# Introduction

In a world where digital communication has been more prone to data breaches, unauthorised access, and undesired retention of sensitive information are escalating in a society where digital communication has grown pervasive. Flash Messenger tackles these issues front on by delivering a secure messaging solution that employs cutting-edge encryption techniques, giving you peace of mind that your communications are safe from prying eyes.

Flash Messenger is cutting-edge chat software that puts your privacy and security first. When required, Flash Messenger will ensure that communication is smooth, private, and ephemeral. This method allows you to send and receive encrypted messages that can only be read once before disappearing, guaranteeing that your personal chats stay completely secret.

The platform was created with simplicity and use in mind, allowing anybody to effortlessly compose and send messages with just a few clicks. Furthermore, we recognise that seamless authentication is critical for a hassle-free experience. As a result, we provide secure login through Google, employing their sophisticated authentication infrastructure to provide a smooth and trustworthy sign-in procedure.

# Business Requirements

Flash Messenger may meet your demands whether you are an individual searching for a safe means to transmit sensitive information or a corporation wishing to retain client confidentiality. Our dedication to privacy, data security, and industry best practices distinguishes us as a global leader in private messaging. The aim of this messenger is to rigorously adhere to data protection legislation, and we are committed to preserving your personal information. You can be certain that your chats on the messenger will stay purely between you and your intended recipients because of our commitment to user-centric design and security.

## Functional Requirements

1. Secure Messaging:
   1. The system should allow users to securely transmit and receive encrypted communications.
   2. To maintain secrecy, messages should be encrypted during transmission and storage.
2. View Once Only
   1. • Messages should be constructed such that the receiver may only read them once.
   2. • After the recipient views the message, it should instantly evaporate and become unreachable.
3. User Authentication via Google:
   1. • Users should be able to log in to the system securely using their Google credentials.
   2. • The system should support OAuth or comparable Google authentication protocols.
4. Message Composing and Sending
   1. • Users must be able to create new messages.
   2. • Users should be able manually input their email addresses.
   3. User should be able to see the messages received from other users.

## Non-functional Requirements

1. Security
   1. • The system should utilise strong encryption methods to protect communications and user data.
   2. • It should adhere to best practices in the industry to prevent unauthorised access to messages and user information.
2. Reliability
   1. • The system should be extremely dependable and available, with as little downtime and data loss as possible.
3. User-Friendly Interface
   1. • The user interface should be simple and straightforward to use.
   2. • Users should be able to properly comprehend the message view-once capabilities.
4. Privacy
   1. • The system must follow privacy standards and not keep any superfluous user data.
   2. • It should properly convey to consumers its data usage policy.
5. Compliance
   1. • The system must adhere to applicable data security and privacy laws and regulations.
   2. • It must follow Facebook authentication principles and criteria.

## Security Requirements

1. Data Encryption:
   1. All messages and sensitive data transmitted and stored within the system must be encrypted using strong cryptographic algorithms to ensure confidentiality.
2. Secure Authentication:
   1. The system should implement a secure and robust authentication mechanism for user login, supporting Google OAuth or similar industry-standard protocols.
3. Secure Data Transmission:
   1. Messages should be transmitted over secure channels, such as HTTPS, to prevent eavesdropping and man-in-the-middle attacks.
4. Message Expiry and Deletion:
   1. Implement a mechanism to automatically delete messages after they have been viewed once to ensure that sensitive information is not retained unnecessarily.
5. Session Management:
   1. Ensure that user sessions are properly managed, with secure session handling, and sessions should expire after a reasonable period of inactivity.
6. Secure Third-Party Integrations:
   1. If integrating with third-party services or APIs, ensure that proper security measures are in place to protect against any security risks associated with those integrations.