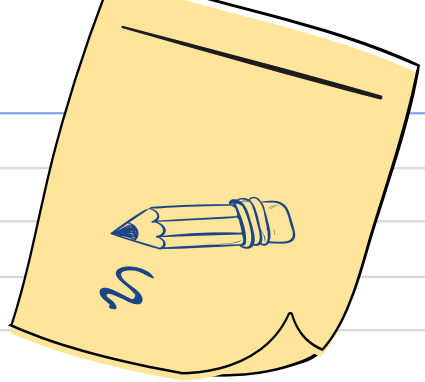
Two-Factor Authentication using TOTP

GVHD: Nguyễn Ngọc Tự

Bùi Hoàng Trúc Anh - 21521817
Nguyễn Ngọc Trà My - 21520353
Lê Hoàng Oanh – 21521253

Ngữ cảnh ứng dụng



Để tăng tính bảo mật trong các ứng dụng chuyển tiền online, server sẽ yêu cầu người dùng nhập lại mật khẩu và tạo thêm mã TOTP để xác thực người dùng.

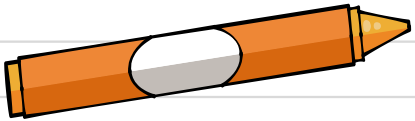
Tài sản cần bảo vệ

Tài khoản trực tuyến của người dùng

Những bên liên quan

Server

Các dịch vụ này yêu cầu người dùng sử dụng TOTP để bảo vệ tài khoản của họ.



User

Là người sử dụng TOTP để bảo vệ tài khoản trực tuyến của mình

Mục tiêu bảo mật

$a^2+b^2=c^2$

Đảm bảo tính xác thực

đảm bảo rằng mã xác thực được tạo ra chỉ có thể được sử dụng một lần và chỉ có thể được tạo ra bởi người dùng cụ thể đã được cấp quyền truy cập

Đảm bảo tính bảo mật:

đảm bảo rằng mã xác thực được tạo ra không thể bị đoán trước hoặc giả mạo bởi các kẻ xấu.

Kịch bản triển khai!

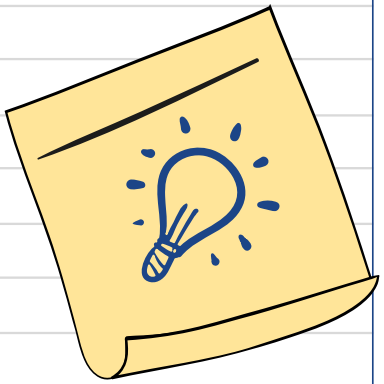
Xây dựng 1 local server và 1 ứng dúng cho client trên window. Khi client nhập mật khẩu để xác thực yêu cầu chuyển tiền, ứng dụng sẽ tự động sinh ra một mã OTP. Sau đó ứng dụng sẽ gửi mã OTP này cùng với mật khẩu đến server để xác thực client. Client xác thực server bằng certificate tự ký của server.

Tài liệu tham khảo

- Balasta, D. U., Pelito, S. M. C., Blanco, M. C. R., Alipio, A. J., Mata, K. E., & Cortez, D. M. A. Enhancement of Time-Based One-Time Password for 2-Factor Authentication.

- Seta, H., Wati, T., & Kusuma, I. C. (2019, October). Implement time based one time password and secure hash algorithm 1 for security of website login authentication. In 2019 International Conference on Informatics, Multimedia, Cyber and Information System (ICIMCIS) (pp. 115-120). IEEE

- Dobreva, J., Lumburovska, L., Trpcheska, H. M., & Dimitrova, V. (2021). A Comparative Analysis of HOTP and TOTP Authentication Algorithms. Which one to choose?. Security & Future



Phân công

Nguyễn Ngọc Trà My	thuyết trình, tìm hiểu thuật toán, demo
Lê Hoàng Oanh	ghi báo cáo đồ án, tìm hiểu thuật toán
Bùi Hoàng Trúc Anh	ghi báo cáo đồ án, tìm hiểu thuật toán, demo

End.