Secure Exchange of E-Mail with BASF

Brief Instructions for External Communication Partners

1 Introduction

BASF maintains eMail contact with a large number of communication partners. Since confidential information is often exchanged, BASF supports the exchange of encrypted and digitally signed eMail via a secure gateway.

Compared to an end-to-end solution, this procedure offers the advantage of substantial transparency and a high level of ease of use. In this way we intend to achieve higher levels of acceptance and increased security.

The secure mail gateway functions as a postmaster and centrally carries out the necessary encryption and decryption of eMails as well as performs digital signatures. Emails sent from BASF to external recipients are encrypted on the gateway and affixed with a digital signature when appropriate. Conversely, eMails from external partners are decrypted on the gateway and when appropriate the digital signature is checked there as well. The decrypted eMails are then forwarded to the appropriate BASF employees.

As exchange formats S/MIME and PGP encoding are supported.

2 Using S/MIME

S/MIME is a standard exchange format for secure mail traffic. It is supported by most conventional mail clients, e.g. Microsoft Outlook, Outlook Express, Netscape Messenger and Lotus Notes[1].

We assume that you already use an S/MIME-capable eMail client. If this is not the case, please contact your administrator or consider to use PGP (chapter 3) for secure eMail communication with BASF.

2.1 Certificates

Before secure message exchange can take place, both communication partners will have to have digital certificates (see FAQs) and will have to inform each other regarding the certificates. For this purpose the BASF eMail gateway provides certificates for BASF employees which are signed by the root certificate of our eMail gateway.

The root certificate of the BASF eMail gateway can be found at www.basf.de/securemail, where you can download it, install it in your eMail client and check the fingerprint (see FAQ) of the root certificate. You should do this before beginning to exchange certificates with a BASF employee.

If you have an S/MIME-capable client, but do not yet have your own certificate, you can request a certificate from a certification center such as TC Trustcenter, Thawte, S-Trust or Verisign (see FAQ).

[1] Use of Notes-internal S/MIME functionalities is not recommended until Lotus Notes R6 or higher. If you use Lotus Notes R5 or earlier versions, the use of S/MIME can only be recommended when you have installed a corresponding S/MIME plug-in on your PC.

2.2 Certificate Exchange

For encryption, the eMail gateway requires your personal certificate as well as the root certificate of the issuing instance. If your company also uses an eMail gateway to secure eMail communication which works only with a "domain certificate" (see FAQ), the domain certificate is required here instead of your personal certificate.

Send the following to your communication partner at BASF in an unencrypted eMail:

- These certificates
- Name and telephone number of the instances responsible for the certificates

The BASF employee will then make sure that the certificate is made available to the BASF eMail gateway.

In case you can not send the certificate to your BASF communication partner directly via eMail, you have the following alternative possibilities as well:

1. Send a signed email to securemail@basf.com which will contain your certificate and the root certificate in most cases automatically.
2. If your company's root certificate is publicly available in the Internet, it is sufficient to send a link to the certificate.
3. If you can not send your own certificate by eMail, it is sufficient for you to send a signed eMail to your BASF communication partner several hours after you have forwarded the root certificate (or a link to the certificate) to the communication partner. The eMail gateway will then automatically import your certificate.
4. If both your personal certificate and your company's root certificate are available via a publicly accessible directory service (LDAP directory), it is sufficient to send the address of the directory service to your BASF communication partner.

3 Using PGP

Many eMail implementations exist for PGP according to a variety of standards. The BASF eMail gateway has been configured so that it can communicate with a maximum number of PGP users.

In the following we will assume that you already use a PGP-capable eMail client. Should this not be the case, please contact your administrator or consider to use S/MIME (chapter 2) for secure eMail communication with BASF.

3.1 PGP Keys

Before secure exchange of messages can take place, both communication partners must have PGP keys and the keys must be known to the respective other user. For this purpose, the BASF eMail gateway issues PGP keys which have been signed by our Trusted Introducer (see FAQs).

You will find the PGP key of the BASF Trusted Introducer at www.basf.de/securemail. You can download the key from there and import it to your PGP client or check the fingerprint. Do this before beginning to exchange keys with the BASF employee.

3.2 Key Exchange

Take the following steps to exchange PGP keys:

1. Export your PGP key (public key) from the PGP client in ASCII format and send it (see FAQ) in an unencrypted mail to your communication partner at BASF. Also indicate a telephone number where you may be reached for a random spot check of the fingerprint.
   If your company has realized the Trusted Introducer concept (see FAQ), it is helpful when you also send us the Trusted Introducer's key and the telephone number of a contact person who is responsible for the key.
2. You will receive the PGP key of your BASF partner by email and have to import the key to your PGP client manually (see FAQ).

3.3 Encrypted PGP files

If your eMail client does not feature direct PGP support and you can only use PGP for file encryption, you can add the encrypted file to your eMail as attachments. The file is then decrypted by the BASF eMail gateway and forwarded in plain text form to the recipient at BASF.

Conversely, if you receive an attachment from a BASF employee which has been encrypted with PGP, you can first save this attachment to your hard drive and then decrypt the saved copy using PGP.

4 Contacts

Technical questions regarding the eMail gateway can be addressed to

- securemail@basf.com

Questions regarding operations can’t be answered under this email address.

5 Appendix

5.1 S/MIME CA Certificate

Fingerprint

SHA1: 8E6F 5283 630D 7059 0AB1 1603 4B5A 7D29 59DA E3C5

MD5: 35C3 ADDE 5326 F40B FCDD 6B06 622A 030C

5.2 PGP Key Trusted Introducer

Fingerprint

DED8 53C8 80D8 D7CF BE81 13C5 6BE2 EECE 2FF7 E7C4