Configuração da autenticação centralizada em páginas Web

A biblioteca do sistema de autenticação centralizada (CAS) oferece uma *Application Programming Interface (API)* simples que permite a autenticação de utilizadores.

Para integrar a autenticação centralizada em páginas Web do IST, o utilizador deverá começar por verificar se o serviço Web no self-service do IST está ativo.

Todas as páginas que necessitem de autenticação centralizada devem ter o seguinte código em PHP:

```
<?php
// Import server's phpCAS library.
// Try '/usr/share/php/CAS.php' if simply 'CAS.php' does not work.
require_once 'CAS.php';
// Initialize phpCAS
phpCAS::client(CAS_VERSION_3_0,'id.tecnico.ulisboa.pt',443,'/cas');
// Set CAS server certificate
phpCAS::setCasServerCACert('/etc/ssl/certs/ca-certificates.crt');
// Set logout handler
phpCAS::handleLogoutRequests(true, array('id.tecnico.ulisboa.pt'));
// Force CAS authentication
phpCAS::forceAuthentication();
// If the code reaches this step, the user has already been authenticated by the CAS server
// and the user's IST ID can be read with phpCAS::getUser().
?>
```

Atenção: *Os servidores que disponibilizam o serviço Web da DSI já dispõem de uma biblioteca CAS, tornando assim desnecessário descarregar a biblioteca à parte para a sua área pessoal. No exemplo acima é utilizada a bilbioteca CAS do servidor Web. Se pretender utilizar outra biblioteca CAS é responsável por assegurar a actualização da mesma.*

Se tudo tiver funcionado correctamente poderá aceder ao IST ID do utilizador autenticado da seguinte forma:

```
<?php
$user = phpCas::getUser();
// If all is right the next line will print the user's IST ID.
echo("Hello " . $user . "!");
?>
```

Para fazer logout deverá utilizar a função que se segue:

```
<?php
// This will logout the user from all services
phpCAS::logout();
?>
```

Atenção: *Esta função fará logout de todas as aplicações que utilizem a autenticação centralizada do IST!*

Atenção: *Fazer logout no sistema de autenticação centralizada não termina automaticamente a sessão na sua aplicação. Deve garantir que isso ocorre também!*

Fechar a página ou o browser ou chamar a função de logout por si só também não garante que a sessão autenticada fique invalidada! Uma possível consequência é que se dois utilizadores se autenticarem no mesmo browser (por exemplo num computador público), o segundo utilizador poderá ficar com a sessão do utilizador anterior. É da inteira responsabilidade dos administradores da página Web prevenir que essa situação ocorra.

Invalidar a sessão autenticada

Para invalidar a sessão de uma aplicação Web que utiliza a autenticação centralizadada é necessário executar o seguinte código em PHP:

```
<?php
session_start();
session_destroy();
session_unset();
$_SESSION=array();
exit();
?>
```

Para aceder a uma página com autenticação CAS é necessário utilizar o protocolo **HTTPS**, caso contrário receberá a mensagem **"Aplicação não autorizada a usar o Serviço de Autenticação Central"**.