# Enigmator

PKI Based Email Encryption Solution

TrustSafe Enigmator enables users to send secure e-mail by signing and sending to the recipients in an encrypted e-mail. It ensures confidentiality and integrity of email content, including file attachment, for compliance of Cryptographic and Electronic Messaging Protection Controls.

Key Features

- Sign and/or encrypt email using recipient's digital certificate stored in smart card or hardware token

- Support cryptographic algorithm including AES-256

- Support X.509 certificates and its extension certificate

- Support multiple certificates for digital signing & encryption

- Decrypt mail by auto-detect the multiple certificates stored in the hardware token

- Password time-out setting

- Enforce key-in password when read and send secured mail

- Provide S/MIME Standard

- Provide Mail Conversion Tool

- Seamlessly integrate with both HCL Notes and Microsoft Outlook

Key Components

1. Configuration Database – Manage the root CA, CRL, Patching and Directory connection.
2. Log Module – Log down the error during sending signed and encrypted email.
3. Core Module – Core engine for TrustSafe Enigmator product family
4. For supporting HCL Notes: Provide Notes Mail Template – integrated with TrustSafe Enigmator modules on the standardized HCL Notes mail template.
5. For supporting Microsoft Outlook: Provide Outlook add-on to send and open signed and encrypted email.

System Diagram
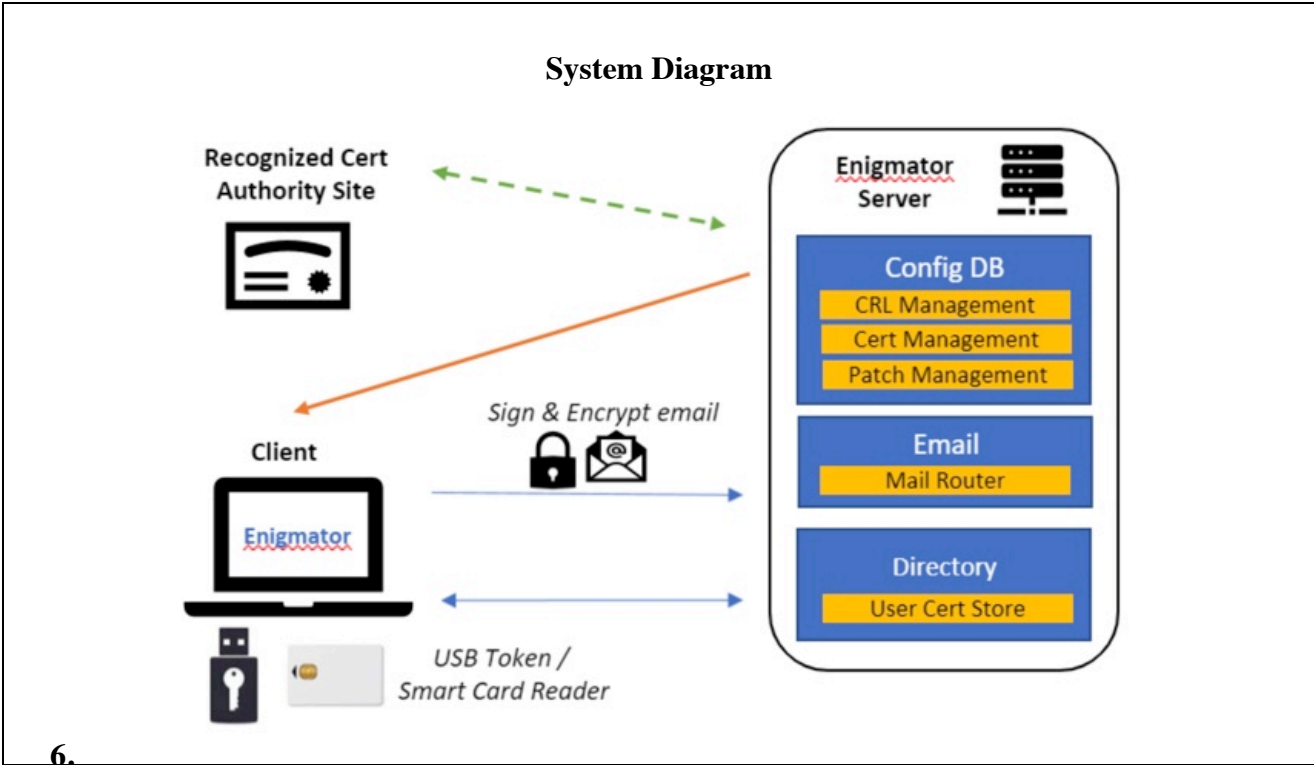
6.

Auxiliary Options	
Key and Cert management Tools to enhance security and administration efficiency	
Central Secure Key Repository	A secure central repository to hold original electronic certificate file & its password
Audit Trial	360-degree monitor email security activities, including Mail, Database, Directory, User login activities & ACL.
Token management	Remotely release a locked Enigmator token. System generates unique random unlock password for different tokens.
Remote Import Cert	Support administrator remotely to transfer new certificate to user at distant workstation when users need to import renew e-cert to their token authenticator

Technical Specification

Encryption Technology Standard	
Digital Signature Algorithms: Encryption Algorithms: Hashing Algorithms: Certificates supported:	RSA 3-DES, AES-128, AES-256 SHA-1, SHA-2 X.509v3 certificate-based (e.g. HK Post e-Cert & Digit-Sign), CRLv2
System Requirements	
Support Smart card / Token	o Utimaco Safeware Smartcards via CardMan o Enigmator Smartcard o Software (P12 file format) o USB Token (SafeNet eToken) o Enigmator Token
Operation System	o Chinese / English Windows 7 (32 / 64 bit) o Chinese / English Windows 8 o Chinese / English Windows 10

 TrustSafe®

Serving organisations from different sectors and regions, TrustSafe offer messaging and collaboration enhancement solutions that go beyond corporate communication enablement. We help clients address their security and compliance concerns without sacrificing work efficiency.

A veteran security solution provider, we started off by developing PKI-based confidential mail system seamless integrated with Domino. The system has then been adopted by a wide spectrum of companies that put data security and confidentiality at the forefront.

www.trustsafe.uk
info@trustsafe.uk
Tel: +44 7895555524