**Two-Factor Authentication Methods**

1. **Time-Based One-Time Passwords (TOTP) with Google Authenticator**
   1. Every user who signs in to our application will receive a unique key that’s stored in our database.
   2. The user must scan the QR within the Google Authenticator app.
   3. The app will generate a 6-digit code every 30 seconds.
   4. At the login screen, users must enter the code provided + their password and the python code we implemented must verify it.

Sample code: (provided within the GitHub folder)

(This method provides strong security, no reliance on SMS/email delivery, & works offline)

1. **One-Time Passwords (OTP) via Email or SMS**
   1. The user logs in to our application 🡪 The password is correct 🡪 Our app sends a random 6-digit code to the user’s email or phone number 🡪 This code must be entered in our application to complete the verification.

Sample code: (provided within the GitHub folder)

(This method is simple and easier for our users because an extra application is not needed)

1. **Push-Based Authentication via Mobile App**
   1. This method does not include typing in a code.
   2. The user will receive a push notification from a mobile app (DUO).
   3. Two prompt messages appear; you can either approve or deny the login attempt.
   4. Our backend waits for a confirmation request from the mobile app.

Sample code: (provided within the GitHub folder)

(This method is more complex than the other two and involves extra steps for our users)