ENCRYPTION.

The key to secure email communication.

Effective email encryption is the prerequisite for data protection

There is an increasing awareness for the importance of email encryption, as evidenced by numerous studies. In addition, the General Data Protection Regulation (GDPR) demands that specific protective measures aimed at giving individuals control over their personal data are taken by organisations. Among these measures is an obligation to encrypt transmitted data.

Quick and easy confidentiality

Centralised signing of emails and email encryption at the NoSpamProxy® Encryption gateway create secure communication between you and your business partners. Since keys and certificates are managed on the gateway and not on the client machines, the cumbersome handling of electronic keys is no longer necessary. In addition, your private keys are optimally protected against attacks, and corporate governance policies are automatically implemented centrally. Of course, received messages are also decrypted at the gateway and available to users for further processing. This enables access via TLS-encrypted connections with smartphones and tablets, as well as the archiving of unencrypted emails.

S/MIME Signature and Encryption

S/MIME is the preferred and internationally recognised standard for electronic signatures and email encryption. It is a standard for asymmetric encryption based on the use of public and private cryptographic keys. In order to use S/MIME, the sender and recipient must be in possession of a certificate. NoSpamProxy® offers full support for the latest encryption methods published in the standard. Legacy methods are also supported to ensure compatibility.

PGP Encryption

NoSpamProxy® Encyption can also be used to generate, import and manage PGP keys based on the OpenPGP standard for signing, encrypting, and decrypting data. With the support of PGP encryption, NoSpamProxy® Encryption offers an additional option for the convenient exchange of encrypted data and messages.

PDF Mail: Secure email communication without certificates or cryptographic keys

In many cases, recipients do not have a PGP key or personal certificate. NoSpamProxy® Encryption's PDF Mail feature provides another simple way to securely send emails and documents without requiring keys or signatures. NoSpamProxy® Encryption automatically converts the email and all attachments into a password-protected PDF document. The password is automatically sent to the recipient via text message. Alternatively, the recipient can set his or her own password by logging in to the NoSpamProxy® Web Portal. To open the document, only a PDF reader is needed.

Email encryption and certificates

The secure encryption of emails requires S/MIME-based certificates that are compliant with the X.509 standard or certificates that can be used with a PGP key. NoSpamProxy® Encryption centralises and automates the management and acquisition of these certificates. IT administrators benefit from a variety of helpful management features.

Additional NoSpamProxy® Encryption features include:

- DOI (for communication between authorities involved in DOI)
- De-Mail (for communication between users of the De-Mail infrastructure)

SecurITy made in Germany

Open Keys: Free cryptographic key lookup

Our free Open Keys service enables you to quickly and easily check whether your communication partners use certificates and to immediately communicate in encrypted form without exchanging signed emails. You can also publish your public key and that of your organisation on Open Keys. Non-NoSpamProxy® customers can also use the service and automatically look for public keys via LDAP or web API at www.openkeys.de.

Open Keys

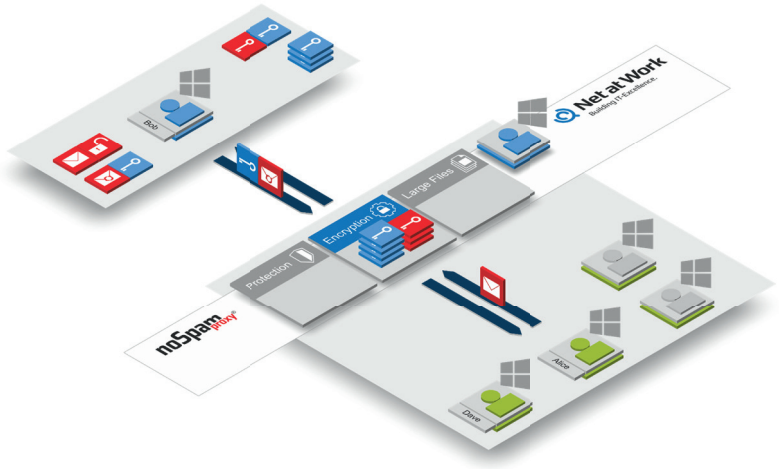
Everything you need in one place

Many providers offer additional services, special functions or interfaces for connection to other systems only as paid additional options. With NoSpamProxy® Encryption, interfaces to leading trust centers, DE-Mail, NdB (formerly DOI) and EDI@Energy are included. Naturally, there are no additional costs associated with the number of EDI messages exchanged.

Perfect synergy between NoSpamProxy® Encryption, Protection and Large Files

If you use NoSpamProxy® not only for encryption, but also for protection against spam and malware as well as for the secure transfer of large files, you will gain added security:

- Thresholds for rejecting messages suspected of being spam or malware can be increased if regular communication with business partners is encrypted and signed.
- Spam and malware scanning can be efficiently performed at the same gateway used to decrypt emails. If other solutions are used, re-routing is required, resulting in loss of time and performance.
- Large file attachments do not have to be transferred in encrypted form with the email, but via a secure upload and download, resulting in increased performance and minimised time delays.
- Additional benefits by coordinating the functionalities of the NoSpamProxy® modules.



De-Mail

NoSpamProxy® can easily be connected to a De-Mail domain, enabling users to send De-Mails directly from their default email clients.

FP AWARD 2015
DE-MAIL INNOVATION

Smart TLS management with NoSpamProxy®

The secure transmission of emails between two email servers using TLS (Transport Layer Security) should by now be a foregone conclusion. However, there are still cases where servers do not or only partially support this important feature.
NoSpamProxy® provides TLS security at the click of a mouse. The protection of the email receipt is provided by the administrator in the receive connectors of NoSpamProxy®. There, the connection security can be optionally permitted. This means that NoSpamProxy® offers StartTLS to the delivering server. The delivering server can then decide for itself whether it wants to encrypt the data or not.

> Net at Work always provided us with friendly, fast and, above all, competent support during the three-week trial operation and afterwards. NoSpamProxy® Encryption runs absolutely stable and makes our daily work much easier.
>
> Georg Ries,
> IT Manager at isarpatent

isarpatent®