Título: **Gestão de políticas de controlo de acesso a portas na UA**

Orientadores: André Zúquete (@ua.pt) e Pedro Fonseca (@ua.pt)
Elementos: 5

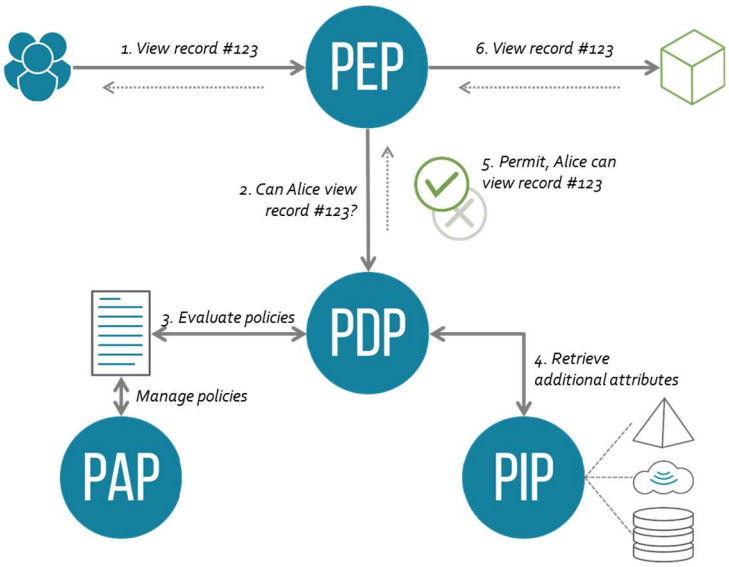
Contexto

O poder de abrir uma porta pode ser concretizado de várias formas, sejam a posse de um objeto (e.g. chave ou cartão RFID), o conhecimento de um segredo (e.g. PIN) ou a posse de uma característica biométrica (e.g. impressão digital). Nalguns casos esse poder pode ser transferido para terceiros (e.g. empréstimo da chave, divulgação do PIN), noutros não, permanece assoado ao seu detentor original.

Está neste momento em curso um projeto de alunos finalistas de várias licenciaturas tendo em vista a conceção de uma fechadura para portas de salas da UA. Esta fechadura tem uma componente mecânica e eletrónica que está a cargo dos alunos finalistas da LEEC e uma componente de interação com os utilizadores que está a cargo dos finalistas da LEIC. A componente que falta, e que foi prevista para os alunos finalistas da LEI, é a da gestão de políticas de controlo de acesso.

Objetivos

Neste projeto pretende-se conceber e concretizar uma plataforma de gestão de controlos de acesso. Esta plataforma deverá concretizar políticas de controlo de acesso às salas (quem pode aceder, quando pode aceder, etc.), políticas de notificação (quem deverá ser avisado de que foi feito um acesso a uma sala, quando é que isso deverá acontecer, etc.) e políticas de gestão das políticas de controlo de acesso às salas (quem pode gerir as políticas, quem deverá ser avisado das alterações realizadas, etc.). Usando como exemplo a arquitetura XACML [1] (ver Figura abaixo), pretende-se concretizar todas as componentes preconizadas exceto a PEP (Policy Enforcement Point), sendo que o PDP (Policy Decision Point) recebe sempre no pedido de decisão um atributo de identidade único de quem pretende aceder à sala. Eventuais atributos adicionais que possam ser necessários para o PDP avaliar as políticas de autorização devem ser obtidos via PIP a partir de perfis pessoais (por exemplo, para saber se o requerente é aluno ou não, se é aluno a que curso está associado, etc.).



Plano de trabalho

O trabalho será dividido nas seguintes tarefas:

- Estudo da arquitetura XACML e das linguagens de especificação de políticas de autorização;
- Definição de uma estrutura lógica de subdivisão e hierarquização das políticas de autorização que facilite a sua escalabilidade e gestão;
- Definição de grupos de requerentes (e.g. alunos de um curso, alunos de uma UC, docentes de um departamento, funcionários de um departamento, funcionários da UA, elementos da segurança, etc.);
- Concretização de políticas de autorização, tendo por base um identificador único fornecido por um PEP;
- Concretização de mecanismos de revisão das políticas de autorização (quem pode abrir uma porta num determinado instante, que portas pode abrir uma pessoa num determinado instante, etc.);
- Implementação e teste do sistema.

Referências

[1] OASIS, “eXtensible Access Control Markup Language (XACML) Version 3.0”, Candidate OASIS Standard 01, 26 September 2012, https://docs.oasis-open.org/xacml/3.0/xacml-3.0-core-spec-cos01-en.html