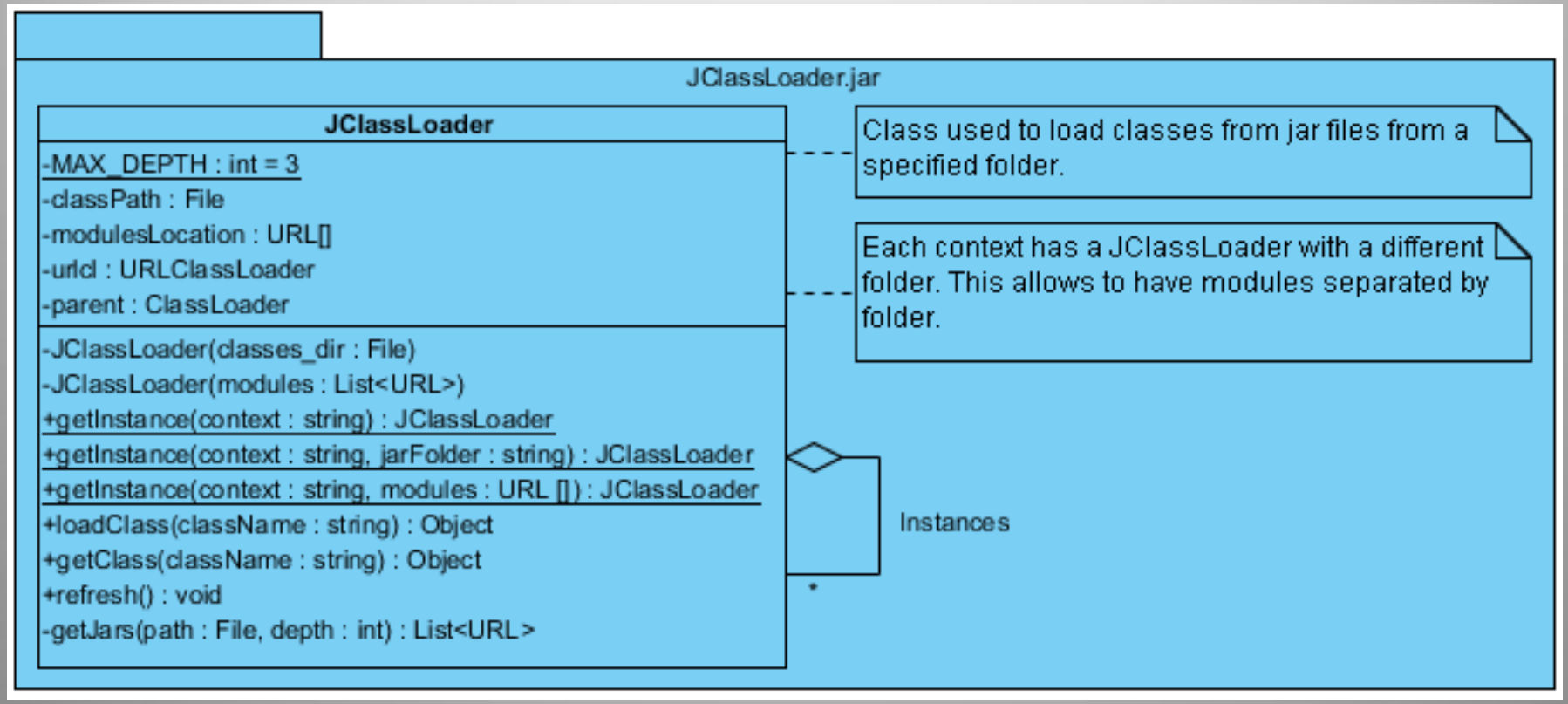
- Objectivos deste projecto
  - Sistema de informação extensível (importação de módulos sem recompilação)
  - Interface de administrador que abstraia a complexidade do XACMLv3
  - Criação de políticas que obedeçam à norma

Policy Administration Point

- Extensibilidade
  - Permitir importação de classes que implementem as interfaces definidas para:
    - Obtenção de informação do Policy Information Point
    - Persistência e obtenção de políticas
- Solução usada
  - URLClassLoader, carrega classes de ficheiros **.jar,* em tempo de execução

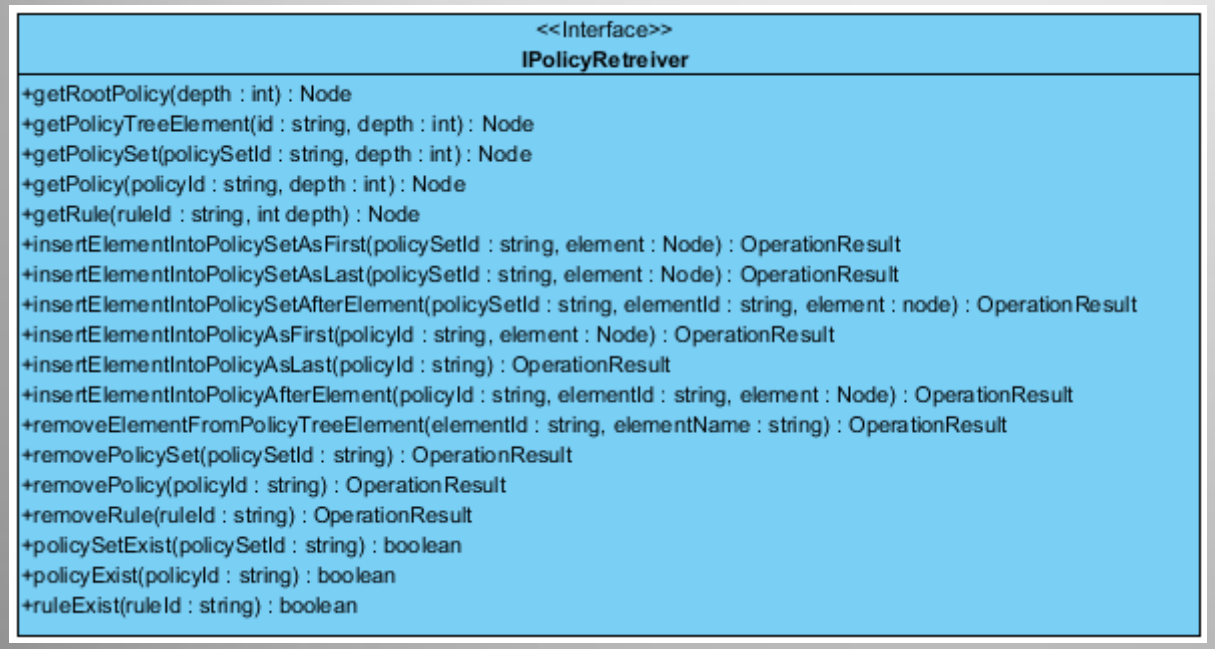
Policy Administration Point

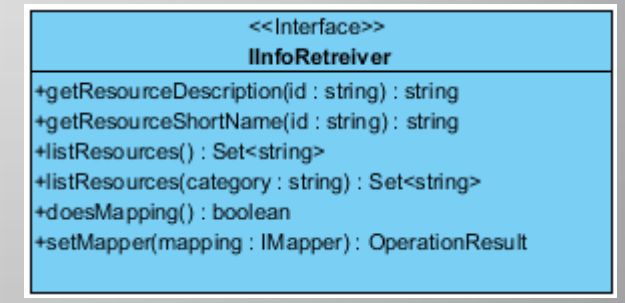
- Extensibilidade (Classe de carregamento de classes)



Policy Administration Point

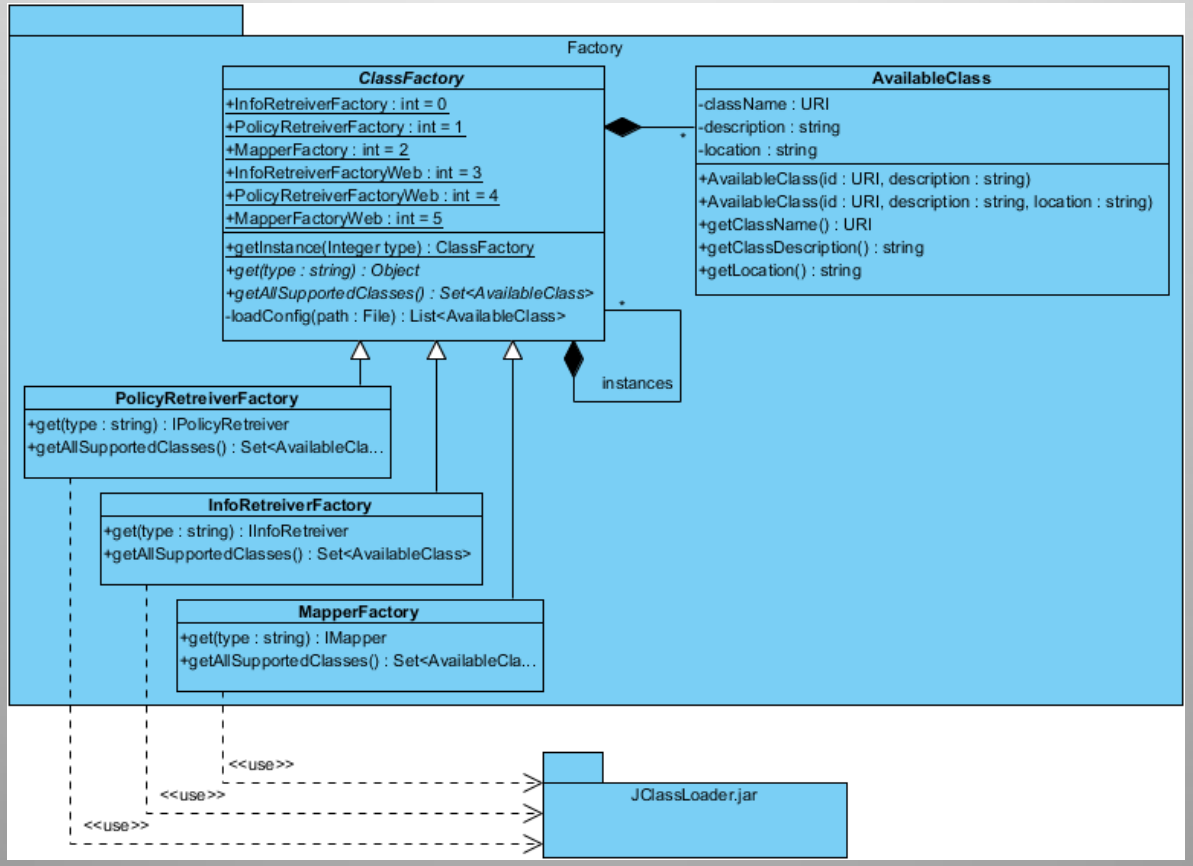
- Extensibilidade (Interfaces)





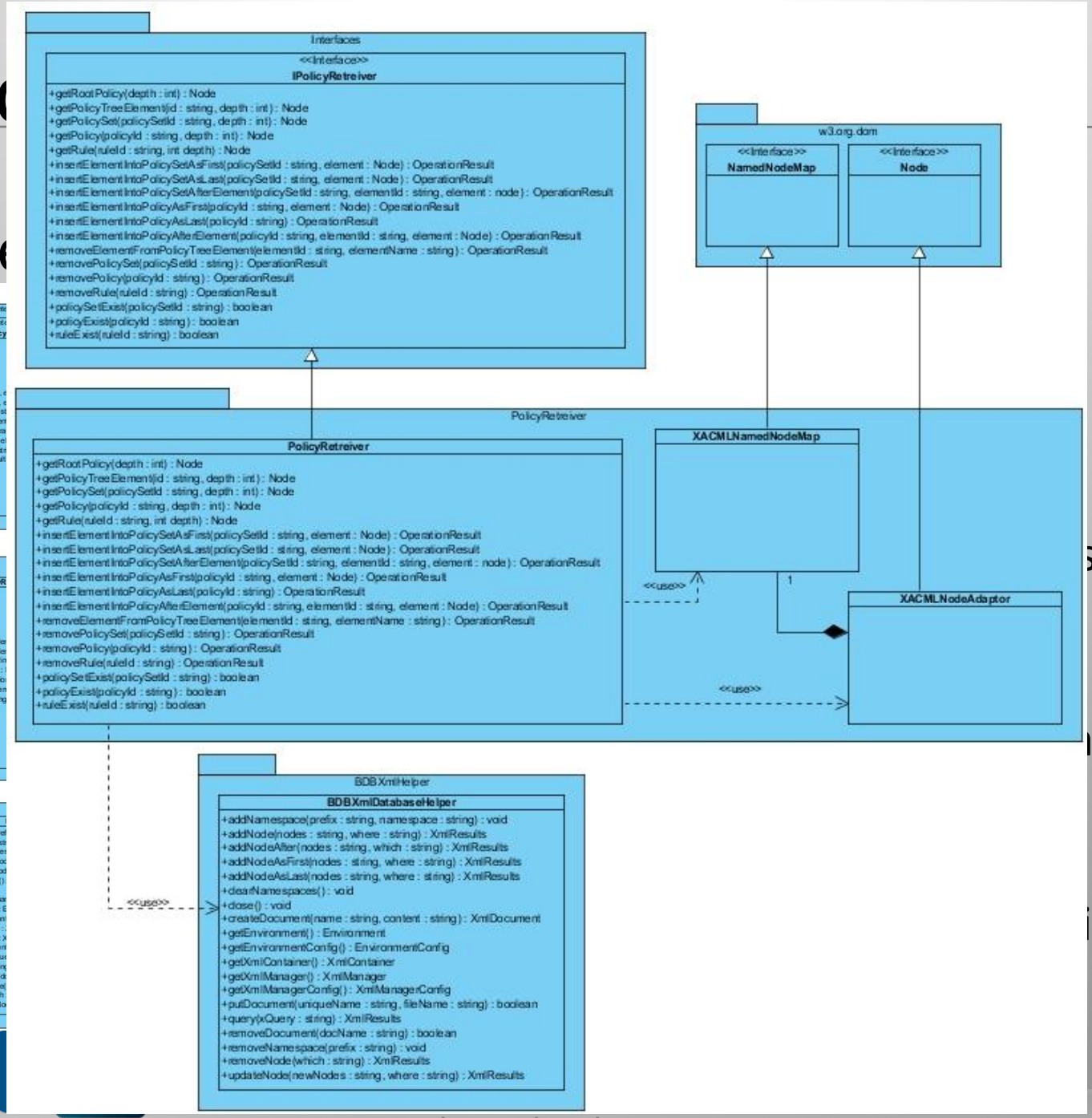
Policy Administration Point

- Extensibilidade (Factory)



Polic

- Exte



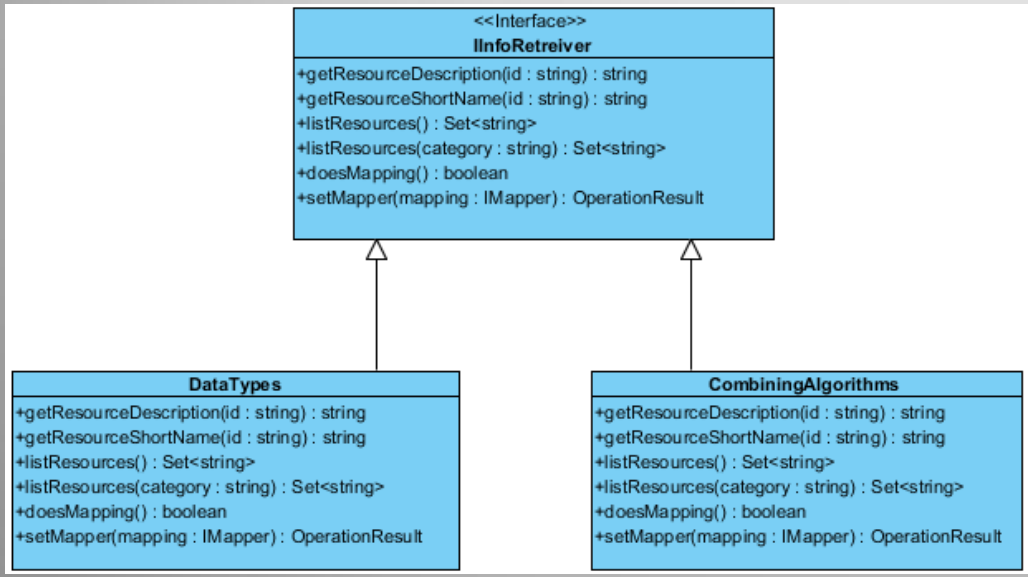
s DB XML

ligações

its

Policy Administration Point

- Extensibilidade (Módulos implementados)



- Info Retreiver
  - Lê ficheiro xml
- Devolve:
  - Tipos de dados
  - Funções
  - Algoritmos combinatórios

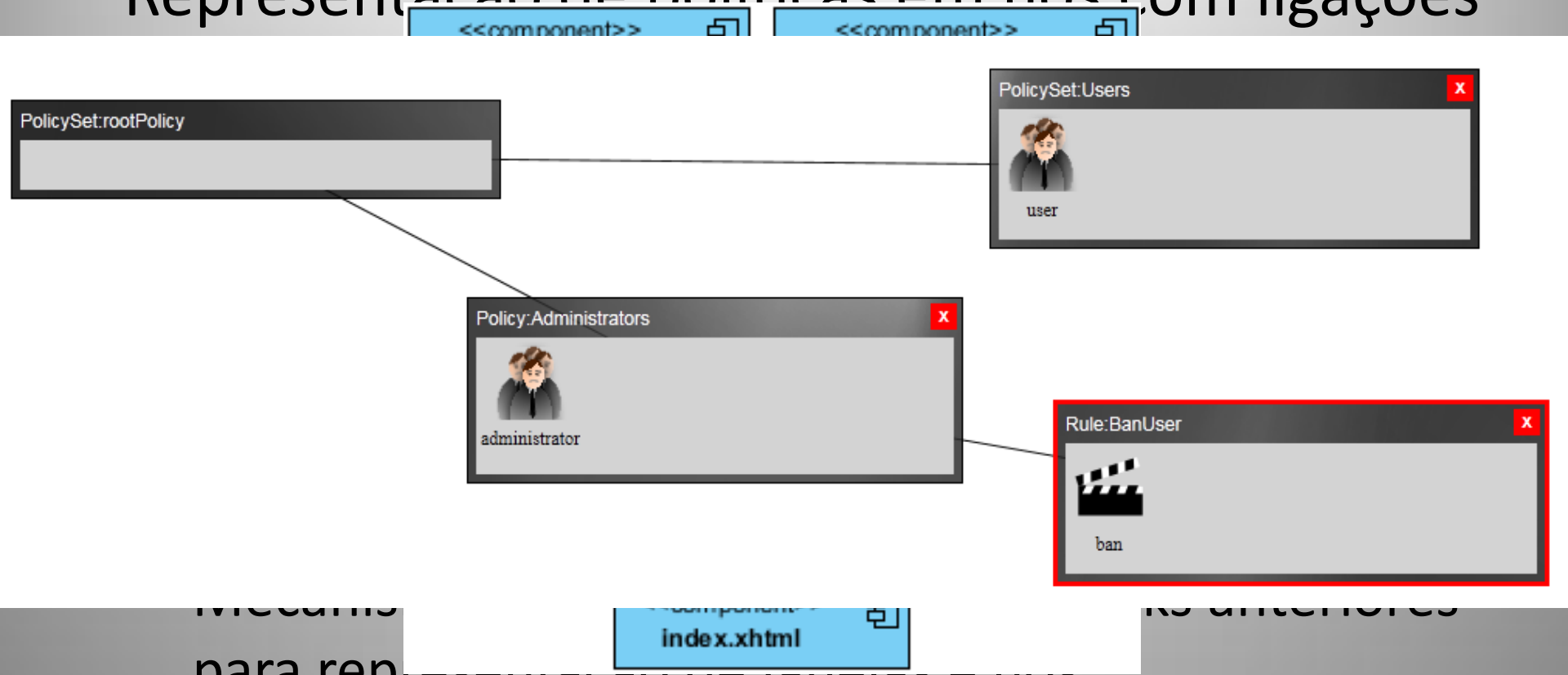
Policy Administration Point

- Abstracção da complexidade do XACMLv3 na interface de administrador

- Solução usada:
  - Interface web com:
    - Representação de políticas em nós com ligações entre eles
    - Abstracção de nomes complexos através de imagens representativas e nomes simplificados
    - Abstracção das regras do XACMLv3 através de opções únicas para cada contexto

Policy Administration Point

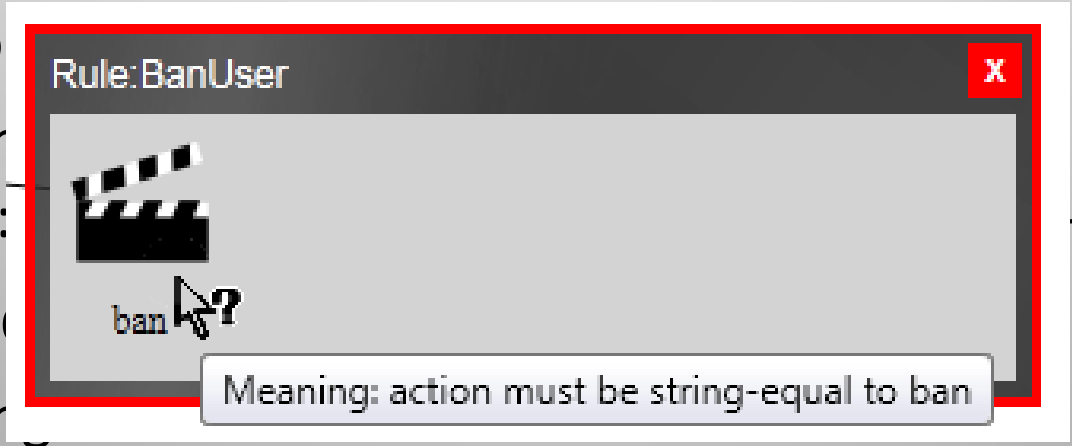
- Representação de políticas em nós com ligações



para representação de janelas e nós

Policy Administration Point

- Abstracção de nomes complexos através de imagens representativas e nomes simplificados
  - Funçõ
    - strin
      urn:
  - Tipos
    - strin
      http://www.w3.org/2001/XMLSchema#string

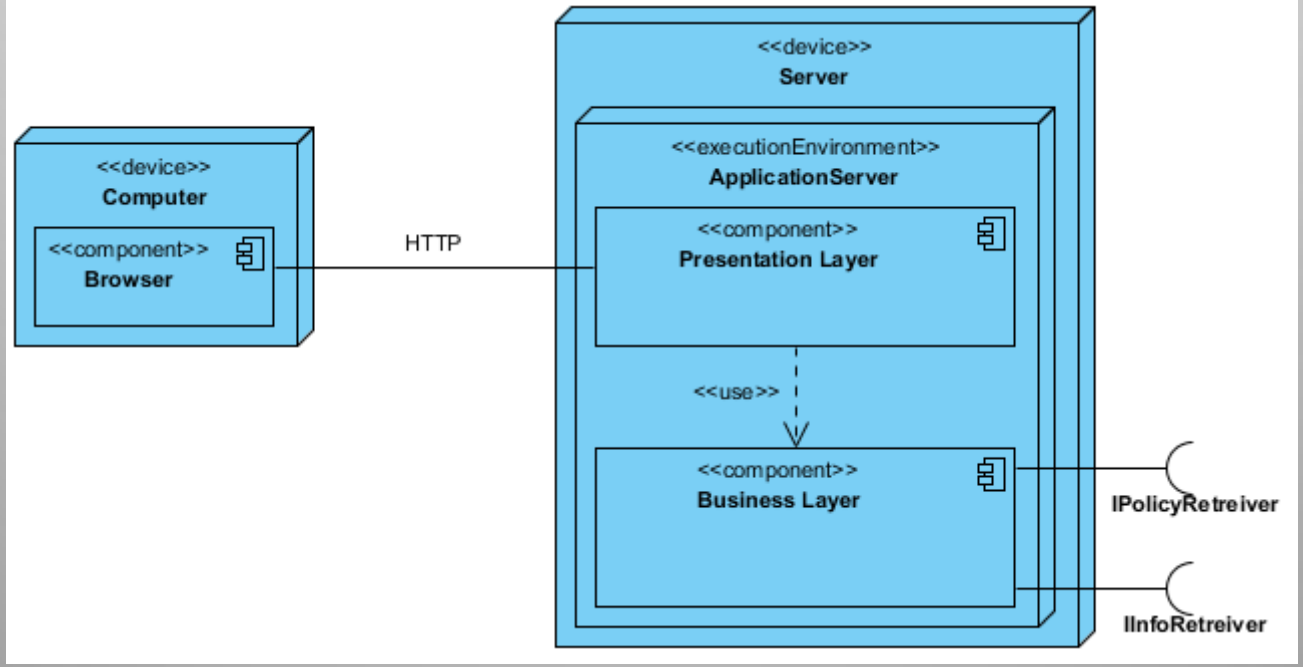


Policy Administration Point

- Criação de políticas que obedeçam à norma
  - Existe um esforço para que, por trás de toda a abstracção, as políticas sejam criadas conforme a norma especificada
  - Em cada contexto, as opções mudam em relação às possibilidades de cada elemento
    - Por exemplo, existe uma toolbox que muda os botões dependendo dos elementos seleccionados

Policy Administration Point

- Implementação: aplicação J2EE



Policy Administration Point

- Implementação: aplicação J2EE (problemas)
  - ClassLoader não funcionou quando colocado em funcionamento numa aplicação web
  - Classes de instância única não tinham sempre a mesma instância

Policy Administration Point

- Class Loader do Java
  - Funciona de modo hierárquico

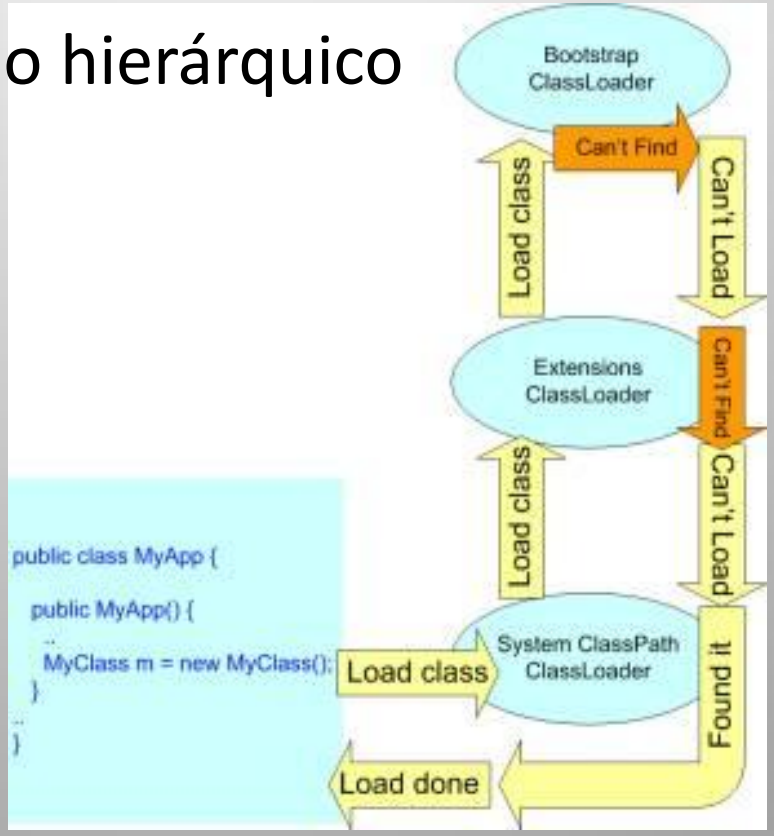


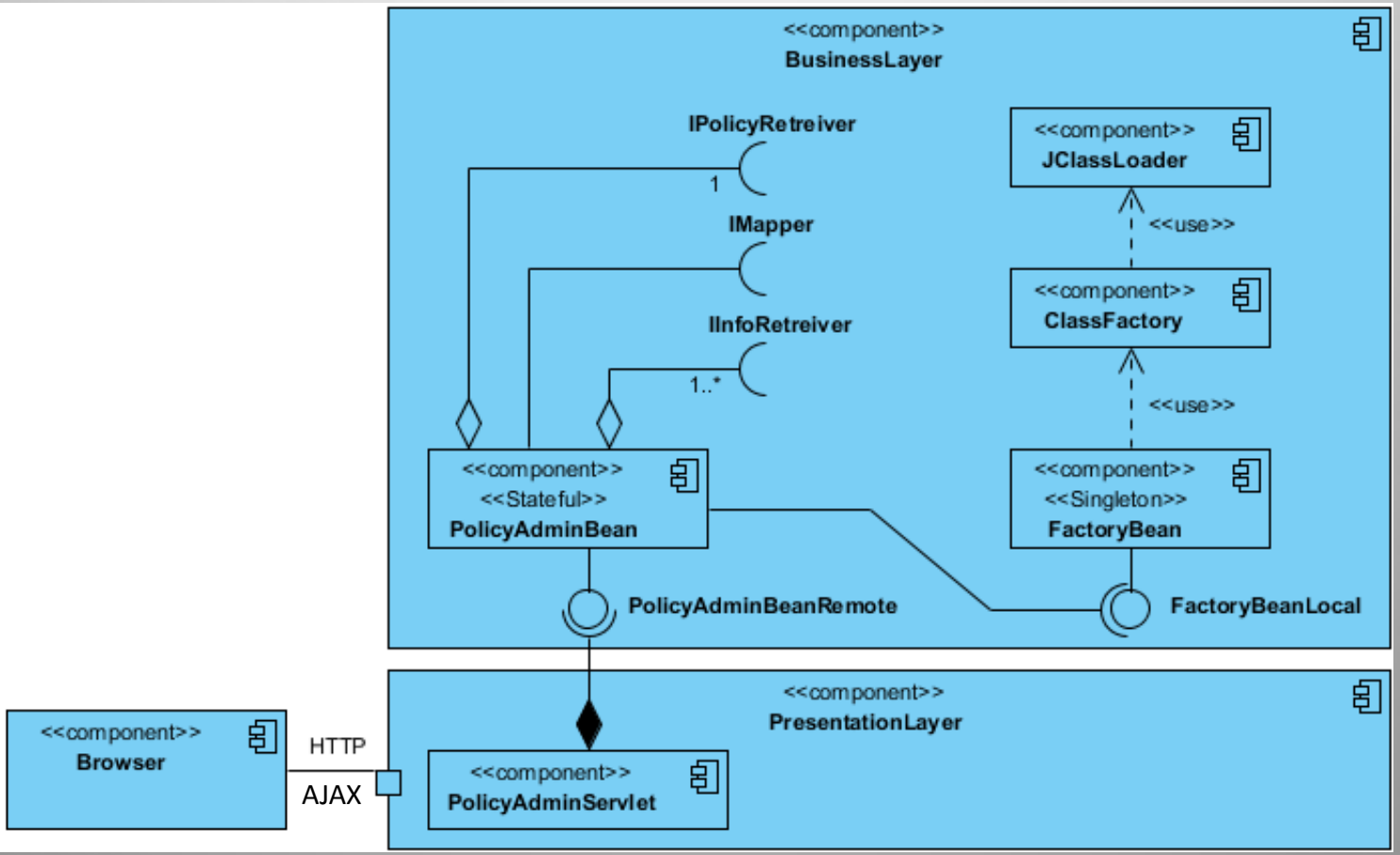
Imagem retirada de http://www.objectsource.com/j2eechapters/Ch21-ClassLoaders_and_J2EE.htm

Policy Administration Point

- Instâncias em web servers
  - Aplicação é colocada em mais do que um “contentor”
  - Para melhor performance, a carga é distribuída pelos contentores

Policy Administration Point

- Juntando tudo…



Policy Administration Point

- Conclusões
  - XACML permite fazer controlo de acessos granulado e genérico
  - A versão 3 trouxe melhorias em relação à versão 2
    - Adição de Advices em alternativa a Obligations
    - Uniões e intersecções de *Targets*
    - *Multi-request*
    - Mas ainda não está terminada…
  - Não existem muitas implementações
  - Problemas de administração de *Targets*

Policy Administration Point

Questões?