E-Mail Encryption Service
Secure email communication — fully automatic and made easy with Hornetsecurity

A secure email communication is getting more and more important — a comfortable management and usability is a must, too. The Hornetsecurity Email Encryption Service connects both arguments with each other in one solution.

**Protection against spying**
Business emails often contain internal company information, personal data or other sensitive content that must especially be protected against spying. A strong encryption solution will help with this.

**Easy use**
Hornetsecurity’s cloud-based encryption technology takes administration out of end users’ hands, removing the need for them to deal with it at all.

**Compliance, transparency and control**
Implementing email encryption in a company always involves defining rules and policies at a central point, but also being able to quickly obtain an overview of all encrypted email traffic at any time.

**Easy management**
Hornetsecurity’s cloud-based encryption technology takes administration out of end users’ hands, removing the need for them to deal with it at all.

**Our cloud service benefits at a glance**
- Without any user intervention, fully automatic
- Independent of the browser used or the operating system
- No installation of hardware or software needed
- Central management of all systems by 24/7 Hornetsecurity surveillance
- Full 24/7 email and telephone support
- Operated in redundant, secured data centers in European locations

Fig: Overview on the encryption service provided by Hornetsecurity
Establishing encryption policies
In the Control Panel, the customer can define, with which encryption types he wants to communicate: TLS, S/MIME or PGP. The administrator can define this either globally or individually for single users, groups or domains.

Certificate orders in just a few clicks
If a client needs new certificates for a user, the administrator can order these through the Control Panel with just a few clicks. The advantage: The period and the type of the certificates (for signing and/or encryption) can be selected easily. The subscription model allows for a permanent buying process of the certificates.

Encryption features
- Personal email certificates for digital signatures and encryption
- Automatic certificate management
- Automatic digital signature and encryption of outgoing emails using S/MIME and PGP
- Automatic decryption of incoming emails
- Automatic key storage in a certificate storage
- Individual setup of encryption policies
- Possibility to test the encryption capabilities
- Simple ordering process of certificates
- Enforcing encryption using the Websafe

Benefit
- Hornetsecurity uses the 2048 Bit coded certificates of one of the biggest and most serious Certificate Authorities. This facilitates the exchange of encrypted data with third parties.
- No effort for buying and installation of needed certificates - Hornetsecurity is taking care of it.
- Securing the email from viewing or editing by third parties during the transport through public networks (the Internet).
- If the public key of the sender is available, the emails are being decrypted and delivered to the recipient.
- Most simple key management. Automatically, without interference by administrators or users.
- Customers can decide whether emails are being sent encrypted or unencrypted and what should happen when the recipient’s key is unavailable.
- Within the Control Panel, the administrator can test which encryption options the communication partner is using.
- Almost no time effort when ordering new certificates: If new certificates are needed, they can be ordered through the Control Panel, also on a subscription model.
- Individual securing of the confidential email communication with specific communication partners.