

Controle de Acesso

Prof. Vilmar Abreu Junior
vilmar.abreu@pucpr.br

Controle de Acesso

- Mecanismo de segurança que permite limitar **ações ou operações** que determinado sujeito (humano ou máquina) pode realizar **sobre um recurso**;
- Coexiste com outros serviços de segurança, como um serviço de **autenticação**;
- Utilizado **após** um usuário estar devidamente **autenticado**, ou seja, ele limitará o acesso a usuários **legítimos**.

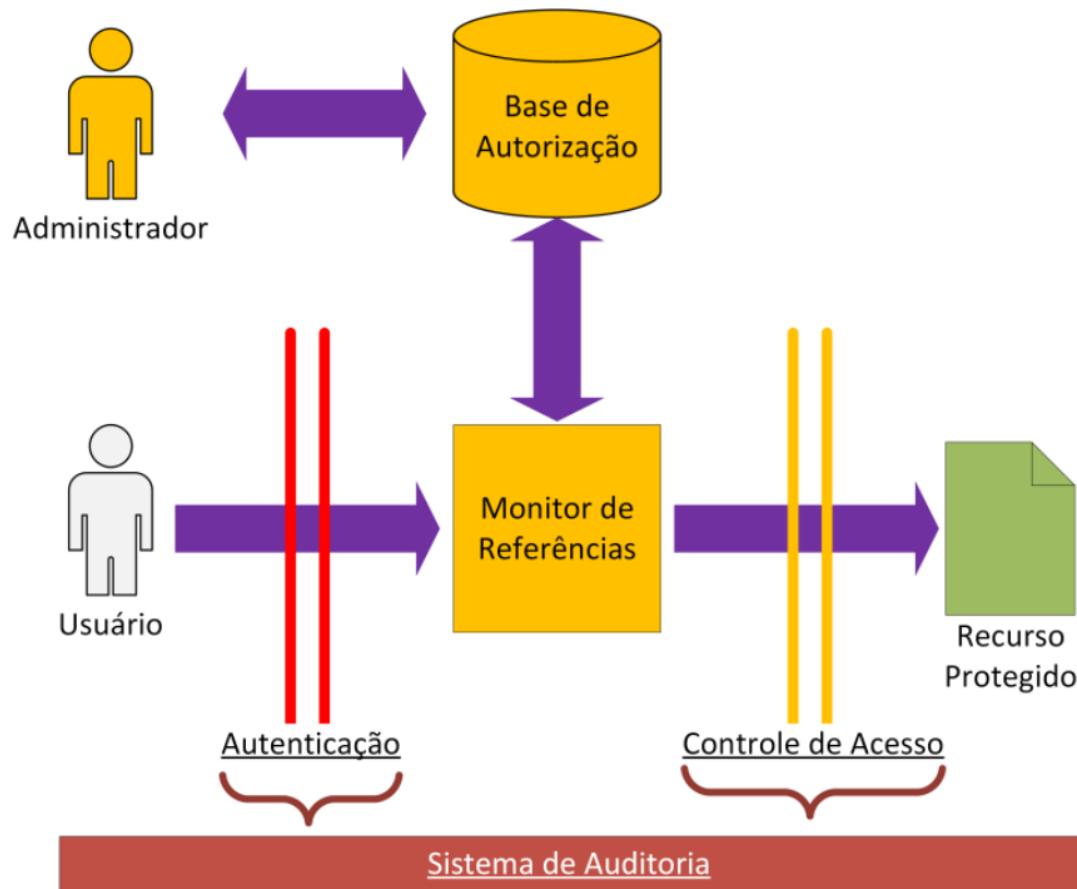
Elementos

- **Sujeito:** Entidade capaz de acessar recursos;
 - **Ex:** usuário, processo, etc;
- **Recurso:** Objeto cujo acesso é controlado;
 - **Ex:** Arquivos, diretórios, páginas, programas, mensagens, etc.
- **Direito de acesso:** Descreve o modo pelo qual um sujeito pode acessar um recurso;
 - **Ex:** Leitura, Escrita, Executar, Remover, Criar, Buscar, etc.

Arquitetura

- **Base de Autorização:** Na forma primitiva, é uma matriz de acesso (sujeito x recurso);
 - Cada célula representa a autorização do usuário sobre o recurso;
- **Monitor de Referências:** consulta uma base de autorização para intermediar o acesso de um recurso;
- **Guardião do Recurso (*enforcement*):** Executa a decisão do Monitor, permitindo ou negando o acesso do usuário ao recurso protegido.

Arquitetura (cont.)



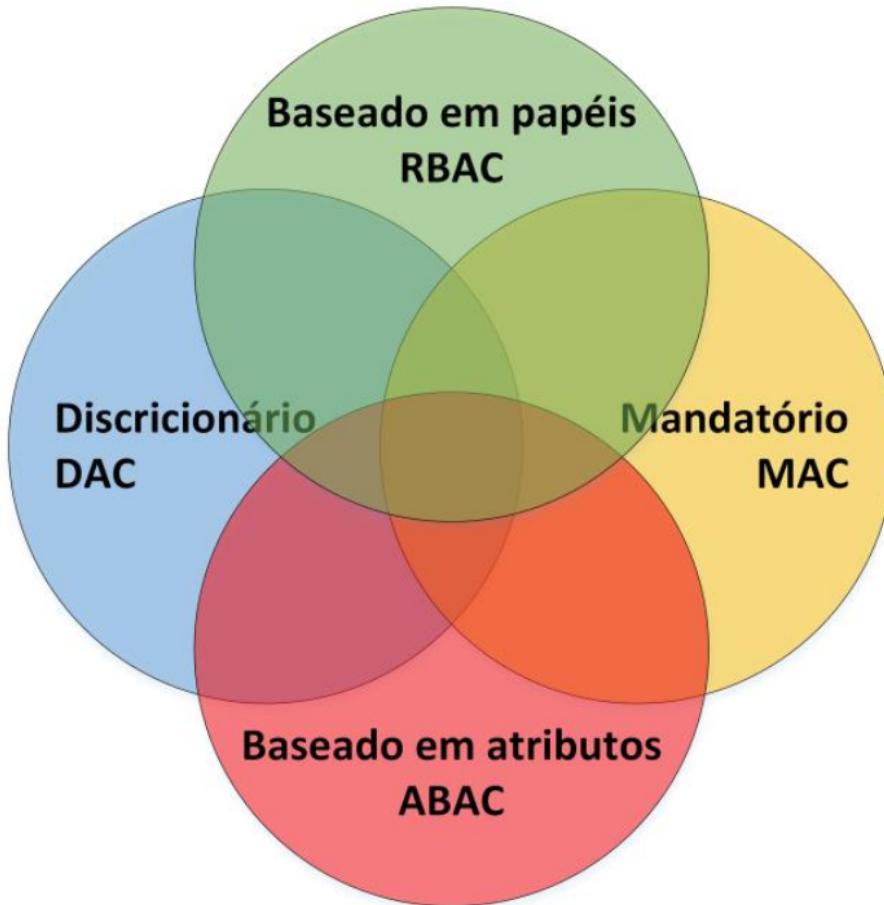
Exercício 01

- Desenvolva um programa que realize o controle de acesso. Para isso o programa deve armazenar previamente as políticas.
 - O usuário deve entrar com o login, ação e o recurso no programa, e o sistema deve:
 - Imprimir na tela: “Acesso permitido” caso exista uma política que permita esse acesso.
 - Imprimir na tela: “Acesso negado” caso não exista uma política que permita esse acesso.

Políticas

- As bases de autorização **contém** políticas de acesso, que determinam o **resultado** da decisão de acesso;
- As políticas mais **tradicionais** são as discricionárias, mandatórias, baseadas em papéis ou em atributos;
- É importante ressaltar que as políticas não são exclusivas, ou seja, podem ser **combinadas**.

Políticas (cont.)



Exercício 02

- Quebra cabeça de políticas de controle de acesso

XACML

- O XACML é um popular **framework** de controle de acesso, que define uma **linguagem** baseada em XML para escrita de políticas de controle de acesso, requisições e respostas;
- Adicionalmente, provê um mecanismo de **avaliação** das políticas de controle de acesso;
- Políticas baseadas em atributos (ABAC);

Exemplo de política

- Abrir o arquivo **[XACML] Politica.xml** pelo navegador.

Mecanismo de Avaliação

- O mecanismo de avaliação do XACML é composto dos seguintes elementos:
 - PAP (*Policy Administration Point*)
 - PDP (*Policy Decision Point*)
 - PEP (*Policy Enforcement Point*)
 - PIP (*Policy Information Point*)
 - Context Handler

Policy Administration Point (PAP)

- Atua como a **base de autorizações**;
- **Gerencia e armazena** as políticas de controle de acesso;

Policy Decision Point (PDP)

- Atua como a **monitor de referências**;
- **Avalia** o pedido de acesso de acordo com as políticas de controle de acesso produzindo a decisão de acesso (permitido ou negado);

Policy Information Point (PIP)

- Atua como central de informações/valores;
- Fornece informações (de acordo com as políticas) referente ao usuário, recurso e ambiente.

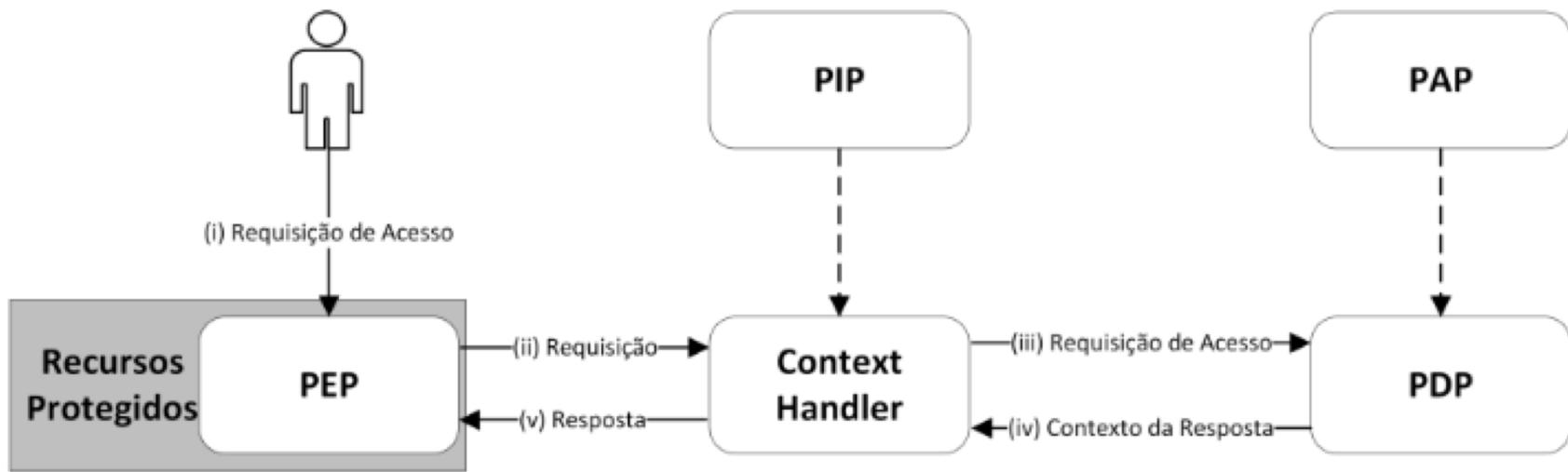
Policy Enforcement Point (PEP)

- Atua como a **guardião do recurso**;
- **Responsável** por encaminhar os pedidos de acesso para o PDP, e conceder o acesso de acordo com a decisão do PDP;

Context Handler

- Atua como **coordenador**;
- **Responsável** por realizar a coordenação, adequação e interoperabilidade de atributos, requisições e credenciais entre as entidades do XACML.

Arquitetura



Bibliotecas

- As principais bibliotecas que implementam a especificação do XACML são:
 - sunxacml (descontinuada)
 - WsO2 Balana



**ESCOLA
POLITÉCNICA**