# A blue and white sign with textPrivacidade e Segurança de Dados

## Mestrado em Engenharia Informática

**Relatório Grupo 66**

**Introdução:**

Este projeto tem como objetivo desenvolver uma aplicação de mensagens peer-to-peer (P2P) segura, que permite a comunicação direta entre utilizadores, garantindo a privacidade e a integridade das mensagens. Inspirada em plataformas como WhatsApp e Signal, a aplicação foi desenhada para oferecer uma experiência de comunicação descentralizada e segura, onde apenas o remetente e o destinatário têm acesso ao conteúdo das mensagens, protegendo-as contra interceções e modificações

A aplicação foi desenvolvida em Java e utiliza comunicação baseada em SSL Sockets para estabelecer uma camada de segurança sobre o protocolo de transporte. Com SSL (Secure Sockets Layer), é possível assegurar que as mensagens trocadas entre os utilizadores estão encriptadas e protegidas contra acessos não autorizados. Esta abordagem permite que a aplicação forneça criptografia de ponta a ponta, autenticação dos utilizadores e verificação de integridade das mensagens, cumprindo assim os requisitos de segurança fundamentais de um sistema de mensagens P2P.

**Novas funcionalidades implementadas:**

Para além das funcionalidades implementadas na primeira entrega foi adicionada a funcionalidade de pesquisa de mensagens e, para além disso, as mensagens deixaram de ser guardadas localmente e passaram a ser guardadas na cloud. Para isto criamos 4 replicas na AWS, 4 na Firebase e 4 na Microsoft. Abaixo está uma imagem do frontend com esta nova funcionalidade implementada.

Figura 1 - Funcionalidade de pesquisa de mensagens



Para além desta funcionalidade decidimos também implementar um comando que permite limpar todas as mensagens que existam na cloud dum certo user ( tal comando está explicado no documento HTR.txt enviado no zip da entrega ). Achamos esta funcionalidade interessante, visto que o professor não tem acesso à nossa conta da cloud e, desta maneira será mais fácil de testar o nosso projeto.

**Garantias de segurança oferecidas:**

Para garantir a segurança nas comunicações, utilizamos SSL Sockets para estabelecer conexões diretas e encriptadas entre utilizadores, permitindo que as mensagens trocadas sejam protegidas contra intercepções. Cada utilizador (peer) cria um SSL Socket para comunicar diretamente com outro utilizador, garantindo assim a privacidade dos dados enviados e recebidos e uma interação descentralizada, além disso no momento do login cada user cria uma keyStore para guardar a sua chave pública e certificado e uma trustStore para guardar os certificados de outros user que considere confiáveis. Para se guardar os dados de cada user criou-se um servidor que consegue comunicar com cada user, de maneira a fornecer informações de outros utilizadores que estejam ativos, este sua keyStore e trustStore tal como os user e para além disso, gera também um ficheiro com o seu próprio certificado.

A cipher suite utilizada na aplicação é a TLS\_ECDHE\_RSA\_WITH\_AES\_256\_GCM\_SHA384, configurada com o protocolo TLSv1.2. Ela combina o algoritmo ECDHE (Elliptic Curve Diffie-Hellman Ephemeral) para troca de chaves segura, garantindo a criação de uma chave secreta compartilhada; RSA (Rivest-Shamir-Adleman) para autenticação das partes, assegurando que cliente e servidor sejam confiáveis; AES-256 em modo GCM para criptografia eficiente dos dados, oferecendo também verificação de integridade; e SHA-384 (Secure Hash Algorithm) para garantir que as mensagens trocadas não sejam alteradas.

TODO: explicar a segurança implementada na cloud, como é criada a chave que encripta as mensagens enviadas, como fica a estrutura na cloud (isto pode ser feito com uma imagem) e como é feita a recuperação de chaves no momento de login.

**Benefícios de Segurança:**● Privacidade e Confidencialidade: A utilização do algoritmo AES-256 em modo GCM para criptografia assegura que todos os dados trocados entre os peers sejam encriptados, garantindo que apenas as partes envolvidas possam acessar o conteúdo das mensagens.

● Autenticidade: O uso do algoritmo RSA para autenticação, juntamente com a verificação de certificados via KeyStore e TrustStore, garante que os peers estão a comunicar com entidades confiáveis, evitando interações com agentes maliciosos.

● Integridade dos Dados: O modo GCM de operação do AES, aliado ao hash seguro SHA-384, protege contra alterações nos dados durante a transmissão, assegurando quequalquer tentativa de modificação seja detetada.

● TODO – explicar que a privacidade dos utilizadores não é violada, e que o conteúdo das mensagens não é descoberto, visto que as mensagens estão encriptadas

TODO – Fazer a conclusão