

Ana Correia - 31831

Diogo Cardoso - 32466

João Silvestre - 32766

29/11/11

*Instituto Superior Engenharia de Lisboa*

**3ª Serie**

Engenheiro: José Simão

Engenharia Informática e de Computadores

Semestre de Inverno 2011/2012

Índice

[Parte Teórica 4](#_Toc310375430)

[Exercício 1 4](#_Toc310375431)

[Alínea 1 4](#_Toc310375432)

[Alínea 2 4](#_Toc310375433)

[Alínea 3 4](#_Toc310375434)

[Alínea 4 5](#_Toc310375435)

[Alínea 5 5](#_Toc310375436)

[Exercício 2 5](#_Toc310375437)

[Exercício 4 6](#_Toc310375438)

[Parte Prática 7](#_Toc310375439)

[Exercício 5 7](#_Toc310375440)

[Alínea 1 8](#_Toc310375441)

[Exercício 6 9](#_Toc310375442)

[Exercício 7 10](#_Toc310375443)

# Parte Teórica

# Exercício 1

## Alínea 1

A diferença ente o “**dono de recursos**” e o “**cliente**” dada pela especificação do protocolo é, o “dono de recursos” é a entidade capaz de autorizar o acesso a um recurso protegido. O “cliente” é a aplicação que acede ao recurso protegido em nome do dono do recurso e com a sua autorização.

## Alínea 2

O perfil “***web application***” descreve aplicações em que a interacção feita com o *authorization server* para se obter o *access token* é feita pelo servidor web, longe da máquina do dono do recurso. Neste perfil o cliente web inicia o pedido de autorização que irá redireccionar o browser do dono do recurso para o *authorization server*, incluindo o seu identificador de cliente, um uri para para onde o *authorization server* deve redireccionar o browser do dono do recurso quando este tomar a sua decisão, entre outros dados. Este irá então autorizar ou negar o acesso do cliente ao recurso, caso autorize, o *authorization server* irá redireccionar então o browser do dono do recurso para o cliente e a obtenção do *access token* irá então ser feita no servidor web do cliente.

O perfil “***user-agent-based application***” descreve aplicações implementadas num browser, tipicamente em linguagens de scripting (JavaScript). Nestas aplicações, não é possível manter o segredo do cliente secreto, pois uma qualquer aplicação na máquina do dono do recurso poderia ter acesso ao segredo do cliente, portanto a autenticação do cliente é feita numa política de “*same-origin”*. Neste perfil o *access token* vem no *redirect* do *authentication server* e é acedido apenas no *browser* do dono do recurso.

## Alínea 3

Enquanto o “*access token*” é utilizado pelo cliente para fazer pedidos autênticados em nome do dono do recurso o “*authorization token”* é um de 4 tipos de “*access grants”* que representam a intenção do dono do recurso de dar ao cliente acesso para o recurso protegido, estes *“access grants*” podem depois ser usados para obter o “*access token*”.

## Alínea 4

Um atacante poderia conseguir alterar o *redirect* URI do *authorization token* ou no caso de um perfil “*user-agent*” poderia conseguir alterar o redirect do *access token*. Uma das formas previstas para impedir este ataque passa por permitir um registo de *redirect* URI, desta forma o atacante nunca poderia mudar o URI para algo seu. No primeiro caso, também existe outra protecção pois para obter um *access token* através do *authorization token* é preciso conhecer o segredo do cliente, que deverá estar bem seguro no servidor web do cliente.

# Bibliografia

(s.d.). Obtido em 8 de 1 de 2012, de http://tools.ietf.org/html/draft-ietf-oauth-v2-10#page-5

(s.d.). Obtido em 8 de 1 de 2012, de SpringSource: http://blog.springsource.org/2011/11/30/10317/