Uma Extensão do XACML para Federação de Identidades em Nuvem Computacional

ALEX FELIPE RAULINO
ORIENTADOR: PAULO FERNANDO DA SILVA

Roteiro

- Introdução
- Objetivos
- Fundamentação teórica
- Desenvolvimento
- Resultados e discussão
- Conclusão e extensões

Introdução

- XACML
- Segurança e Autorização
- Nuvem Computacional
- Federação de Identidades

Objetivos

- Gerenciar políticas de acesso no conceito de federação de identidades.
- Interpretar Request e Response do padrão XACML no conceito de federação de identidades.
- Identificar a política a ser aplicada no conceito de federação de identidades.

Fundamentação teórica

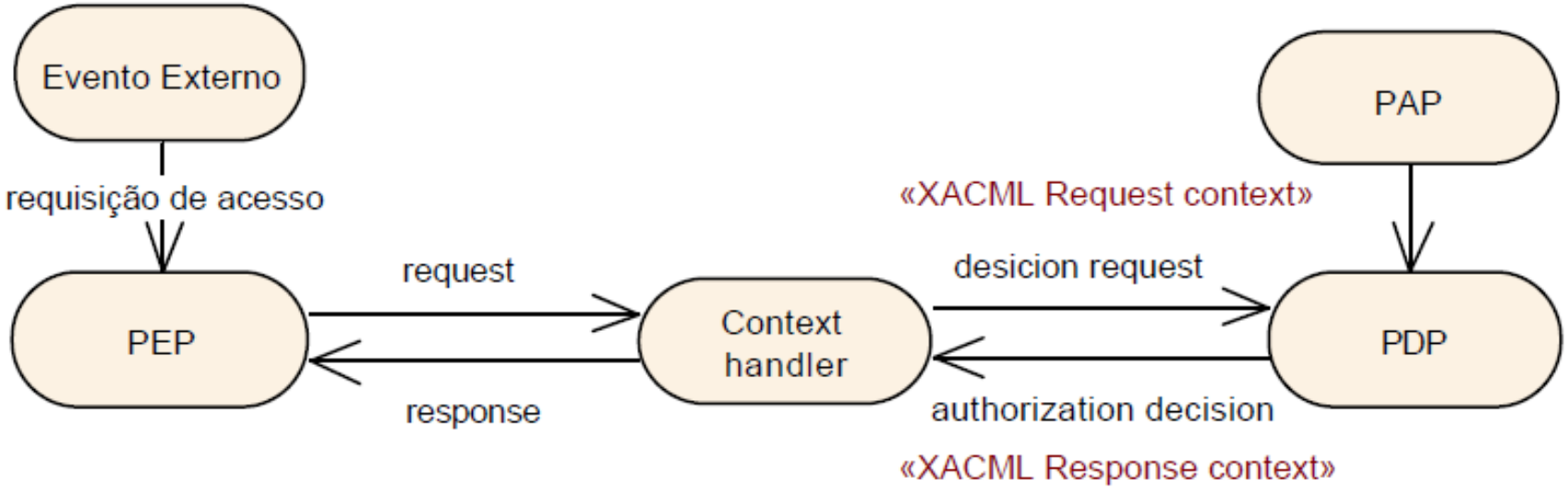
Federação de identidades

- Objetivos da federação de identidades
  - Reduzir os custos de gestão de identidades;
  - Melhorar a experiência do usuário;
  - Prover segurança e confiança end-to-end na integração de aplicações inter-organizacionais.

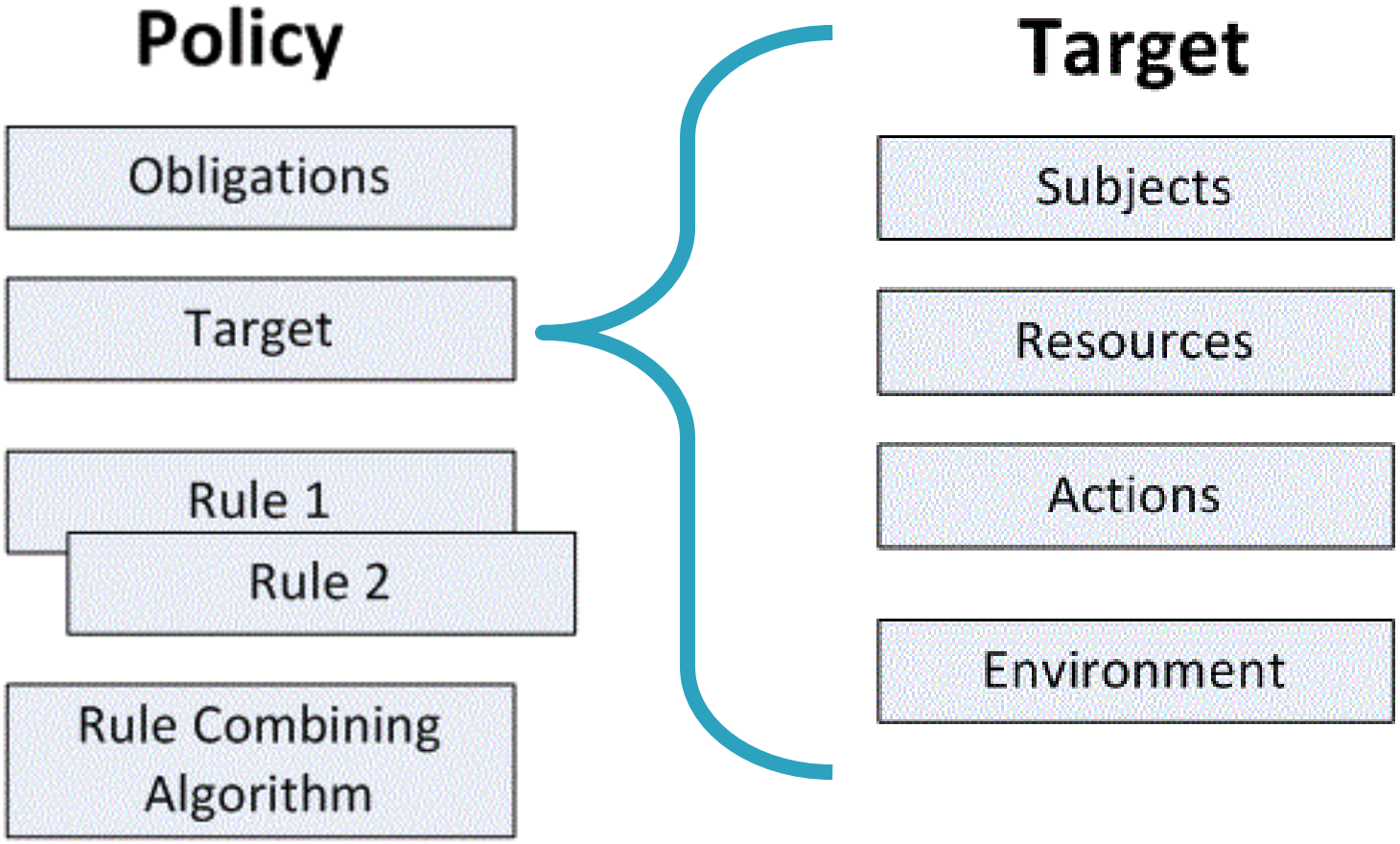
XACML

- O XACML é um padrão proposto pela OASIS (2005) que define uma linguagem para modelar, armazenar e distribuir políticas.

XACML


Evento Externo
requisição de acesso
PEP
request
response
Context handler
desicion request
authorization decision
PDP
PAP
«XACML Request context»
«XACML Response context»

XACML


Policy
Obligations
Target
Rule 1
Rule 2
Rule Combining Algorithm
Target
Subjects
Resources
Actions
Environment

Trabalhos Corelatos

- Federação de Identidades e Computação em Nuvem: Estudo de Caso Usando Shibboleth (LEANDRO, 2012) .
- Controle de Admissão de *Resource reSerVation Protocol* (RSVP) utilizando XACML (TOKTAR, 2003)

Desenvolvimento

Requisitos principais

- Ser desenvolvida utilizando a linguagem Java (RNF);
- Utilizar a IDE eclipse (RNF);
- Ter como base a versão 1.0 ou superior da especificação XACML (RNF);

Requisitos principais

- Deverá permitir gerenciar políticas de acesso no conceito de Federação de Identidades (RF);

- Deverá permitir interpretar *request* e *response* do padrão XACML no conceito de federação de identidades (RF);

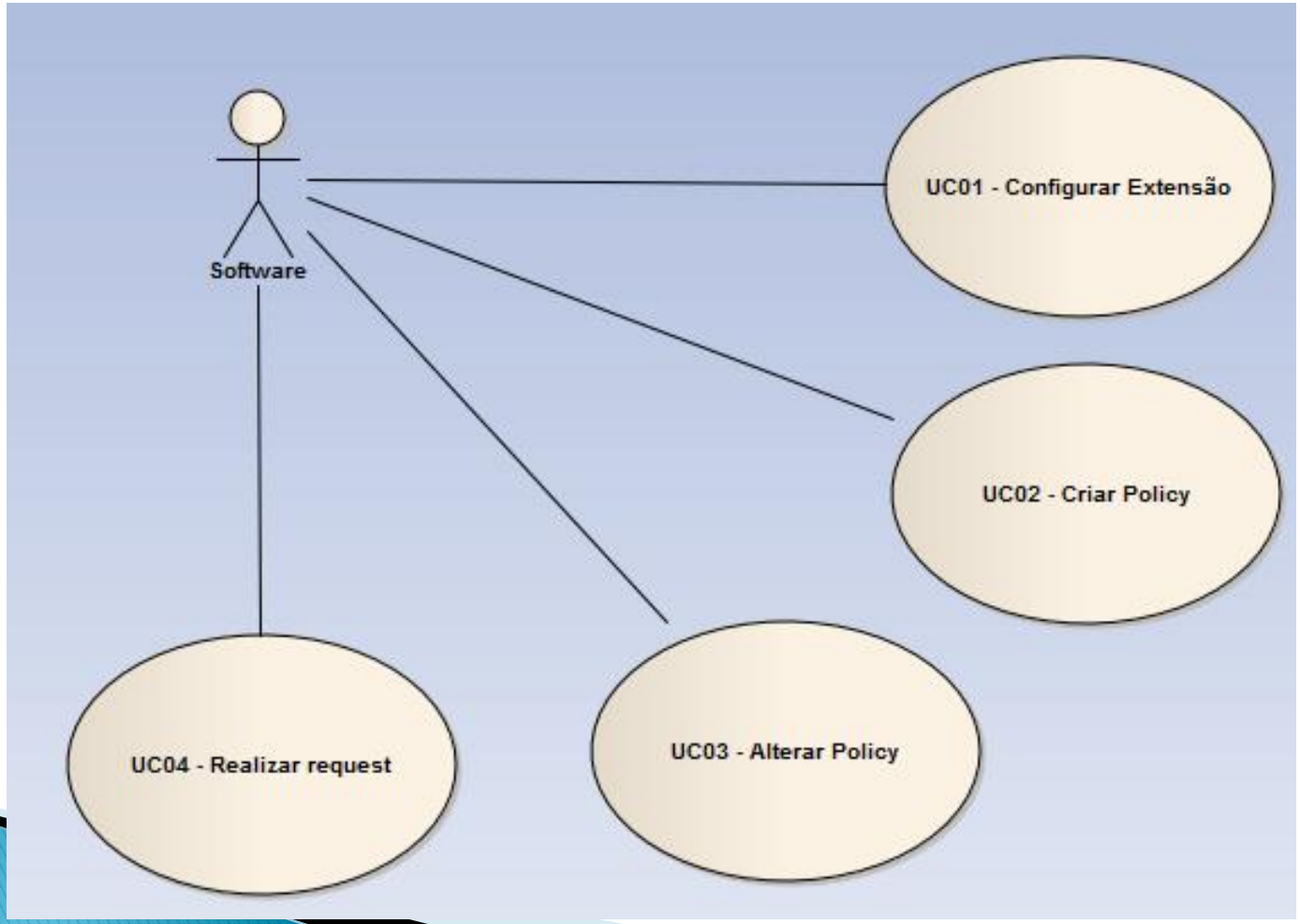
Requisitos principais

- Deverá permitir gerenciar políticas de acesso no conceito de Federação de Identidades (RF);

- Deverá permitir interpretar *request* e *response* do padrão XACML no conceito de federação de identidades (RF);

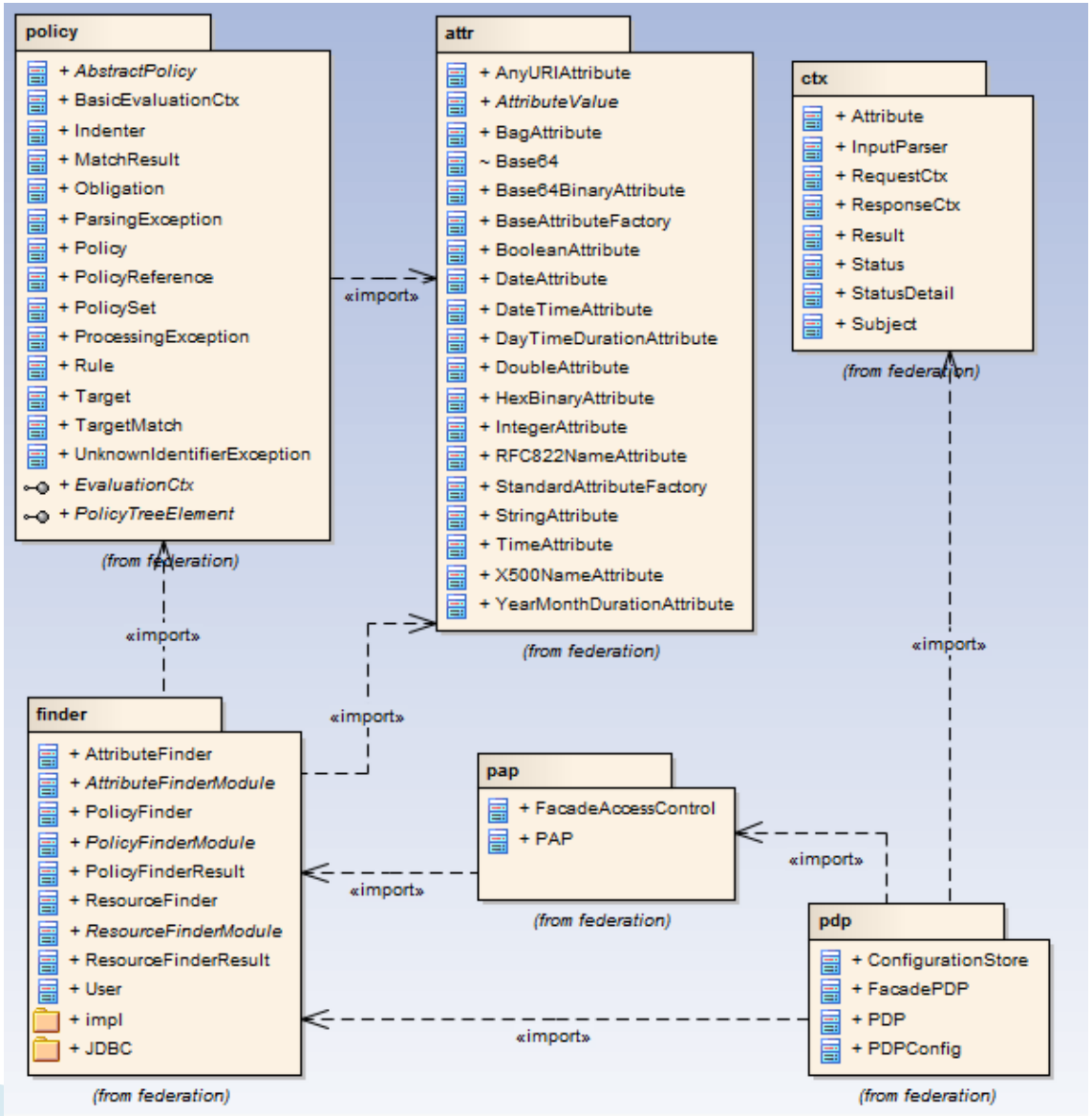
Especificação

- Caso de Uso – Ator Software



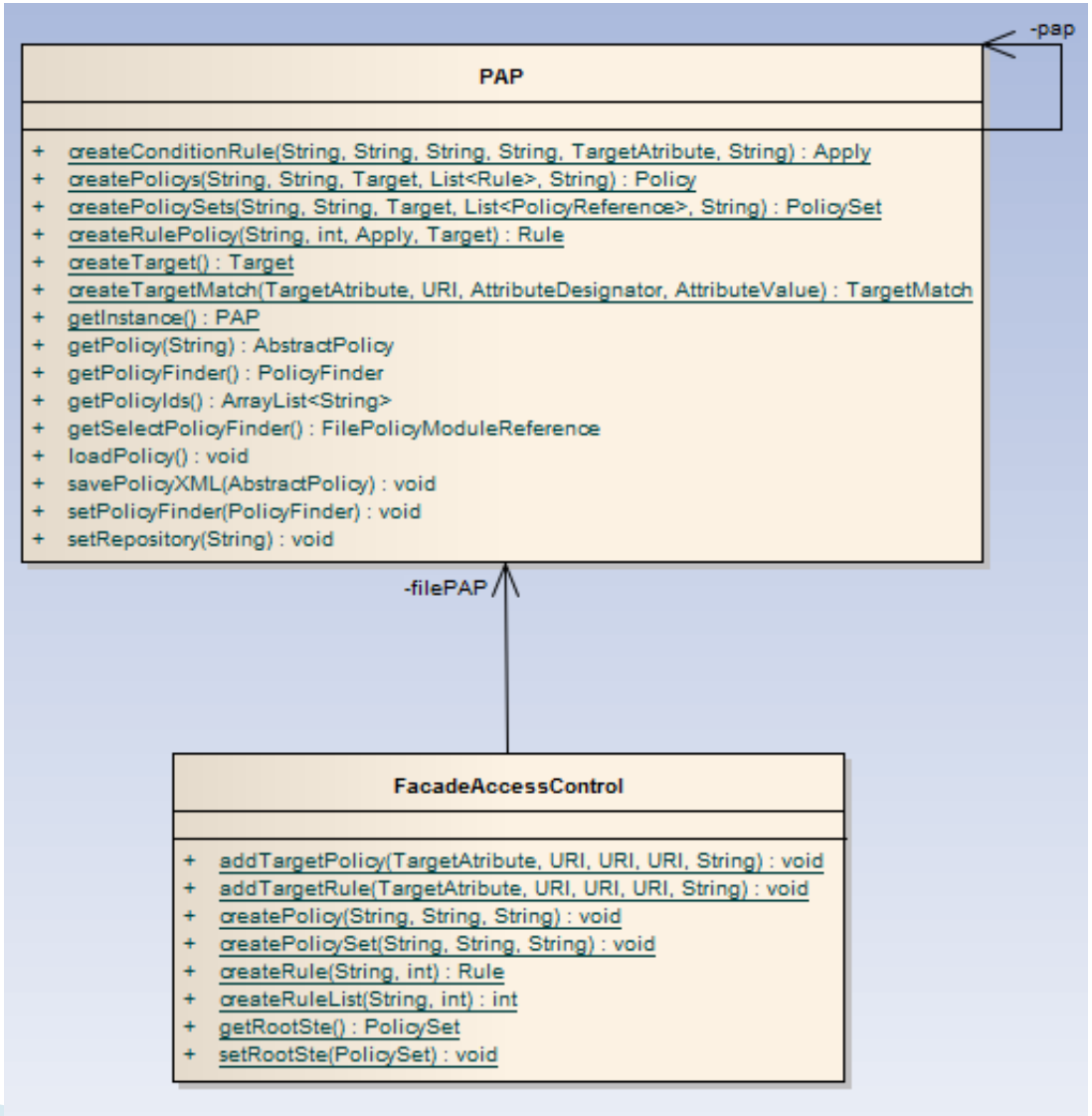
Especificação

- Diagrama de pacote da extensão.



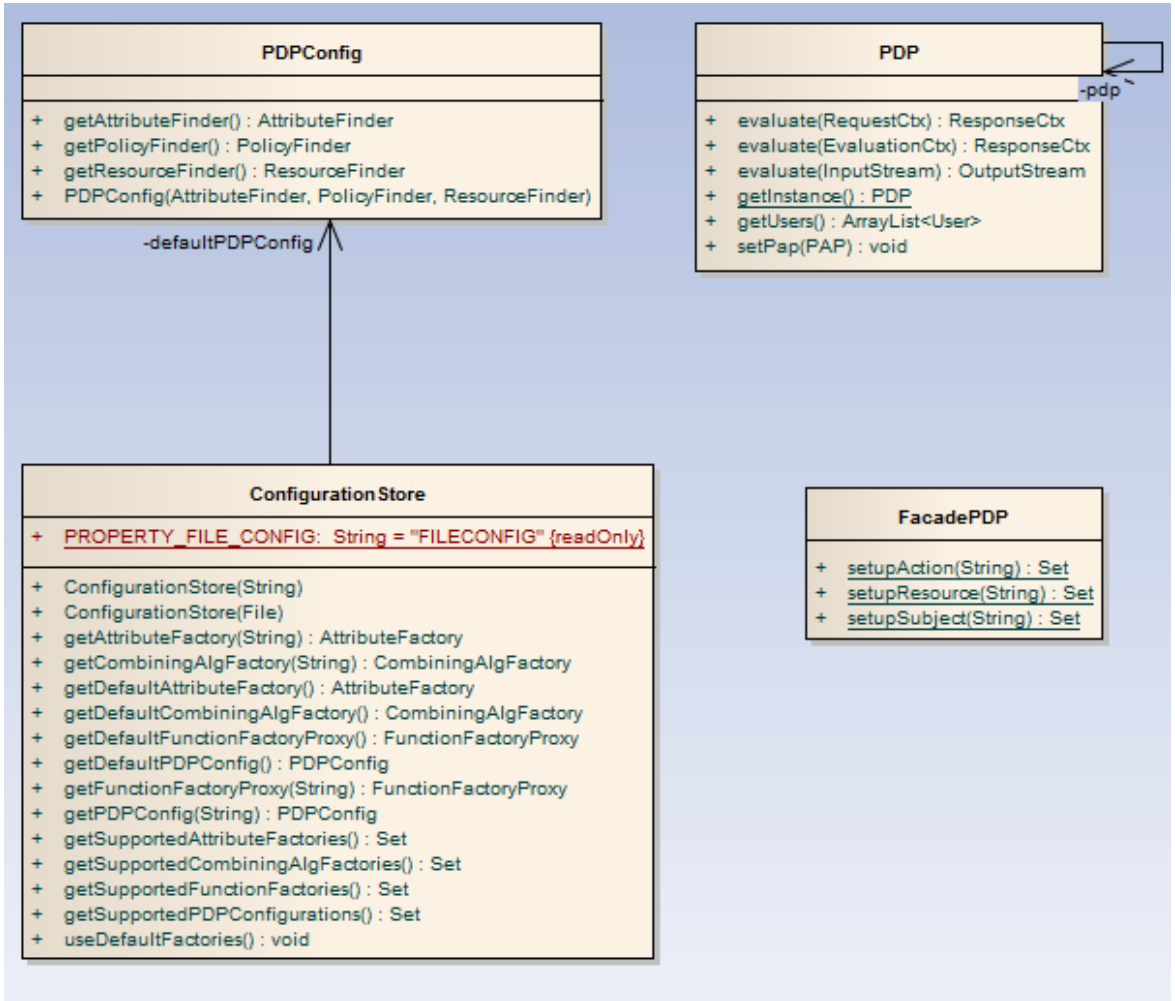
Especificação

- Diagrama de classes do pacote PAP.



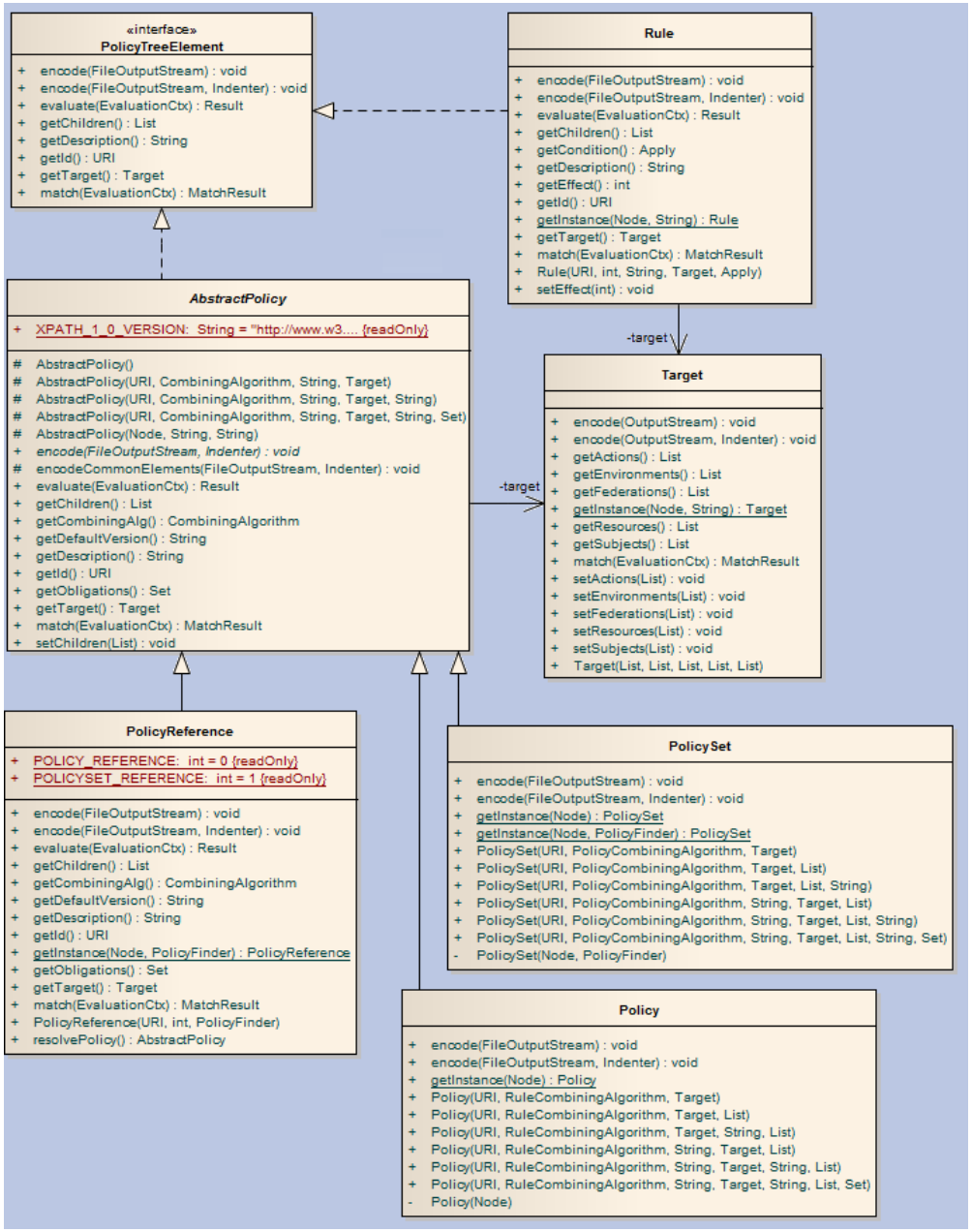
Especificação

- Diagrama de classes do pacote PDP



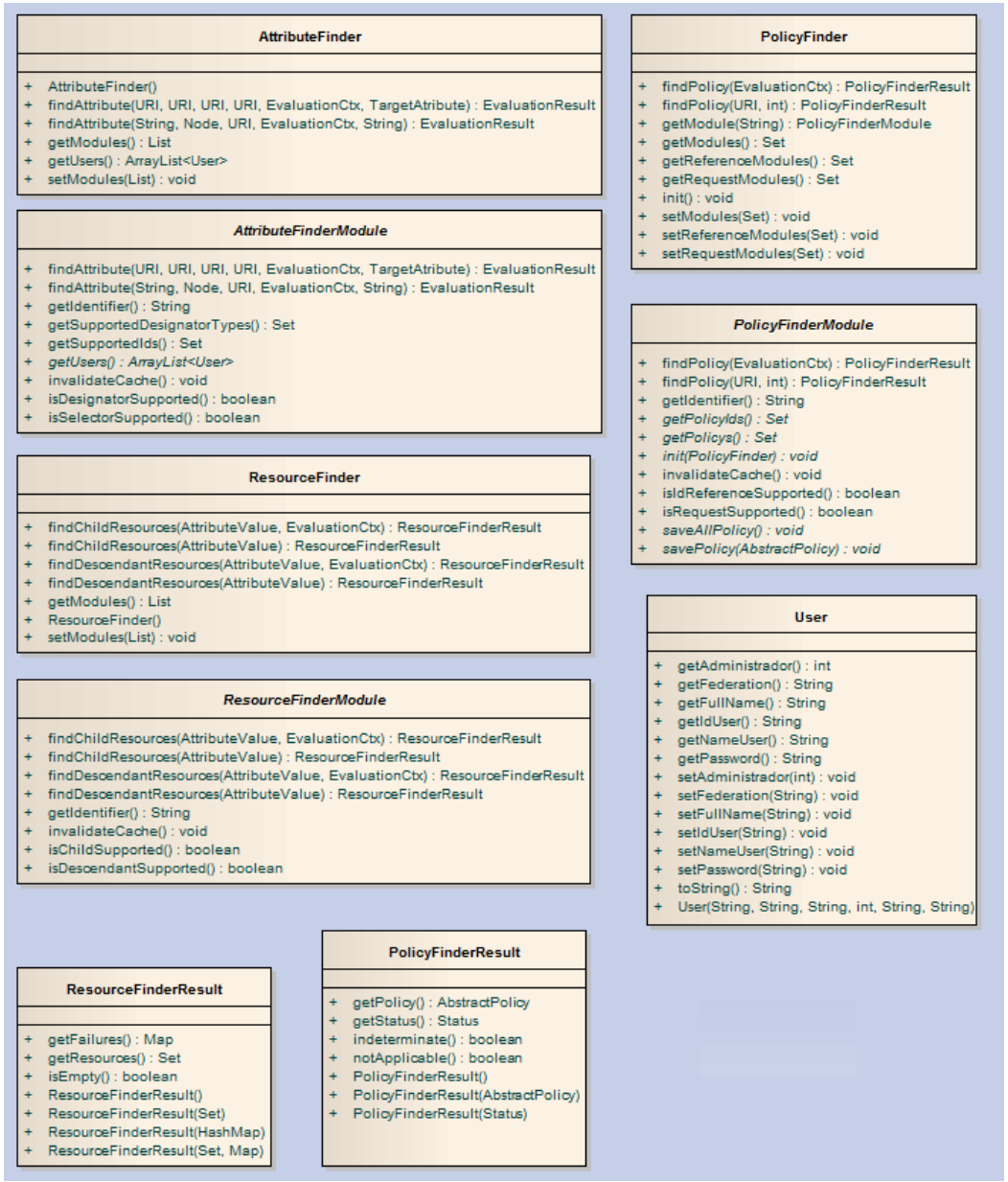
Especificação

- Diagrama de classes do pacote policy



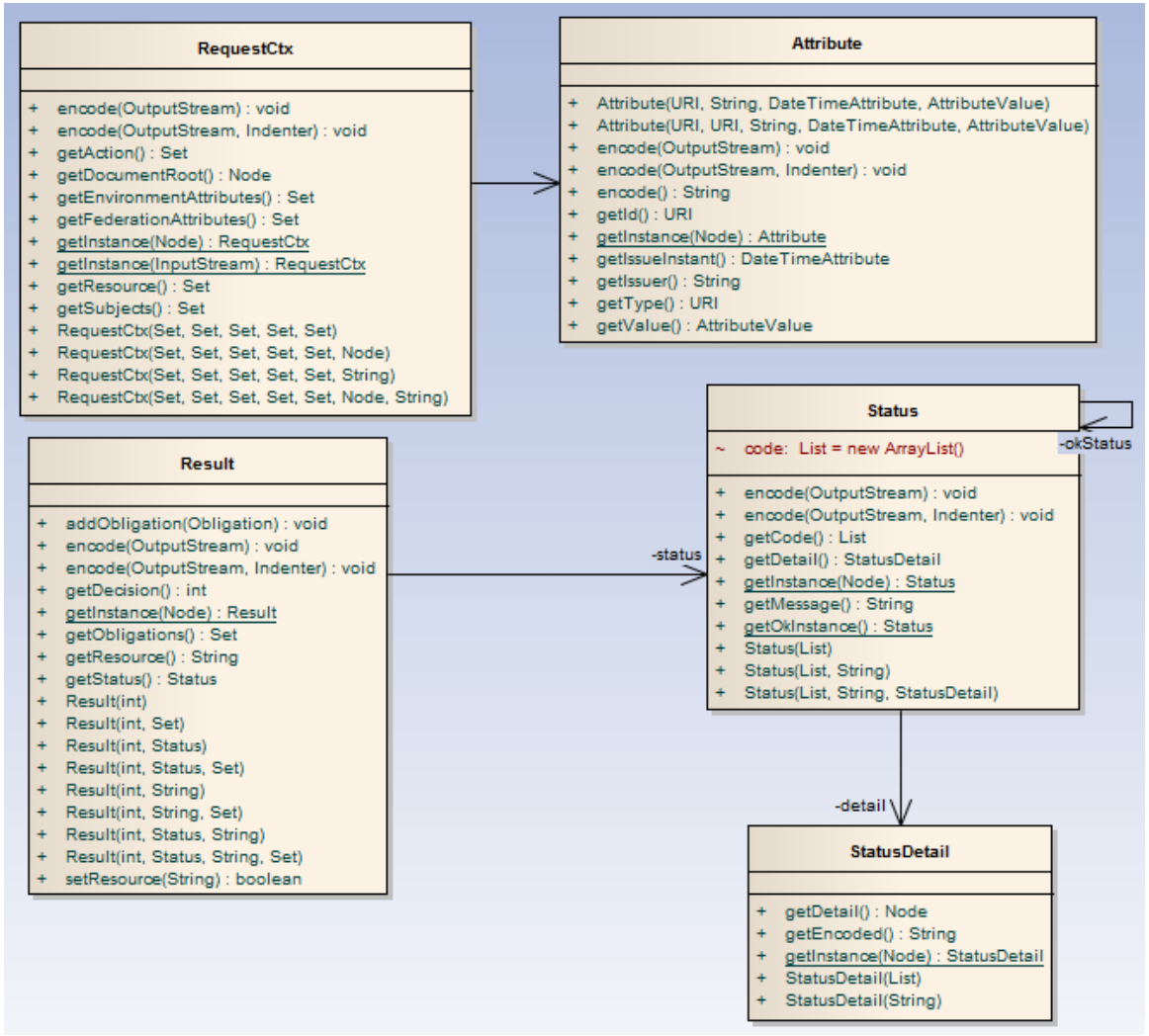
Especificação

- Diagrama de classes do pacote finder



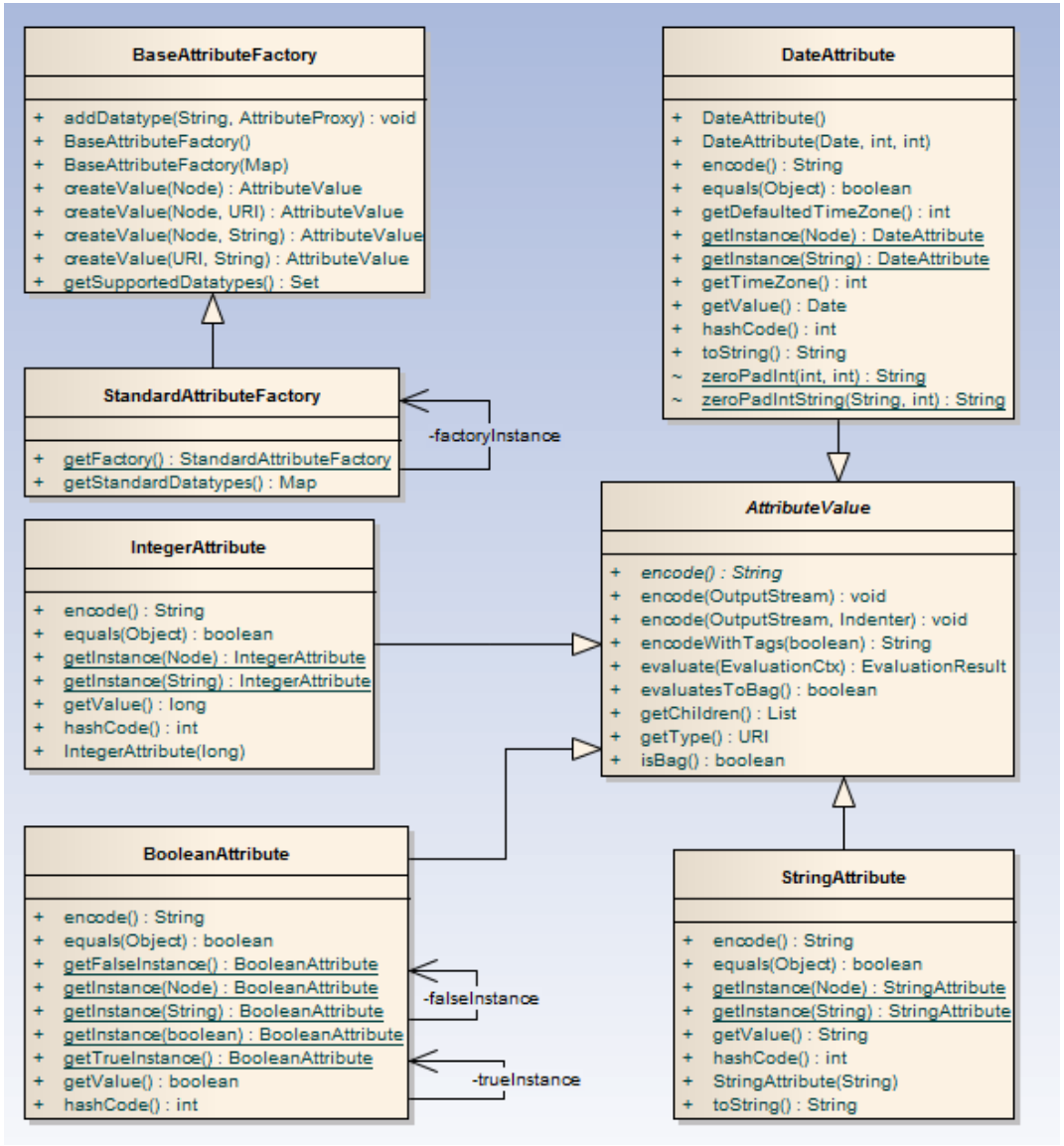
Especificação

- Diagrama de classes do pacote ctx



Especificação

- Diagrama de classes do pacote attr



Especificação

- Especificação *Schema* XML da estrutura de um *Target*

```
<xs:element name="Target" type="xacml:TargetType"/>
<xs:complexType name="TargetType">
    <xs:sequence>
        <xs:element ref="xacml:Subjects"/>
        <xs:element ref="xacml:Resources"/>
        <xs:element ref="xacml:Actions"/>
        <xs:element ref="xacml:Federations"/>
    </xs:sequence>
</xs:complexType>
```

Especificação

- Especificação *Schema* XML da estrutura de um *Request*

```
<xs:element name="Request" type="xacml-context:RequestType"/>
<xs:complexType name="RequestType">
    <xs:sequence>
        <xs:element ref="xacml-context:Subject" maxOccurs="unbounded"/>
        <xs:element ref="xacml-context:Resource"/>
        <xs:element ref="xacml-context:Action"/>
        <xs:element ref="xacml-context:Federation" />
    </xs:sequence>
</xs:complexType>
```

Especificação

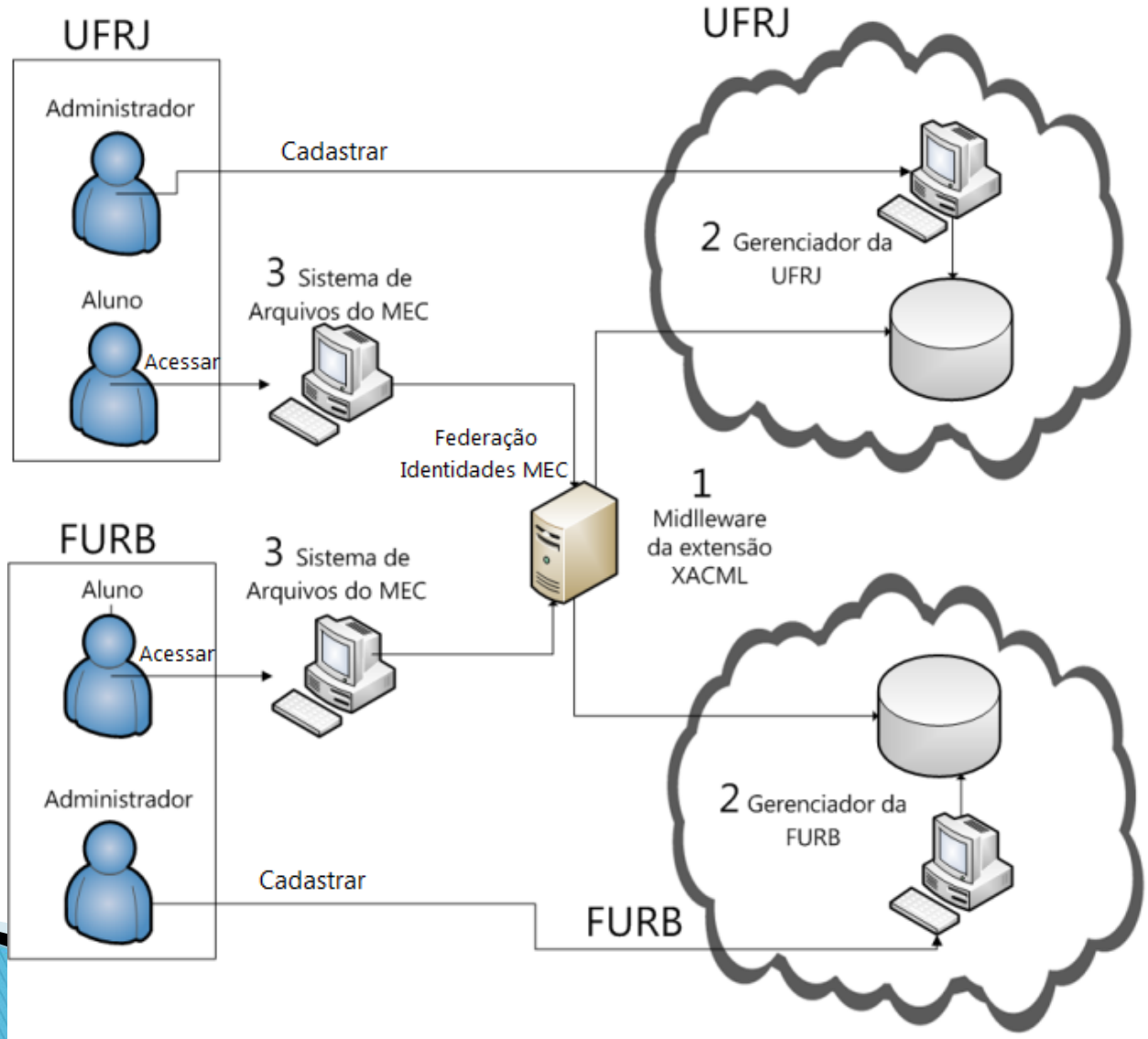
- Especificação *Schema* XML da estrutura do arquivo de configuração do PDP

```
<xs:element name="config">
    <xs:complexType>
        <xs:choice minOccurs="0" maxOccurs="unbounded">
            <xs:element name="confgfiles" type="config:ConfgFilesType"/>
            <xs:element name="pdp" type="config:PDPType"/>
            <xs:element name="attributeFactory" type="config:AttributeFactoryType"/>
            <xs:element name="combiningAlgFactory" type="config:CombiningFactoryType"/>
            <xs:element name="functionFactory" type="config:FunctionFactoryType"/>
        </xs:choice>
    </xs:complexType>
    <xs:attribute name="defaultPDP" type="xs:string" use="required"/>
    <xs:attribute name="defaultAttributeFactory" type="xs:string"
                  use="required"/>
    <xs:attribute name="defaultCombiningAlgFactory" type="xs:string"
                  use="required"/>
    <xs:attribute name="defaultFunctionFactory" type="xs:string"
                  use="required"/>
    <xs:attribute name="defaultFiles" type="xs:string" use="required"/>
</xs:element>
```

Tecnologias e ferramentas

- Linguagem de programação Java.
  - Orientação Objetos
  - Eclipse - Juno *Service Release* 2.
  - NetBeans 7.3.
  - Tomcat 7.0.
  - Apache Axis2/Java 1.6.2.
  - MySql Connector Java 5.1.24.
  - Sunxacml 1.2.
- MySQL Workbench 5.2.26 CE.
- Enterprise Architect 7.5.848.
- XML Tools Plugin 2.3.2.

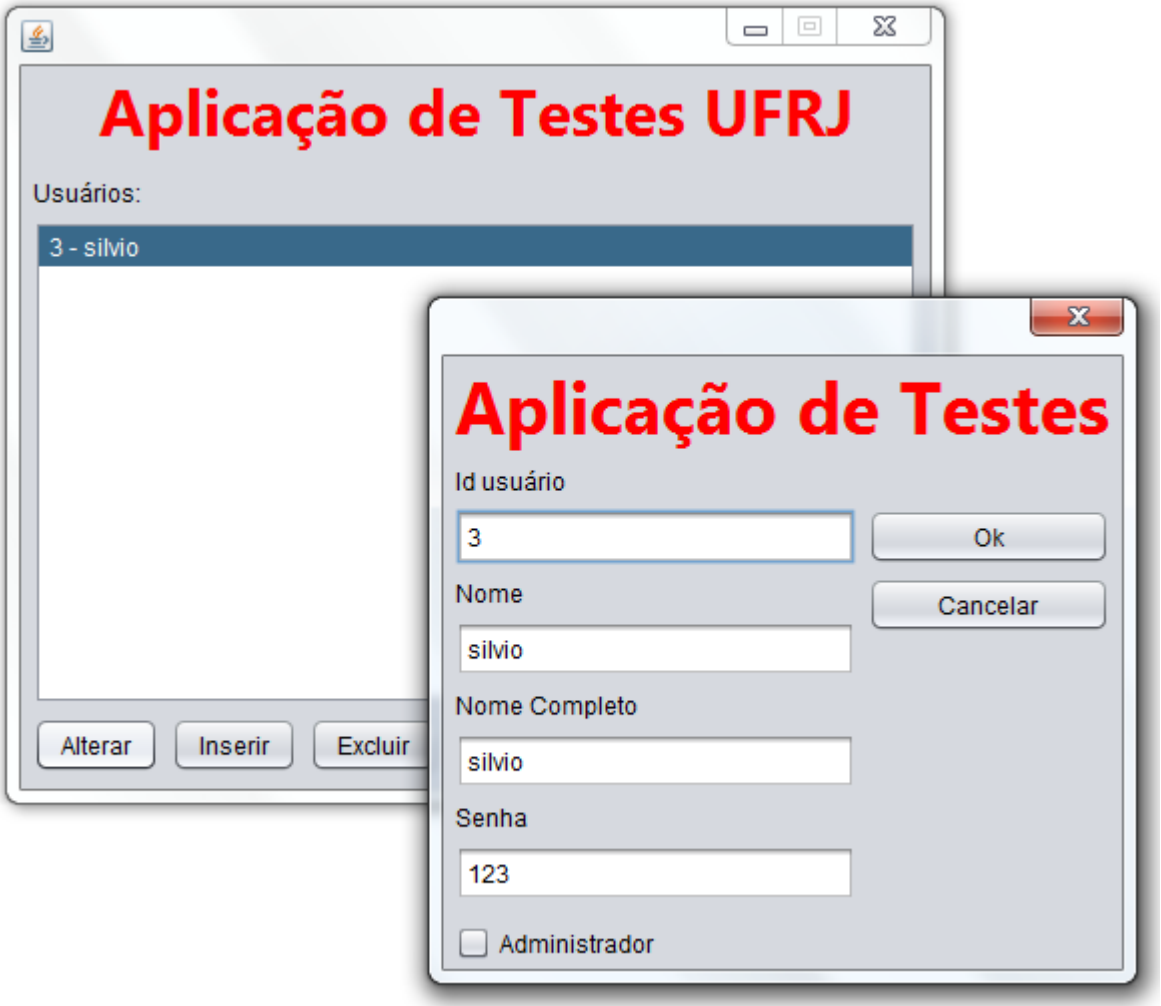
Operacionalidade



Operacionalidade

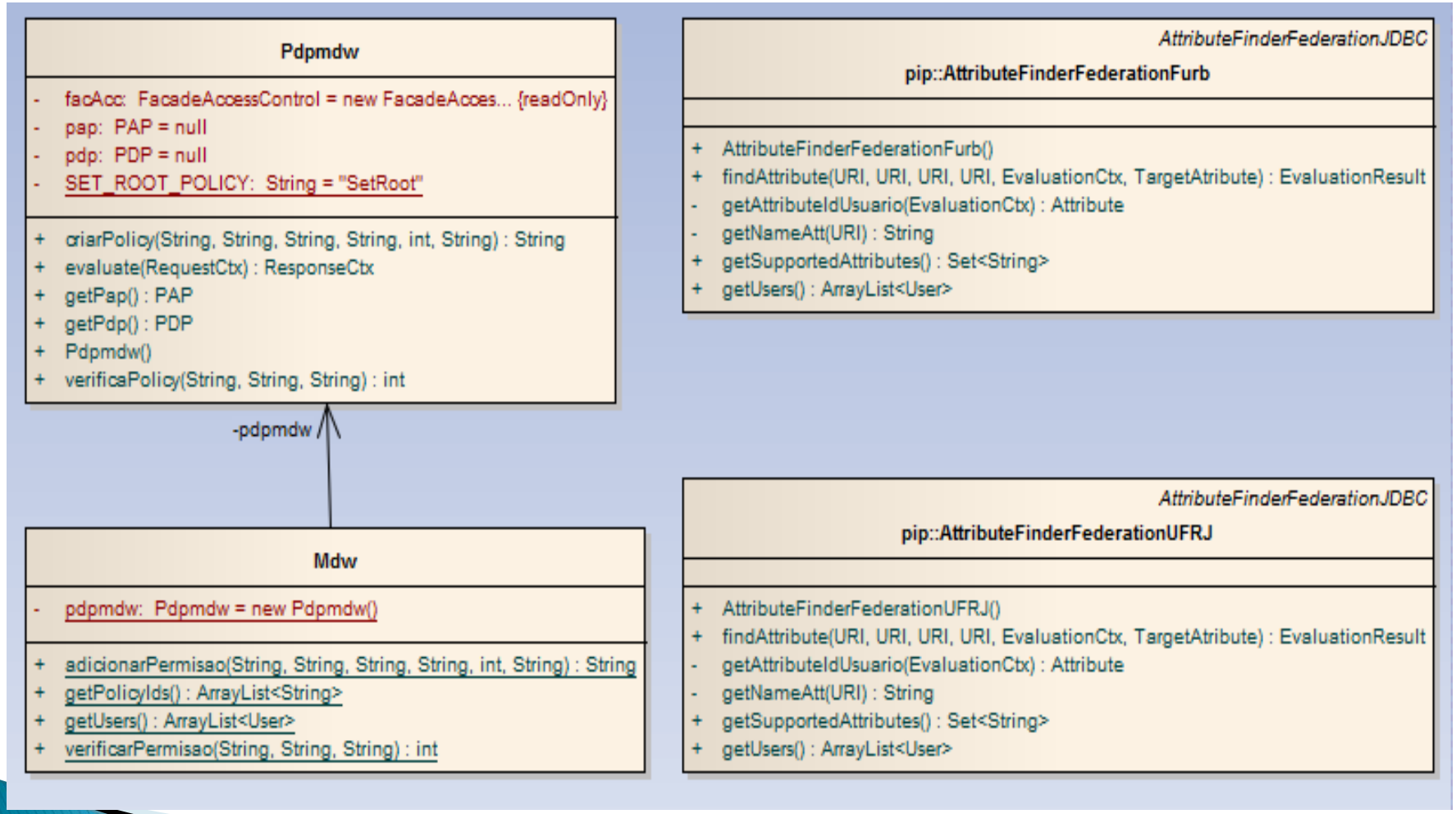
```
    defaultFiles="filesConfig" />
<confgfiles name="filesConfig">
    <policySchema class="">
        <string>C:\\Teste_XACML\\policy\\cs-xacml-schema-policy-01_FED.xsd</string>
    </policySchema>
    <contextSchema class="">
        <string>C:\\Teste_XACML\\request\\cs-xacml-schema-context-01_FED.xsd</string>
    </contextSchema>
</confgfiles>
<pdp name="pdpSample">
    <attributeFinderModule class="com.sun.xacml.federation.finder.impl.SelectorModule"/>
    <attributeFinderModule class="xacmlmdw.pip.AttributeFinderFederationFurb"/>
    <attributeFinderModule class="xacmlmdw.pip.AttributeFinderFederationUFRJ"/>
    <policyFinderModule class="com.sun.xacml.federation.finder.impl.FilePolicyModule">
        <list>
            <string>C:\\Teste_XACML\\policy\\SetRoot.xml</string>
        </list>
    </policyFinderModule>
    <policyFinderModule class="com.sun.xacml.federation.finder.impl.FilePolicyModuleReference">
        <list>
            <string>C:\\Teste_XACML\\policy\\</string>
        </list>
    </policyFinderModule>
</pdp>
```

Operacionalidade

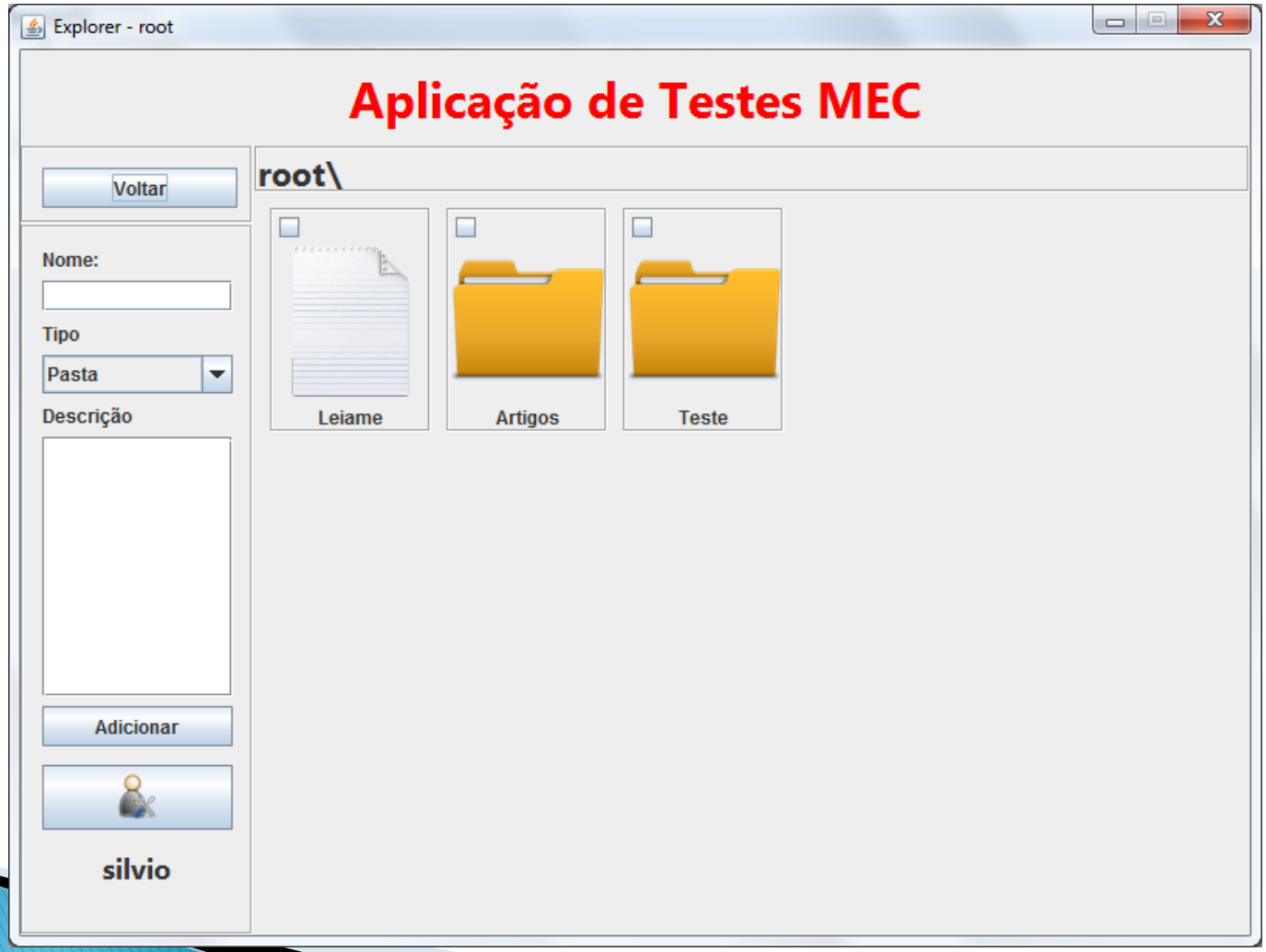


Operacionalidade

Operacionalidade



Operacionalidade



Resultados e Discussão

Características	Este Trabalho	Toktar(2003)	Leandro(2012)
Federação de Identidades	✓	x	✓
XACML	✓	✓	x
Extensão XACML	✓	✓	x
Java	✓	✓	✓
Utilizou outro Protocolo	x	x	✓
Modelo de Nuvem	✓	x	✓

Conclusões

- Os objetivos do trabalho foram atingidos;
- A linguagem XACML se demonstrou muito flexível e extensível;
- XACML e conceito de federação de identidades;
- A API Sun's XACML.

Extensões

- Autenticação de usuário considerando o conceito de federação de identidades.
- *Middleware* genérico.
- A extensão com JSON.

Demonstração da Extensão

OBRIGADO!