Nordea

Fact Sheet PGP

PGP ensures secure delivery of files and provides encryption and signing.

About PGP

The PGP system provides two features, signing and encryption.

Signing

Signing is used for prevent file tampering and verify the sender.

When signing the message the sender uses its private key, and the recipient uses the sender’s Public key.

Encryption

Encryption is a way to hide what is in a Message and make sure of the privacy

When encrypting a Message the sender uses the recipient’s public key and the recipient uses its private key to decrypt.

What is needed

The Customer (Trading partner) must have OpenPGP compatible software like GnuPG.

Nordea uses the OpenPGP standard which is developed by the OpenPGP Working Group in the IETF. The current specification is RFC 4880.

Encryption procedure

- The Customer encrypts their payload with the public Nordea key.
- The Customer signs their payload with their own secret key
- The Customer sends the signed and encrypted payload to Nordeas

Hash-Algorithms

Supported: MD2, MD5, RIPE-MD/160, SHA-1, SHA-224, SHA-256, SHA-384, SHA-512

Symmetric Encryption Algorithms

Recommended: TRIPLEDES (3DES)
Supported: TRIPLEDES (3DES), BLOWFISH,
CAST5

Output file

Only ASCII-Armor

Nordea Services supporting PGP

Corporate eGateway

More information

www.openpgp.org