# End-to-End Encrypted Messaging Application

## Introduction

The End-to-End Encrypted (E2EE) messaging application is designed to address the privacy and security concerns associated with traditional messaging apps. Unlike many existing messaging platforms that require users to register using their phone numbers or other identifiable information, the E2EE messaging application aims to provide a more anonymous and secure communication experience. This document outlines the motivation behind creating this application and highlights the problem statement it addresses.

## Problem Statement

Most messaging applications today rely on user registration through phone numbers or other personal information, which can potentially compromise user privacy. This information can be used to track and monitor user behaviour, including chat frequency, message count, and other patterns. Such tracking undermines the privacy and confidentiality of user communications, which is a growing concern in the digital age.

Inspired by the privacy-focused Tor browser, which assigns a new identity and creates an encrypted channel for each visited domain, the E2EE messaging application adopts a similar approach. By creating a new identity for each user interaction and establishing encrypted communication channels, the application aims to protect user anonymity and prevent the identification of user behaviour.

The primary objective of this application is to simplify the messaging experience while ensuring privacy and security. Users can search for other individuals using their unique IDs and initiate conversations without the need to provide personal information or bind their identities to the application. By eliminating the reliance on traditional identification methods, the E2EE messaging application offers users a higher level of privacy and control over their communication.

## Technological

## Future Development

As part of the ongoing development, the E2EE messaging application aims to adopt a decentralized approach for the messaging server infrastructure. By decentralizing the server infrastructure, the application seeks to minimize the risk of information leaks from a single server. This approach enhances the security and privacy aspects of the application by distributing the data across multiple nodes, making it more resilient to attacks and reducing the chances of centralized data breaches.

The decentralized architecture also aligns with the philosophy of maintaining user privacy and control. Users can have greater confidence in the security of their communications, knowing that their messages are not concentrated in a single location.

## Conclusion

The E2EE messaging application provides a privacy-focused and secure communication platform that prioritizes user anonymity and confidentiality. By eliminating the need for personal information and implementing end-to-end encryption, the application offers users a way to communicate freely without compromising their privacy. With future development focused on decentralized server infrastructure, the E2EE messaging application aims to further enhance security and minimize the risk of data breaches.

By embracing this approach, users can enjoy a messaging experience that respects their privacy and gives them control over their personal information.