



XÁC THỰC 2 YẾU TỐ VỚI GOOGLE AUTHENTICATOR

TRÌNH BÀY: TRẦN PHƯỚC LỘC



XÁC THỰC 2 YẾU TỐ LÀ GÌ?

Nôm na thì xác thực 2 yếu tố là thêm một bước xác thực thay vì chỉ cần tài khoản và mật khẩu. Ví dụ khi người dùng bật tính năng này, lần tiếp theo khi đăng nhập thành công tài khoản và mật khẩu, người dùng sẽ phải tiếp tục xác thực thêm một bước nữa(email,otp,...) để có thể thực hiện những chức năng khác (ví dụ:vào trang dashboard).



TẠI SAO CẦN XÁC THỰC 2 YẾU TỐ?

- Tăng bảo mật với những thông tin quan trọng
- Thông báo cho người dùng để đảm bảo người dùng chắc chắn với những quyết định của mình
- giảm thiểu rủi ro nếu người dùng bị rò rỉ tài khoản và mật khẩu



GIỚI THIỆU ỨNG DỤNG GOOGLE AUTHENTICATOR

Google Authenticator là phần mềm tạo mã code được sử dụng để đăng nhập vào trong tài khoản gồm có 6 số ngẫu nhiên. Theo đó 6 số này chỉ có thời hạn sử dụng trong vòng 30 giây.

Nếu như hết thời gian này thì ứng dụng sẽ tạo tự động với 6 số ngẫu nhiên mới khác. Đồng thời sẽ thực hiện liên tục như vậy cho đến khi bạn điền thành công.



TẠI SAO LẠI CHỌN GOOGLE AUTHENTICATOR ĐỂ TRIỂN KHAI?

- Miễn phí
- Tăng tốc độ xác thực (email, otp cần thời gian để gửi mail, mã otp đến hộp thư , điện thoại)
- Tăng độ bảo mật
- Tương thích với nhiều thiết bị
- dùng được ngay cả khi điện thoại không kết nối internet

Bên cạnh những ưu điểm, vẫn còn đó những mặt hạn chế:

- không hoạt động được nếu điện thoại hết pin
- Ứng dụng không hỗ trợ recovery hay backup lại QR code
- Cần nhiều bước setup ở phía người dùng

TỔNG KẾT: Mặc dù vẫn còn những hạn chế, nhưng so với những lợi ích mà ứng dụng mang lại thì vẫn rất đáng để triển khai



GOOGLE AUTHENTICATOR HOẠT ĐỘNG NHƯ THẾ NÀO?

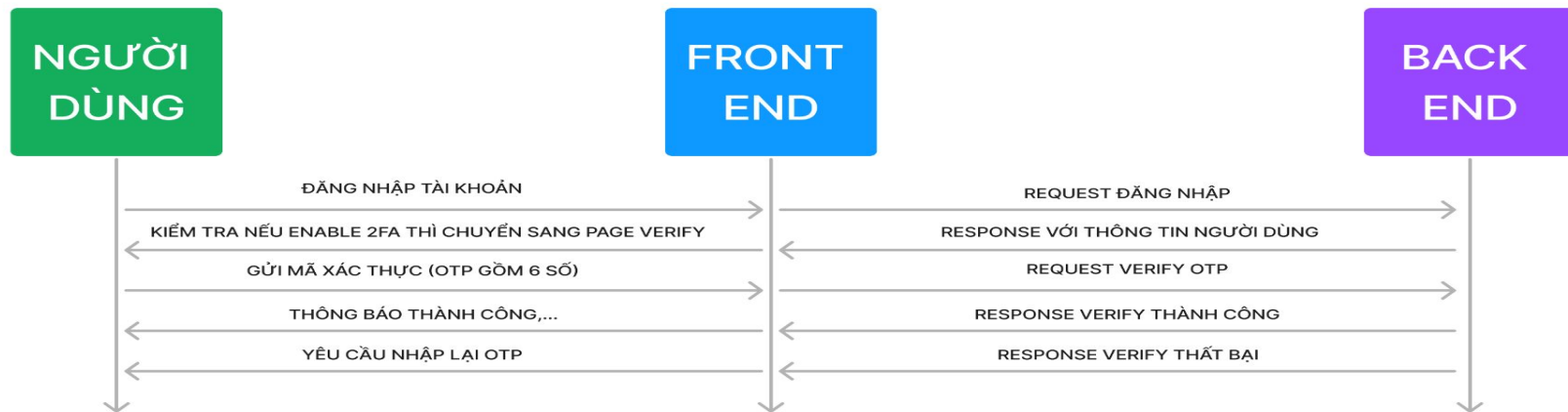
Google Authenticator App sử dụng thuật toán TOTP (Time-based One-Time Passwords).

- Nhà cung cấp ứng dụng sẽ tạo một secret key chia sẻ giữa dịch vụ và ứng dụng Google Authenticator.
- Google Authenticator sẽ dựa trên secret key và thời gian hiện tại để tạo ra mã OTP và hiển thị lên điện thoại người dùng (thường là 30 giây sẽ tạo một mã mới)
- Khi xác minh danh tính, người dùng nhập mã OTP trên ứng dụng Google Authenticator vào page xác thực trên dịch vụ
- Dịch vụ sẽ xác thực sẽ tính toán ra mã OTP dựa vào thuật toán TOTP và kiểm tra xem có khớp với mã người dùng vừa nhập hay không, nếu khớp thì xác thực thành công và ngược lại.

FLOW HOẠT ĐỘNG CỦA XÁC THỰC 2 LỚP KẾT HỢP GOOGLE AUTHENTICATOR



FLOW HOẠT ĐỘNG CỦA XÁC THỰC 2 LỚP KẾT HỢP GOOGLE AUTHENTICATOR





CÁC BƯỚC TRIỂN KHAI XÁC THỰC 2 LỚP

TẠO MỚI QR CODE

- Tạo secret key: có thể dùng id hoặc email hoặc sdt của người dùng để tạo, nhưng tốt nhất nên encode sang Base32 để unique nhất có thể, Url sau khi tạo đầy đủ:

```
String otpAuthUri = "otpauth://totp/" + identify + "?secret=" + secret + "&issuer=" + issuer +  
    "&algorithm=SHA1&digits=6&period=30";
```

- Dùng thư viện để generate QR Code từ Url
- Demo code



CÁC BƯỚC TRIỂN KHAI XÁC THỰC 2 LỚP

VERIFY OTP

- Dùng thư viện để verify
- Demo code



TRẢ LỜI CÂU HỎI