**Secure Messaging App**

Technical Specification Document

*Student: Nematullah Ibrahimi*

*Course: UI/UX Design*

*Date: September 23, 2025*

# 1. Project Title and Overview

**Project Title:** Secure Messaging App

**Overview:** A privacy-first mobile messaging app that provides end-to-end encryption by default, simplified identity verification, and resilient backup/recovery. The product aims to make secure communication intuitive for non-expert users while offering advanced controls for power users. Key objectives: reduce user errors, increase verification adoption, and improve recovery flows.

# 2. Target Audience

* Primary users: Privacy-conscious individuals, journalists, activists, and small teams that require secure communication.
* Secondary users: General consumers who want privacy, small businesses, and family groups.
* User demographics & behaviors: Ages 18–55, moderate-to-high smartphone usage, value privacy, use messaging daily, multi-device users.
* User needs: Simple onboarding, reliable message delivery, recoverable identity/backups, clear indicators of security status.

# 3. Core Features

1. MVP (must-have):

* • Automatic end-to-end encrypted messaging (text, voice, media).
* • Simplified identity verification (just-in-time prompts + quick compare).
* • Encrypted cloud backup with secure recovery PIN + recovery recommendations.
* • Ephemeral messages and message preview controls.
* • Cross-device sync with easy device linking.

1. Planned (phase 2):

* • Advanced group controls and admin verification.
* • Risk-adaptive prompts and progressive disclosure for sensitive actions.
* • In-app micro-education for verification and backups.

# 4. Design Goals

* Aesthetic goals: Modern, minimal, high-contrast UI; clear iconography; friendly microcopy.
* Functional goals: Mobile-first responsive design, fast common flows, visible feedback for security actions, low cognitive load.
* Accessibility goals: Meet WCAG AA where possible, large touch targets, readable typography, clear error descriptions.

# 5. Challenges and Considerations

* • Verification features are technical — need user-friendly metaphors and just-in-time education.
* • Recovery flows risk account loss — must balance security and recoverability.
* • Cross-platform sync introduces complexity (key management) and UX friction.
* • Accessibility and localization across languages and cultures.
* • Regulatory constraints (e.g., data retention laws) and network limitations in low-bandwidth regions.

# 6. Tools and Resources

* Design tools: Figma (primary), Adobe XD (backup), Miro (workshops), Notion (documentation).
* Development & prototyping: React Native / Flutter for prototypes; InVision or Figma prototypes for usability testing.
* Reference apps & inspiration: Signal, Wire, WhatsApp (UX patterns); Dribbble & Behance (visual inspiration).
* Research sources: Usability studies (Whitten & Tygar 1999), design patterns from Security & Usability collections.

# Optional Enhancements / Visuals

|  |
| --- |
| **Mood board placeholder:** |
| *Diagram placeholder: (User flow - Onboarding → Verification → Backup)* |
| *Icons placeholder: (Security status, backup, verify)* |