



OTP Gen

Students: Thinh Nguyen, Florida International University

Instructor/Faculty: Dr. Masoud Sadjadi, Florida International University

PROBLEM

- Sophisticated cyber threats can no longer be prevented with traditional login and password combinations.
- Protecting sensitive data and online accounts is now more important than ever.
- User account protection has been significantly enhanced with 2FA, which gives the authentication procedure an additional layer of security.

REQUIREMENTS

- Users will be able to create 30-second OTPs using the system, after which they will be able to create new ones.
- To speed up the process of entering in the secret key, the system will allow users to scan a QR code for the secret key.
- Users can delete inactive accounts from the system by swiping left and clicking the delete option.
- Users will be able to look up accounts by name using the system.

IMPLEMENTATION

- A popular library for handling routing and navigation in React Native apps is called React Navigation. Its support for many navigator types, such as stack, tab, and drawer navigators.
- By requiring both a password and a one-time code, 2FA adds an extra layer of protection. A React Native package called jsotp is used to create and validate One-Time Passwords, or OTPs.
- Users can utilize the device's camera to scan QR codes with QR Code Scanning. It's simple to create this feature with libraries like react-native-qrcode-scanner and react-native-camera.

SUMMARY

- Through the requirement of a second form of verification in addition to the normal password, Two-Factor Authentication (2FA) improves security. Even in the unlikely circumstance that the password is compromised, the risk of unwanted access is greatly decreased by this additional layer.
- Since 2FA apps are meant to be user-friendly, users may easily and rapidly generate One-Time Passwords (OTPs). In an increasingly digital environment, peace of mind could be achieved by individuals and companies by better protecting sensitive data and accounts from illegal access by implementing 2FA.

REFERENCES

- <https://www.getapp.com/security-software/a/duo-security/reviews/>
- <https://www.trustradius.com/products/google-authenticator/reviews?qs=pros-and-cons#reviews>

CURRENT SYSTEM

- Duo only lets you remember one device at a time
- Google authenticator does not support multiple-device or more platforms



VERIFICATION

- OTP that lasts for 30 seconds, then generate a new one
- Use the scan function to read the secret key from the QR code.
- Press the delete button by swiping left to remove inactive accounts.
- Check up accounts utilizing the system by name

OBJECT DESIGN

