Signature/Encryption

Digital mail signature/encryption

To ensure the confidentiality of communications, GNS Gesellschaft für Nuklear-Service mbH offers the option of transmitting encrypted e-mails.

Procedure with key:

The procedures S/MIME and PGP are supported. Please use our public keys when communicating with your contact person.

Please send your public key to mailgateway@gns.de

Procedure without key:

GNS sends e-mails via a webmailer. This system allows you to reply to confidentially sent e-mails in encrypted form.

Please note that despite the use of these procedures, no legally binding declarations can be made in this way!

Further information:

For encryption with S/MIME you need a certificate, which you can obtain free of charge from some trust centers.

For PGP encryption, you must first install GnuPG or PGP on your computer. Further information can be found at the German Federal Office for Information Security.

GNS sends signed e-mails. This means that the recipient already has the certificate of the GNS e-mail contact as soon as he receives an e-mail from the GNS.
The certificates are also provided on the following page, where the certificates can be downloaded: https://www.globaltrustpoint.com/