+91 80 6740 1400
eservices@emudhra.com
emudhra.com/about/company.html

eMudhra Limited
Sai Arcade, 3rd Floor,
No.56, Outer Ring Road,
Devarabeesanahalli,
Bangalore - 560103

emSafe – Secure encryption/ decryption engine

Encrypt and Decrypt all the sensitive information and documents using Asymmetric keys.

As the world is progressing towards Digitalization, Securing data is imperative for organizations to protect corporate secrets, to secure classified information, and predominantly to protect personal information to guard against identity theft and cyber-threats as well as illegal or unauthorized access.

There are two methods of encryption: symmetric and asymmetric encryption. Symmetric encryption, also known as secret key encryption, pertains to the sender and the recipient holding the same keys to encrypt and decrypt a message. A**symmetric encryption**, or **Public Key Encryption** uses a key pair—a **public key** for encrypting a message, and a **private key** to decrypt it.

emSafe ensures confidentiality of data by encryption and decryption of files or data. The solution uses symmetric key stored in the USB crypto token/HSM to ensure the end-to-end data security by encrypting and decrypting of data. emSafe is a highly scalable application which can be hosted across bank data center.

emSafe uses **Asymmetric keys based encryption/decryption** where in a key can be used to encrypt as well as to decrypt a message. Most importantly, a message that is encrypted with a private key can only be decrypted with a corresponding public key. Similarly, a message that is encrypted with a public key can only be decrypted with the corresponding private key.

---

emSafe – Encryption/Decryption
emSafe ensures confidentiality of data by encryption and decryption of files or data. The solution uses key stored in the USB crypto token/HSM to ensure the end-to-end data security by encrypting and decrypting of data.

emSafe is a highly scalable application which can be hosted across bank data center.

Symmetric Encryption
In Symmetric encryption a single key shall be used to encrypt as well as to decrypt a message. Encryption algorithms such as Data Encryption standard (DES), 3DES and AES 256 shall be used for encryption.

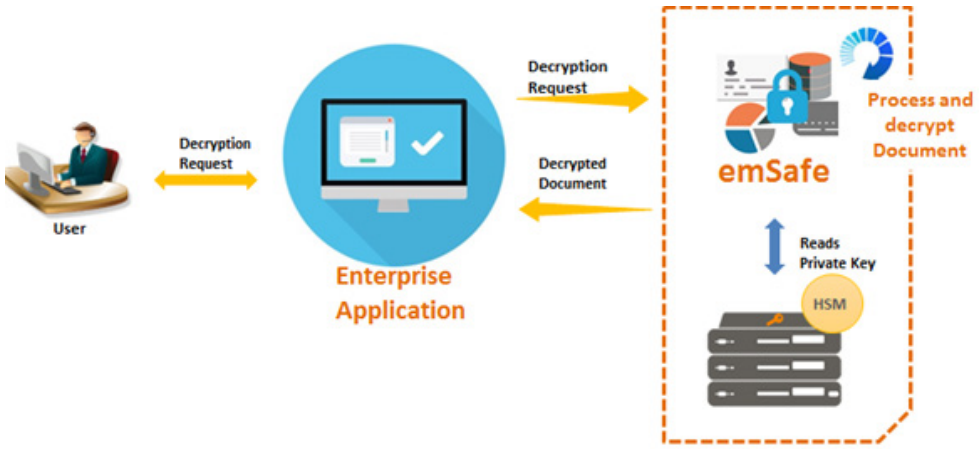
Asymmetric Encryption

In Asymmetric encryption technique a message that is encrypted with a private key can only be decrypted with a corresponding public key. Similarly, a message that is encrypted with a public key can only be decrypted with the corresponding private key.

Storage Encryption

- User A request for encrypting of data/document, and selects the User B Public key for encrypting document using emSafe application.
- emSafe application on the other hand employees public key to encrypt data using secured Algorithms.
- Encrypted document will be secured and cannot be decrypted using any other Key other than User B's private key.

Decryption



- User B requests for decryption of document, which is encrypted by User A using User B public key.
- emSafe application reads the Private key from the HSM and performs the decryption of the document.
- Decrypted document will now be accessible to user B to view.

emSafe Node to Node Encryption

Node to Node encryption follows the complete encryption of the document from originator node to receiver node without any threat for middle man attack, complete encryption process shall work in the same order using Public key for encryption and private for decryption of the data.

Public Key algorithm	RSA
Symmetric Key algorithm	AES
RSA Public Key Technology	RSA Encryption Standard (1024, 2048 bit) PKCS#12 Portable format for a user's private keys

Use case