Google 2FA - Security

Here we will use Google Authenticator as the second factor of authentication (2FA)

Google Authenticator is an app that is installed on a smart phone. It generates a specific time-based one time password, that can be used as the code to login.

The advantage with this method is we do not need to build 2FA infrastructure, nor do we need to send SMS tokens to the phone.

In order to configure Google Authenticator,

Use a python HMAC OTP library like: https://github.com/tadeck/onetimepass

1. Establish an application-specific secret to share with Google Authenticator.
2. Hash the username with the secret.
3. Store the Hash in the database against the user.
4. Display the hash as a QR Code and as text
5. Ask user to install Google Authenticator if they don't have it and open the app
6. Ask the user to add an account for the "FRIENDS App" and scan the QR code.
7. at login, using Google Authenticator libraries, ask user to login, and then to provide the authenticator code (TOTP)
8. Validate login normally and compare authenticator code (TOTP) with what was generated on server.
9. If login and TOTP match, allow login.

Sources

https://www.codementor.io/@slavko/google-two-step-authentication-otp-generation-du1082vho

https://medium.com/@richb_/easy-two-factor-authentication-2fa-with-google-authenticator-php-108388a1ea23

https://hackernoon.com/how-to-implement-google-authenticator-two-factor-auth-in-javascript-091wy3vh3