

Based on the ongoing Cryptographic projects, Secure Technology Lab, IDRBT has developed its indigenous product **EnDeSign™** that provides Information Security on your desktop.

Salient features of **EnDeSign™**

- ◆ **Easy to use**
The Graphic User Interface allows the user to achieve the functionalities desired at the click of a mouse. The user manual, describes these procedures in detail. In addition, an online help also forms part of the application.
- ◆ **Encryption**
File Encryption / Folder Encryption using AES algorithm with 128-bit key length.
- ◆ **Decryption**
File Decryption/ Folder Decryption.
- ◆ **Keys**
Key Encryption/ Key Decryption using RSA algorithm (512/1024/2048 bit key length).
- ◆ **Digital Signature**
Signing and Verification using X.509 v3 Certificates.
- ◆ **Smart Card Integration**
Integration of digital signing through Smart Cards (on demand)
- ◆ **CRL Verification**
Validation of revoked certificates in CRL during key encryption and verification.

Write to us at the following address for a 30-day evaluation version of the software. You can download the same from "Downloads" link of the website on INFINET <http://www.infinet.org.in/>. In special cases, APIs can be provided to integrate with existing applications.

For details contact:

The Director,
Institute for Development and Research in Banking Technology
Castle Hills, Road#1, Masab Tank, Hyderabad - 500 057. India.

Ph: +91-40-3534981/82/83/84

Fax: +91-40-3535157

Visit us at: <http://www.idrbt.com/>
<http://www.idrbt.ac.in/>

©2001, IDRBT, All rights reserved.

EnDeSign™



ENcrption
DEcrption
SIGNature
Software



SPEARHEADING TECHNOLOGY ABSORPTION IN BANKING

EnDeSign™ : SECURITY ON YOUR DESKTOP

Internet has revolutionized the ways in which organisations do business. The Internet Protocol (IP) is undeniably efficient, inexpensive and flexible. However, the existing methods used to route IP packets leave them vulnerable to a range of security risks such as spoofing, sniffing and session hijacking and provide no form of non-repudiation for contractual or monetary transactions. Therefore, companies have demanded a more secure system to conduct business and have more internal control over security. Besides securing the internal environment, organizations need to secure communications between remote offices, business partners and customers.

EnDeSign™ provides complete encryption of file and folders along with digital signatures. It brings along a host of features, including:

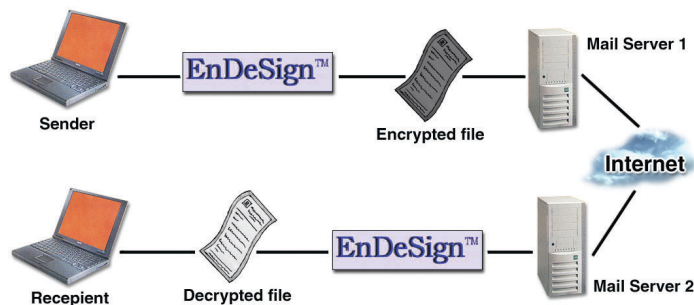
Privacy: Keeps the message confidential and prevents eavesdropping.

Authentication: Digital signatures are used as proof of identity.

Non-Repudiation: Files are digitally signed, thereby providing proof of origin.

Integrity: As files are hashed and signed, integrity is assured.

EnDeSign™ does not restrict use of any specific mail client/server. The flow is depicted in the figure below. Further, it is available on a variety of platforms like Windows-NT/2000, Windows-9x, Linux and Solaris-Intel®



EnDeSign™ is powered with Advanced Encryption Standard (AES) Algorithm (Rijndael) of 128-bit key length (minimum). Symmetric Key Encryption and Signature are carried out using RSA algorithm. AES algorithm has been chosen for EnDeSign because:

- RC2, RC4 and IDEA are all subject to intellectual property claims.
- 3DES is much less efficient than more modern ciphers.
- The AES is efficient and has withstood extensive cryptanalytic efforts.

➤ Encryption/Decryption

Encryption is the process of transforming plain text data into an unintelligible form (cipher text) in such a way that the original data cannot be recovered without using an inverse decryption process with secret key.

Encryption comes in two flavours:

◆ Symmetric or Secret Key Encryption

Symmetric Encryption uses the same key to encrypt / decrypt and the execution is faster.

◆ Asymmetric, or Public Key Encryption

Asymmetric Encryption uses two keys. While one key is public and may be freely distributed, the other key is private and should be kept a secret. Data encrypted with either key can be decrypted using the other key.

➤ Signature/Verification

A signature is a message digest (hash value) that is encrypted with the signer's private key. It provides three security features - Authentication, Non-repudiation and Integrity. Only the signer's public key can decrypt the signature, because it provides authentication and non-repudiation. If the message digest of the message matches the decrypted message digest of the signature, then integrity is assured.

➤ Key Encryption/Decryption

The symmetric key generated during the encryption process is again encrypted with the recipient's public key for ensuring it's secured transmission. It's then decrypted at the recipient's end with his private key, which in turn provides the original symmetric key required for the decryption of the encrypted file.

ENryption
DEryption
SIGNature

It's
great

