ISEL

Authentication and Authorization Node component

Alunos:

- **Nome:** João Barata **nº** 44857 **Tel.:** +351 918673224 **E-mail:** A44857@alunos.isel.pt
- **Nome:** Diogo Leandro **nº** 44868 **Tel.:** +351 967564849 **E-mail:** A44868@alunos.isel.pt
- **Nome:** Tiago Matias **nº** 44827 **Tel.:** +351 910891726 **E-mail:** A44827@alunos.isel.pt

Coordenador e Co-Coordenador:

- Eng. João Pereira **E-mail:** joao.pereira@gfi.world
- Eng. José Simão **E-mail:** jsimao@cc.isel.pt

Data: 10/03/2020

Introdução:

Nos dias que correm existe, principalmente no contexto de desenvolvimento aplicacional, uma enorme necessidade de garantir e confirmar a identidade de utilizadores que pretendem aceder a uma determinada aplicação. Como tal este será o tema abordado no nosso projeto.

Dois conceitos importantes acerca deste tema são a autenticação e a autorização de utilizadores.

Autenticação é o ato de confirmar a identidade de alguém e é necessária para percebermos que autorizações tem o utilizador autenticado.

Autorização representa um meio para condicionar o acesso a determinados recursos privados. Assim sendo, o objetivo deste projeto é simplificar e automatizar todo este processo de autenticação e autorização de utilizadores. O projeto vai consistir em vários blocos como demonstrado no diagrama mais à frente, mas de uma forma muito sucinta podemos dizer que irá ter uma base de dados contendo as informações dos vários utilizadores, informações estas que vão ser cuidadas de acordo com o RGPD e que serão encriptadas de maneira a proteger o utilizador e irá ter também uma api que vai ter acesso à base de dados de forma a poder responder aos pedidos que lhe irão ser feitos, pedidos estes que irão ser feitos pela última componente do nosso projeto que será a nossa web application.

A ordem de acontecimentos neste projeto irá ser: um pedido de autenticação proveniente de uma third party application ou da nossa web application, esse pedido vai ser respondido pela nossa api, de seguida a api vai ter de pesquisar na nossa base de dados com a ajuda do data access layer, quando obtiver as informações necessárias para a resposta envia-a.

There is little point in doing a project that merely regurgitates the work of others. Your own though, ideas and developments are important, and these are what people reading your report are interested in. Through your project you will develop not only your own skills, but also the ideas and work of others.

Dawson, C., 2009, Projects in Computing and Information Systems, Second Edition, Pearson Education Limited, Essex, England

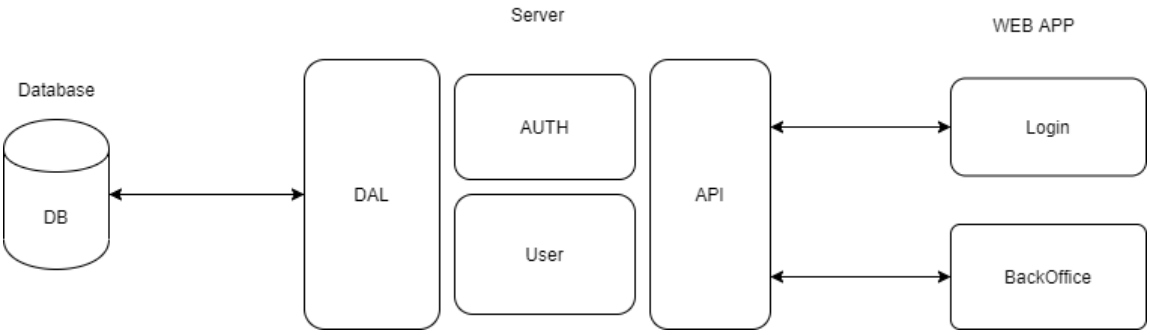

Figure 1 -Diagrama de Blocos do Projeto

Objetivos:

- Desenvolver ferramentas genéricas que possam ser utilizadas por third parties;
- Desenvolver competências de trabalho escolar crítico e independente;
- Adquirir conhecimento sobre os diferentes protocolos de rede e de autenticação;
- Garantir comunicações seguras e identificadas;
- Garantir que é devidamente cumprido o RGPD (Regulamento Geral de Protecção de Dados);
- Discutir padrões de arquitetura procurando uma solução geral e reutilizável;
- Aplicar conhecimentos adquiridos no percurso académico pelos intervenientes;
- Adquirir e consolidar conhecimentos sobre Aplicações Web;
- Adquirir e demonstrar conhecimentos e habilidades de programação em JavaScript.

Justificação:

O projecto permitirá aos alunos aplicar desenvolver e fortalecer, conhecimentos adquiridos ao longo do percurso académico tais como Programação Assincrona, Desenvovimento de API's e desenvolvimento de sistemas de informação seguindo os protocolos comuns da indústria. Como tal este servirá como momento pedagógico para os intervenientes, preparando-os para situações de mundo real e proporcionando-lhes não só as competências teóricas mas também o know-how cada vez mais relevante no mundo do trabalho.

Este projeto é, na sua grande maioria, baseado em autenticação e autorização de clientes ao servidor, como tal, este tópico exigirá aos alunos a aquisição de habilidades técnicas no uso das tecnologias Kerberos, openId e SAML. É evidente a existência e necessidade de realizar um produto com alto nível de segurança para tal, é necessário existir uma profunda análise em cada decisão tomada.

ISEL

Âmbito do Projeto:

O projeto a realizar deve ser genérico e modular, ou seja, não pode restringir a web app que o integra a uma determinada estrutura visto que tem como objectivo ser incorporado numa aplicação preexistente da gfi.

Embora a elaboração do projeto siga as diretivas e ideais da gfi qualquer aplicação web que pretenda utilizar o módulo, poderá fazê-lo se respeitar o protocolo e documentação do mesmo.

Este módulo permite:

* Autorizar e autenticar utilizadores a uma determinada aplicação de forma simples

* Gerir e controlar as permissões de acesso a recursos por determinados utilizadores

* Gestão de diferentes sessões de um mesmo utilizador em diferentes clientes.

* Gestão de listas negras e cinzentas

Abordagem e Resultados:

Este projeto será realizado utilizando a linguagem Javascript pois consideramos ser a linguagem mais apropriada para desenvolvimento de aplicações web onde será também utilizado o NodeJS como interpretador javascript devido á sua performance e escalabilidade.

Para a gestão da base de dados iremos usar o MYSQL/MariaDB pois este projeto irá ser integrado futuramente com uma third party application que utiliza MYSQL/MariaDB.

Serão utilizados padrões/protocolos de autenticação e autorização tais como o SAML ,OAuth e Kerberos.

O OpenID irá também ser utilizado para inserir uma camada de identidade ao protocolo OAuth.

A nossa web application vai ser uma SPA (Single Page Application) pois tendem a ser mais rápidas do que as MPA's (Multiple Page Application) devido à maior parte dos seus recursos ser carregada apenas uma vez, pretendemos também utilizar a biblioteca ReactJS, pois achamos ser importante aprender a utilizar esta tecnologia visto que é neste momento uma das tecnologias mais utilizadas para a elaboração de user interfaces.

Para gerir configurações e permissões de utilizadores iremos utilizar um RBAC (Role-based access control) definindo posteriormente os diferentes roles e respetivas permissões.

Por fim o nosso web server vai utilizar o express pois é uma solução bastante fácil de usar e que vai de acordo com o que nós pretendemos na definição de endpoints e além disso tem compatibilidade com o passport, ferramenta que iremos usar bastante para a autenticação de utilizadores.

Obstáculos:

Este projeto requer que exista bastante pesquisa e bastante espírito crítico sempre em busca de maximizar a eficiência e garantir a segurança durante todo o processo de autenticação.

Como este projeto utiliza também as identidades dos diferentes clientes, poderá ser um obstáculo encontrar uma solução que respeite o Regulamento Geral sobre a Protecção de Dados.

A gestão de diferentes sessões do mesmo utilizador também pode vir a ser um obstáculo neste projeto, visto ser um desafio diferente do que os alunos têm encontrado ao longo do seu percurso.

Plano do Projeto: