Gentran Integration Suite

Encryption Method

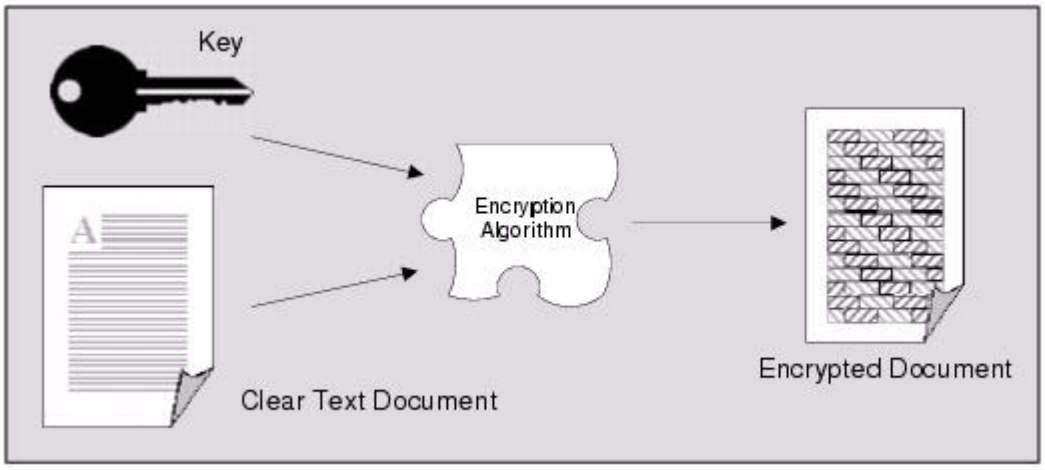
Version 4.2

Gentran Integration Suite Encryption Method

Gentran Integration Suite uses a combination of public/private key encryption, which is also known as symmetric encryption, and asymmetric key encryption. The advantage of symmetric key encryption is that it performs the encryption task more quickly than asymmetric encryption. The advantage of asymmetric encryption is that it allows you to send an encrypted document to a trading partner who does not hold your private key. This Gentran Integration Suite hybrid method uses the best characteristics of each type of encryption and follows the widely adopted S/MIME standard for securing documents.

To use the best of both, Gentran Integration Suite uses the faster symmetric key to encrypt the document, such as a lengthy EDI transaction set, and the asymmetric key for the smaller task of encrypting the one-time session key. The session key can then be securely included with the document for exchange and allows your trading partner to decrypt the contents without sharing your secret key.

The following figure shows an encrypted document using a key acknowledgment that secures integrity during exchange:



Benefits of Encryption

Encrypting and digitally signing documents by using certificates provides you with the following assurances about each document exchange:

- Unauthorized people cannot access and read documents.
- Document integrity remains intact. That is, data cannot be changed, added, or deleted without your authorization.
- Only authorized trading partners can send you documents. Likewise, you can send documents to only those trading partners who authorized you to send documents to them.
- Trading partners who send documents cannot contend they did not send them (referred to as non-repudiation of origin).
- Trading partners to whom you send documents cannot contend they did not receive them (referred to as non-repudiation of receipt).

Encrypting Document Data

Gentran Integration Suite offers the option to automatically encrypt and store data securely in the file system and automatically decrypt them when the files are accessed for transfer or translation.

Gentran Integration Suite supports the use of a customer override property file to override property settings in the property files. The customer override property file is not changed during installation of Gentran Integration Suite upgrades or patches. To prevent having your customized settings overwritten, you should use the customer override property file whenever possible rather than editing the Gentran Integration Suite property files directly.

To enable the Encrypt Document Data service:

1. In the ***install_dir***/properties directory, locate (or create, if necessary) the **customer_overrides.properties** file.
2. Open the **customer_overrides.properties** file in a text editor.
3. Specify the following configurations:

```
Encrypt Data on Disk Enabled
#Document encryption/decryption settings
ENC_DECR_DOCS=ENC_FS
#ENC_DECR_DOCS=NONE
ENC_ALG=DES


Encrypt Data on Disk Disabled
#Document encryption/decryption settings
ENC_DECR_DOCS=ENC_FS
#ENC_DECR_DOCS=NONE
ENC_ALG=DES
```

4. Save and close the **customer_overrides.properties** file.
5. Create a system certificate to encrypt the keys used for the file encryption.