

E-Mail Encryption

In the Böllhoff Group

Information for our business partners

Inhaltsverzeichnis

1	E-Mail Encryption in general	1
1.1	S/MIME.....	1
1.2	PGP	1
2	Correspondence with Böllhoff	2
2.1	PGP	2
2.2	S/MIME.....	2
2.3	Webmailbox.....	2
2.4	PDF encryption	3
3	Webmailbox Workflow.....	4
4	Links to the topic.....	6

1 E-Mail Encryption in general

Maintaining confidentiality, security and integrity for documents that we exchange with our business partners is very important to us.

For this reason, you have the opportunity to share with us information on encrypted channels.

The following methods can be used:

1. Secure WebMail-Box
(for users who do not use their own e-mail encryption)
2. PGP
3. S/MIME

Böllhoff provides an email gateway for secure communication, which can deal with S / MIME and PGP key material.

If you do not have a PGP or S / MIME certificate, you can securely exchange documents with us via an SSL-protected webmail box.

As soon as a Böllhoff employee sends you an encrypted message for the first time, an e-mail will be sent to set up your webmail box.

The exact procedure is described below.

1.1 S/MIME

S/MIME (Secure / Multipurpose Internet Mail Extensions) or X.509 is a widely accepted method, more precisely a protocol, for sending digitally signed and encrypted messages. S/MIME allows you to encrypt and digitally sign e-mails.

When you use S / MIME with an e-mail, recipients can be sure that they have exactly the message in the mailbox that the sender has sent. In addition, receivers of messages can be sure that the message originates from the specific sender and not from someone pretending to be the sender. For this, S/MIME provides cryptographic security services, such as authentication, message integrity, and origin registration (using digital signatures). It also provides more privacy and security (by encryption) for electronic messaging.

(Source: Microsoft Technet Oct. 2015)

1.2 PGP

Pretty Good Privacy (PGP) is a program developed by Phil Zimmermann for encrypting and signing data.

PGP uses a so-called public-key method in which there is a unique key pair:

A public key is used to encrypt each data for the recipient and to check its signatures, and a private secret key, which only the recipient has and is normally protected by a password. Messages to a recipient are encrypted with their public key and can then be decrypted exclusively by means of their private key. These methods are also referred to as asymmetric methods, since transmitters and receivers use two different keys.

(Source: Wikipedia Oct. 2015)

2 Correspondence with Böllhoff

The secure data exchange with communication partners within the Böllhoff group can be carried out using the S / MIME or PGP method, alternatively via the Secure WebMail-Box or password-protected PDF document.

The guidelines in the encryption system at Böllhoff provide for the use of encryption and signature.

Encryption means the obliteration of a message content for third, not integrated into the communications people. In this case, the message is made readable only by the legitimate recipients by means of the methods already described.

The digital signature, similar to a medieval seal, is a confirmation of the authenticity of the message to be transmitted. By marking an e-mail with the private key of the sender, a kind of checksum is created which can be verified with the public key part of the sender for authenticity.

2.1 PGP

The exchange of PGP key material is often also done directly by e-mail. At Böllhoff, an email gateway is used which can encrypt and decrypt emails with low user load.

Email Gateway = server which receives the e-mails from the mail server and encryptes them based on specific rules and retransmits

If you already have a PGP key, you can make the public part available to the communication partner at Böllhoff.

You can find the public keys of the communication partners at Böllhoff on the key servers:

ldap: //keys.boellhoff.com or ldaps: //keys.boellhoff.com

2.2 S/MIME

The exchange of S/MIME key material is often also done directly by e-mail. At Böllhoff, an email gateway is used which can encrypt and decrypt emails with low user load.

Email Gateway = server which receives the e-mails from the mail server and encrypted based on specific rules and retransmits

If you already have an S/MIME key, you can make the public part available to the communication partner at Böllhoff.

The public S / MIME-Organization-Certificate of Böllhoff can be found on our website:

<http://www.boellhoff.com/securemail/certificate>

2.3 Webmailbox

If you do not use an encryption method such as PGP or S / MIME, we enable you to communicate securely with us via the Böllhoff Secure WebMail server.

Please use this platform to exchange confidential information with Böllhoff. The documents in this area are kept available for 60 days, a maximum of 200 MB space is available.

If no key of the recipient is known on our security system, a procedure can be used in which the actual e-mail is not sent directly to the recipient but remains on our Secure WebMail server. This is stored protected in a secure mailbox to which only the recipient gets access with a specially defined passphrase (password).

This URL can be accessed by the user at any time to access his webmail box

<http://www.boellhoff.com/securemail/webmail>



The webmail box can also be used to provide key material (S / MIME, PGP).

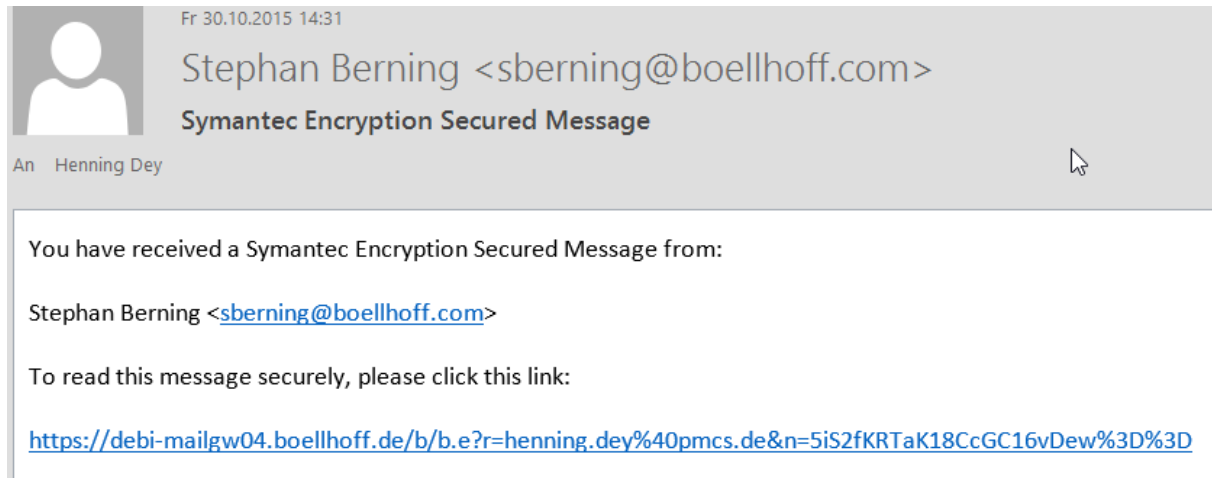
2.4 PDF encryption

If no security key is known on our security system, a procedure can be used in which the actual e-mail is stored in an encrypted PDF. This is secured with a passphrase (password) defined previously by the recipient. The PDF is then sent directly to the recipient and can be read with its passphrase.

The use of encrypted PDF documents is optionally adjustable by the recipient in the webmail box.

3 Webmailbox Workflow

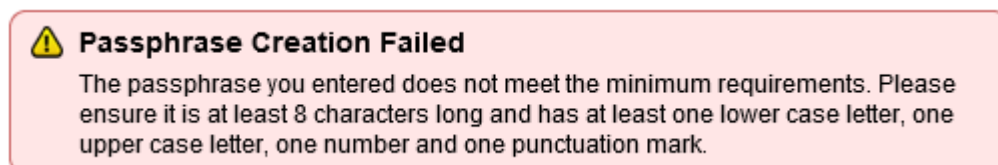
If you will be contacted with an encrypted message, you will receive an email with the following content:



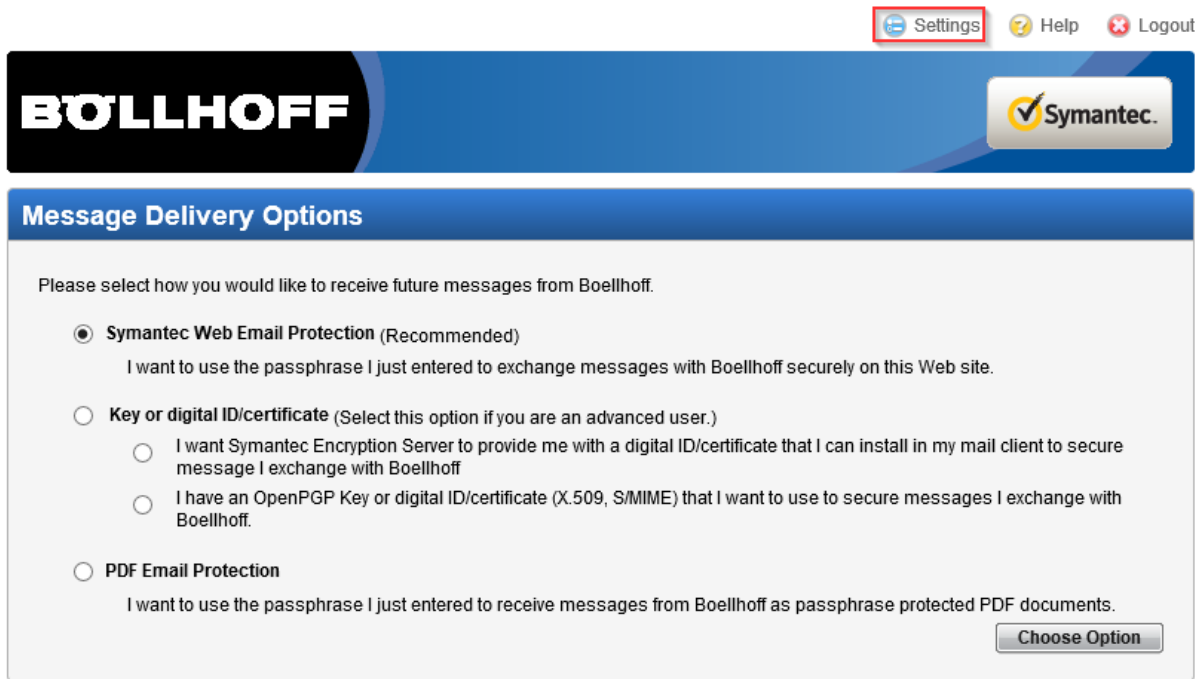
When you visit the website from the e-mail, a passphrase must be defined:

A screenshot of a web page for creating a passphrase. The top has a blue header with the 'BOLLHOFF' logo on the left and a 'Symantec' logo on the right. Below the header is a blue bar with the text 'You have received an encrypted message from Boellhoff'. The main content area is white and contains the following text: 'Please create a passphrase to secure future messages delivered to you. This server requires your passphrase to meet the following requirements:'. This is followed by a bulleted list: '• They must be at least 8 characters long.', '• It must include an uppercase letter, a lowercase letter, a digit and a punctuation mark.' Then it says: 'For example, "kittycat" is not a valid passphrase, but "k1ttYc@t" is a valid passphrase. Here are some recommendations for protecting your passphrase:'. This is followed by another bulleted list: '• Use an easy to remember passphrase that you don't need to write down.', '• Don't use obvious passphrases that can be easily guessed.', '• Don't make your passphrase a single word.', '• Don't use famous quotations.' Below the list are two input fields: 'Passphrase: [text box]' and 'Confirm Passphrase: [text box]'. At the bottom right of the form is a 'Continue' button. The footer of the page reads 'Copyright © 2014 Symantec Corporation. All Rights Reserved.'

If the passphrase does not meet the standards set, an error message is displayed:



After successful login to the web portal, a selection page is displayed. Here you can set the setting for the future e-mail transmission.



The screenshot shows the top navigation bar with 'Settings' (highlighted with a red box), 'Help', and 'Logout' links. Below the navigation bar is a blue header with the 'BÖLLHOFF' logo on the left and the 'Symantec' logo on the right. The main content area is titled 'Message Delivery Options' and contains the following text: 'Please select how you would like to receive future messages from Boellhoff.' There are three radio button options: 1. 'Symantec Web Email Protection (Recommended)' with a sub-option 'I want to use the passphrase I just entered to exchange messages with Boellhoff securely on this Web site.' 2. 'Key or digital ID/certificate (Select this option if you are an advanced user.)' with two sub-options: 'I want Symantec Encryption Server to provide me with a digital ID/certificate that I can install in my mail client to secure message I exchange with Boellhoff' and 'I have an OpenPGP Key or digital ID/certificate (X.509, S/MIME) that I want to use to secure messages I exchange with Boellhoff.' 3. 'PDF Email Protection' with a sub-option 'I want to use the passphrase I just entered to receive messages from Boellhoff as passphrase protected PDF documents.' A 'Choose Option' button is located at the bottom right of the form.

Copyright © 2014 Symantec Corporation. All Rights Reserved.

Symantec Web Email Protection

Use of the Web mailbox with reply function and local storage of the messages on the PGP-Mailgateway.

Schlüssel oder digitale ID bzw. digitales Zertifikat

Key material can be provided here. This can be both an S / MIME certificate and a PGP key.

PDF Email Protection

With this setting, encrypted e-mails are sent, which are encrypted with the passphrase of the webmailbox.

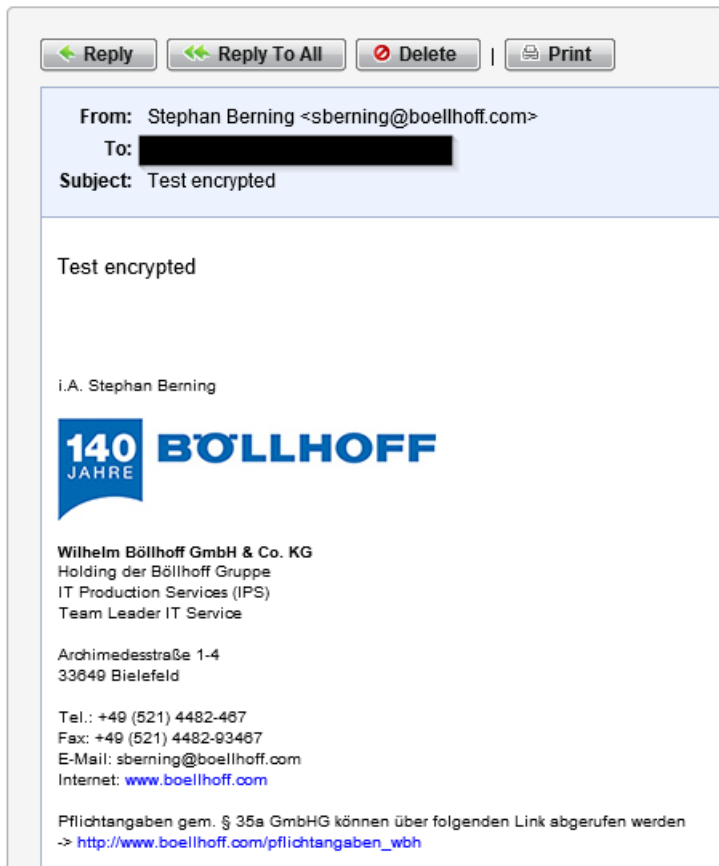


The settings dialog can be changed later via the menu Settings (red marked in the screen section).

This URL can be called at any time to access your own webmail box

<http://www.boellhoff.com/securemail/webmail>

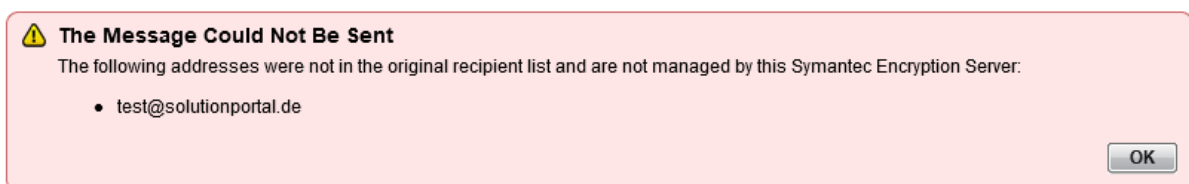
The sent e-mail is now visible via the inbox of the webmailbox:



The usual functions can be used here. You can also use the "Compose" button to communicate with Böllhoff employees.



Please note that only internal users can be registered. The warning is as follows:



4 Links to the topic

Information for our Business partners:

<http://www.boellhoff.com/en/securemail>

<http://www.boellhoff.com/de/securemail>

Public Part S/MIME Certificate Böllhoff:

<http://www.boellhoff.com/securemail/certificate>

Link Secure WebMail-Box for Business partners:

<http://www.boellhoff.com/securemail/webmail>