HORNETSECURITY

FACT SHEET

# EMAIL ENCRYPTION

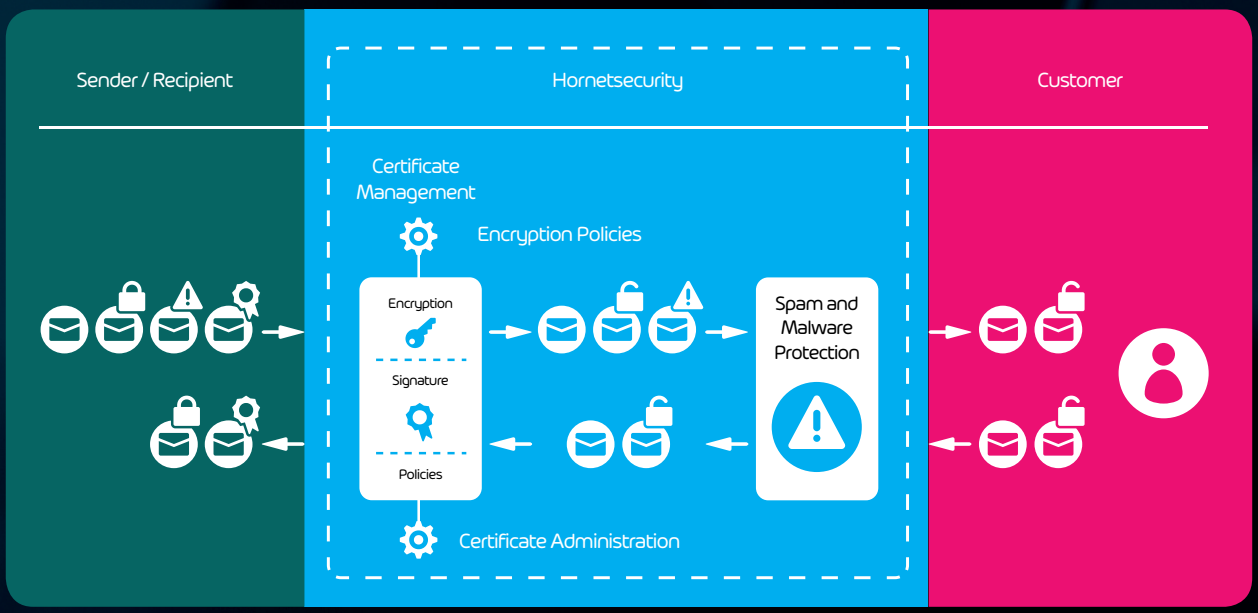
All-round encrypted exchange of emails with email encryption for reliably secure emails communication.

Business emails often contain in-house, personal or other sensitive content that could be intercepted and accessed without authorization if inadequately protected. With Email Encryption, confidential information in email communication is effectively and securely encrypted.

**Protection from:**

- **Manipulation of email messages**
- **Spying**
- **Tapping into confidential information**

## **INTEGRATION OF EMAIL ENCRYPTION** IN THE EMAIL MANAGEMENT SYSTEM




**Email Encryption from Hornetsecurity handles all aspects of certificate management.**

Encryption, decryption and signing take place fully automatically and transparently for incoming and outgoing emails. The booking and use of spam and malware protection is required in order to guarantee the functions and efficiency of Email Encryption.

HORNETSECURITY

FACT SHEET

## COMPREHENSIVE FEATURES FOR **SECURE EMAIL EXCHANGE:**

**Automatic digital signing and encryption of outgoing emails via S/MIME and PGP:** Securing emails against unauthorized modification or inspection by third parties during transmission over public networks.

**Automatic certificate management and key storage:** Hornetsecurity handles the procurement and installation of required certificates. These are kept in a central certificate store.

**Personal email certificates:** Hornetsecurity uses 2048-bit encoded certificates from one of the largest and most reputable certificate authorities (CA). When encrypting with S/MIM, each user receives his own certificate. Alternatively, certificates supplied by the customer can be imported and used.

**Automatic decryption of incoming email:** If the sender's public key is available, emails are automatically decrypted and delivered to the recipient.

**Individual setup and definition of encryption guidelines:** The control panel is used to define which encryption types are used to establish contact with communication partners: TLS, S/MIME, PGP or Websafe. This is possible either as a package or individually for specific users, groups or domains. In addition, you can define how to proceed if the key of a recipient is not available.

**Testing option for encryption suitability:** In the Control Panel you can check which encryption options the communication partner supports. The email address of the recipient is entered and the encryption technology that can be used in communication with this address is then displayed.

**Confidential communication via Websafe:** Even if the communication partner cannot receive encrypted emails, the encryption and confidentiality of email communication with certain individuals is still guaranteed.

## **AUTOMATIC ENCRYPTION** WITH MINIMAL ADMINISTRATION:

**Handling of user certificates:** New certificates for users can be requested, renewed or permanently obtained via the control panel (S/MIME subscription).

**Adaptable scalability:** It is always possible to adjust the number of encrypted email users to the needs of the customer.

**Automatic update:** Because of the cloud-based encryption service, companies always have the latest version of the service at their disposal.