**Đặt vấn đề**

Để đảm bảo việc dữ liệu của người dùng chỉ có thể được truy cập, giải mã bởi chính người đó hoặc có thể cấp quyền cho người khác truy cập thì em đề xuất giải pháp mã hoá đầu cuối End-to-End Encryption (E2EE)

Về cơ bản hiện tại thì có 2 loại mã hoá chính:

* Mã hoá đối xứng → dùng 1 key duy nhất để mã hoá và giải mã
* Mã hoá bất đối xứng → dùng 1 cặp key(public/private key) để mã hoá và giải mã

**Mô tả giải pháp**

Để giải quyết bài toán trên ta kết hợp hai loại mã hoá trên như sau:

Mỗi khi người dùng tạo tài khoản sẽ gen cho người dùng các key sau (thao tác gen ở dưới thiết bị người dùng):

* 1 secret\_key ( vd: aaa-vvv-333-sddd–ssss được lưu trên thiết bị của người dùng và backup vào cloud, key chain …vvv
* 1 cặp public\_key, private\_key

Chức năng của các key:

* secret\_key sẽ là key gốc của người dùng, không chia sẻ cho bất kì ai kể cả máy chủ, dùng để mã hoá private\_key.
* public\_key, private key sẽ dùng để mã hoá và giải mã dữ liệu bảo mật cụ thể ở đây là data gen của người dùng

Luồng thực hiện:

Lưu trữ các key:

* Sau khi tạo được các key thì ta sẽ lấy secret\_key để mã hoá private\_key theo mã hoá đổi xứng ta được encrypt\_private\_key
* Lưu trữ thông tin {public\_key, encrypt\_private\_key} ứng với userId của người dùng lên máy chủ

Upload data gen:

- Đăng nhập vào ứng dụng —> get thông tin public\_key tương ứng với userId—> dùng public\_key mã hoá dữ liệu gen—> upload data gen lên máy chủ

Lấy data gen và giả mãi

* Đăng nhập vào ứng dụng —> get data gen đã được mã hoá và encry\_private\_key từ máy chủ
* Dùng secret\_key được lưu ở máy để giảm mã encrypt\_private\_key —> thu đươc private\_key
* Dùng private\_key giả mã data gen được mã hoá → thu được data gen

Chia sẻ thông tin data gen giữa các người dùng được cấp quyền

Gọi A là người cấp quyền, B là người được uỷ quyền truy cập vào data gen của A

* Máy chủ gửi thông tin public\_key của B cho A
* A dùng public\_key của B đã mã hoá dữ liệu gen của A ( được giải mã như cách đã trình bày ở trên)
* B lấy private\_key của mình ( đã trình bày bước lấy private\_key ở trên) để giải mã data gen đã được mã hoá của A →> thu được data gen của A

Tham khảo code ở folde genKeyAndEncryptData