

Document exchange

Salem Almotiry

Qassim University

Abstract

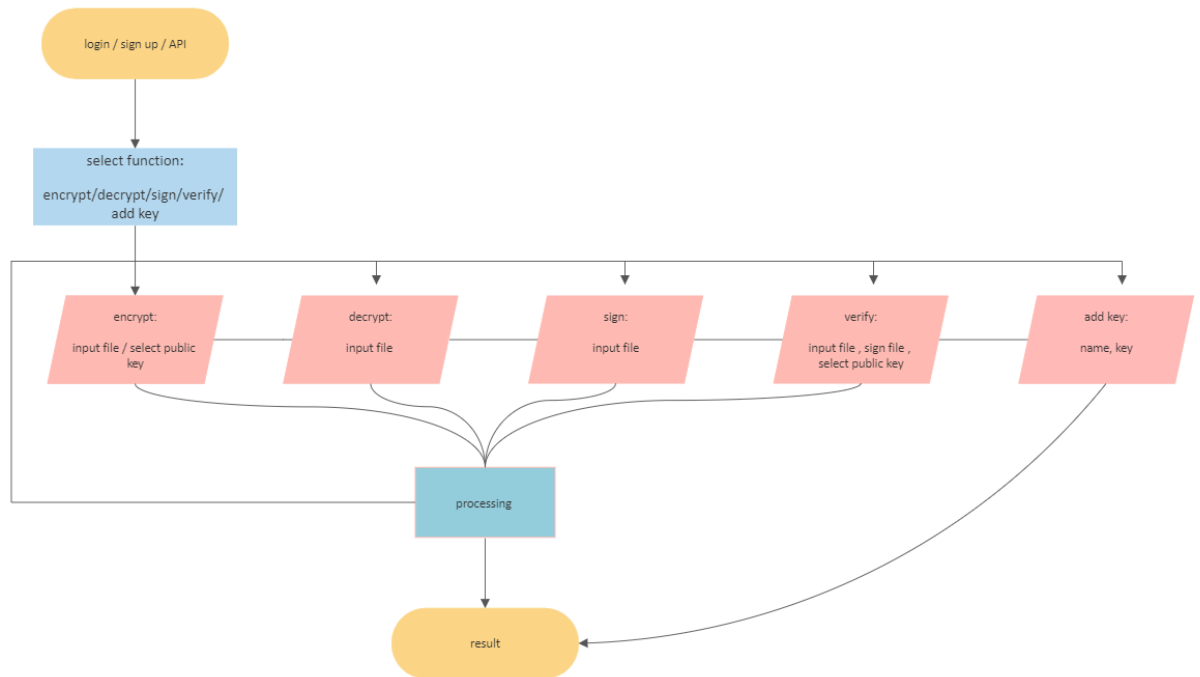
Teams and startups have difficulty building a security system to exchange documents internally.

This API is designed to make it possible to build a flexible document exchange system. This project is divided into two sections.

1. website for individual uses content main RSA function
2. API offers all RSA functions with high customizability

To encrypt, decrypt and other function to exchange documents are easier and modifiable

Document exchange



Input and Output

Explaining input and output RSA function

rsa_encrypt_file(file_path,save_path,pub_key)

RSA encrypt function takes three parameters original file that going to encrypt, a path to save the encrypted file, and the public key. Output expected is an encrypted file

rsa_decrypt_file(file_path,save_path,priv_key)

RSA decrypt function takes three parameters encrypt file that going to decrypt, a path to save the decrypted file, and the private key. Output expected is an encrypted file

sign(file_path,save_path, privkey)

RSA sign function takes three parameters file that going to sign, a path to save the signed file, and the private key. Output expected is an encrypted file

verify(file_path, signature_path, pubkey)

RSA verify function takes three parameters original file, a signed file, and the public key.

Output expected is a true or false