

## CPRE 492 STATUS REPORT #7

January 28, 2020 - February 13, 2020

Group: SDMAY20-52

Project Title: KEY EXCHANGE OUTSIDE OF TCP/IP

Client & Advisor: Julie Rursch

Team Members:

- Logan Woolery            Lead Integrations Engineer
- Jacob Moody            Server Developer Lead
- Joel Wacker            Android Developer
- Andre C                Quality Assurance Testing
- Jack Potter            Client Architecture Tester
- Jordan Svoboda        IOS Developer

### Past Week Accomplishments

- ❖ Andre- Client-side development
  - Flutter confirmed to be working on both iOS and Android
  - Assisted with client side implementation
    - Started networking functionality
    - Combined widgets (used for menus) in application
- ❖ Jacob-Continued development of backend code
  - Work on improving error handling
  - expand test coverage
  - start work on deploying of server
- ❖ Jack
  - experimented with open source QR code libraries
  - Experimented with implementation of dart QR code libraries
    - Attacked various issues here for a while
- ❖ Joel
  - Found flutter plugin for requesting hardware permissions
    - On application page load, should request permissions as needed, needs further testing
- ❖ Jordan-Implementation of client-side encryption
  - Implemented code for encryption, decryption and symmetric key generation
    - Used steel\_crypt library
  - Implemented a database for storing other user's names, public keys and the symmetric keys for the user's chat with those other users

- Stored using unique public key as the ID
- Created a file with functions to mitigate SQL injection attacks when performing database queries
- Separated all file access, database and cryptography functions out of the main Flutter file and into their own files for more modular code

❖ Logan

- Research into UI/UX in flutter
- Begin to make it look like a frontend developer at least looked at it

### Pending Issues

- ❖ Implement PGP keys in Flutter
- ❖ GUI design needs to be improved
- ❖ Development of tests for code (both Client and Server)

### Individual Contributions

Team Member	Contribution	Weekly Hours	Total
Jacob Moody	Development	8	19
Joel Wacker	App Development	7	17
Andre C	Flutter Research Client side functions	26	33
Jordan Svoboda	iOS development	20	30
Logan Woolery	Testing	10	18
Jack Potter	Research	10	17

## Plans for Coming Week

- ❖ Andre-
  - Continue development of client-side networking (highest priority)
  - Get server running to test communication between client/server
  - Develop suite tests in Go for server (lowest priority)
- ❖ Jacob-
  - Have server deployed and publicly addressable
  - improve general code quality
  
  - start measuring performance metrics for possible problematic areas
  
- ❖ Jack
  - Finalize QR implementation
  - Investigate alternative channels of communication
    - Audio via 3.5mm jack
    - NFC
- ❖ Joel
  - QR Code rework to allow for version 40 QR codes
  - Server integration
    - Setup test post requests for handling chat via server API
  
- ❖ Jordan- Continue client side encryption implementation
  - Write more thorough tests for the database and cryptography functions
  - Add a column to the database that stores the path to the file containing the messages in the related chat
    - This will allow for easy modification (like addition of new messages) and easy deletion of chats that are no longer needed/readable due to key changes
  - Find a way to implement PGP keys into our application for authenticating with the server and message integrity verification
    - No libraries for this in Flutter, so I need to do some research on this
  
- ❖ Logan
  - Begin UI implementation
  
  - Devise a consistent theming