- Create Key:

+ Nhập App Name

+ Nhập KEK1

+ Nhập KEK2

+ Nhập DEK1

+ Nhập DEK2

=> Trả về:

+ KEK1:

+ Version:

+ App Name:

+ File DEK Descrypt cấu trúc appName/version/tenfile.key

Ví dụ:

+ KEK1: AAAAAA

+ Version: 1

+ AppName: 123pay

+ 123pay/version/a3552gb456sdg3563dgg.key

App add config các thông tin sau:

+ App Name

+ Version

+ KEK1

+ File DEK Descrypt cấu trúc appName/version/tenfile.key

- Encrypt Data:

+ Start App: nhập KEK2

+ Lấy KEK1, version từ config

+ Lấy file DEK Description theo đường dẫn appName/version/tenfile.key

+ DEK = Decrypt AES 256 (DEK Decrypt,KEK1 + KEK2)

+ Encrypt Data theo DEK

+ Lưu vào DB 2 field Data Encrypt và version Encrypt

Ví dụ:

+ KEK2: BBBBBB

+ KEK1: AAAAAA

+ Version: 1

+ File DEK Decrypt: 123pay/1/a3552gb456sdg3563dgg.key

- Decrypt Data:

+ Start App: nhập KEK2

+ Lấy KEK1 từ config

+ Lấy data cần decrypt, version từ DB.

+ Lấy file DEK decrypt 123pay/1/a3552gb456sdg3563dgg.key

+ DEK = Decrypt AES 256 (DEK Decrypt,KEK1 + KEK2)

+ Decrypt Data với DEK

Ví dụ:

+ KEK2: BBBBBB

+ KEK1: AAAAAA

+ Lấy data encrypt “cccccc” với version là 1

+ File DEK Decrypt: 123pay/1/a3552gb456sdg3563dgg.key

+ DEK = Decrypt AES 256 (DEK Decrypt,KEK1 + KEK2)

+ Decrypt Data với DEK

- Change key:

+ Nhập AppName

+ Nhập KEK1

+ Nhập KEK2

+ Nhập DEK1 mới

+ Nhập DEK2 mới

=> Trả về:

+ Version mới

+ Tạo file DEK Encrypt theo KEK và lưu vào thư mục version mới.

=> Update config App lại version mới, để các data mới về sau Encrypt theo DEK mới. Data cũ sẽ decrypt theo DEK cũ. Sau đó chạy ứng dụng change Data để chuyển đổi dữ liệu cũ sang DEK mới.

- App Change Data:

+ Nhập KEK1.

+ Nhập KEK2.

+ Nhập version mới

+ Hệ thống lấy data encrypt, version từ database.

+ Lấy DEK cũ theo version trong DB để decrypt data.

+ Encrypt Data lại theo DEK mới và update vào database mới Data mới + Version mới.

- Cron chạy kiểm tra các app tồn tại 2 version quá 30 ngày thì xóa thư mục DEK Decrypt version cũ. Có thẻ Alert cho mọi người qua email hay SMS.