Exchanging Secure E-Mails with BASF

Frequently Asked Questions (FAQ)

Encryption

In order to securely exchange eMail, it must first be encrypted so that it can be decrypted and read only by the recipient intended by the sender. The necessary key is transferred in the form of a digital certificate. This certificate indicates which key is to be used for eMail encryption for a particular recipient. The key entered there can only be used for encryption and not for decryption. It can therefore be transmitted safely via insecure networks.

BASF's secure eMail gateway uses the recipient's digital certificate to encrypt outgoing mail so that only you as the recipient can read the content of the eMail. Furthermore, the eMail gateway automatically decrypts data which you send to a recipient at BASF so that your communication partner at BASF can read the data.

Digital Signature

A digital signature makes it possible to identify the sender of an eMail. It also provides proof of the fact that the data have not been altered during transmission: The digital signature is destroyed if the data is changed after being sent. In order to check digital signatures, a digital certificate is needed, based on which the signature can be attributed to a particular person or company.

The secure eMail gateway at BASF makes it possible to digitally sign outgoing eMail with a user certificate so that you as the recipient can check the authenticity of the eMail beyond any doubt. Furthermore, the eMail gateway checks digitally signed eMails and shows the recipient the creator of the eMail.

Digital Certificates

A certificate is a public key which is digitally signed by a trustworthy instance referred to as a certification authority or trust center. This confirms the fact that a public key really belongs to the person indicated in the user ID of the key, and as such can be compared to an electronic identification card.

S/MIME

1. What is a root certificate?

   The root certificate is the digital ID card of a trustworthy instance which is used to sign other digital certificates (-> digital certificates). The root certificate only contains the instance's own digital signature (-> digital signature) and is not signed by any other instance.

2. What does it mean to "check the fingerprint of a certificate"?

   In order to determine the authenticity of a digital certificate, every certificate has a so-called fingerprint. This fingerprint is a unique number which is generated based on the content of the certificate using a one-way mathematical function. This fingerprint is attached to the certificate and can be verified by the user of the certificate.

3. How can I check the fingerprint of the root certificate?

   The root certificate of the secured eMail gateway at BASF can be checked via the web page http://www.basf.de/securemail. Here BASF publishes its certificate as well as the corresponding fingerprint. After downloading the certificate, the fingerprint contained in the certificate can be compared with the fingerprint published on the web page. To do so, the certificate must be opened in a suitable viewer (a double click is usually enough under Windows 2000). Under the heading "Details", the field "Fingerprint" can be compared with the information on the web page. If the two numbers are identical, you can import the root certificate and consider it to be trustworthy. If the information does not match, please inform your communication partner.

4. What is a domain certificate?

   A domain certificate is a certificate which is not allocated to a specific person (e.g. hans.muster@firma.de), but rather to a service of a special domain (e.g. postmaster@firma.de). This means in the case of a secure eMail communication that eMail to all of the recipients in this domain can be encrypted using this certificate.

5. Where can I get a S/MIME certificate?

   If your company does not already operate a public key infrastructure, you can also receive a S/MIME certificate issued by an external service provider, a so-called trust center. Many such service providers also offer the possibility of requesting a certificate at no cost. Here the person is identified exclusively via his eMail address, which must also be specified when requesting such a certificate. More extensive investigation of personal data is not necessary.

   The company TC Trustcenter offers this type of service with its product "*Express Zertifikat*". Here an S/MIME certificate for secure eMail communication can be acquired for free in five steps.

   In the first step the TC Trustcenter root certificate must be installed. Then the user data is collected. In the third step the eMail address is checked, in the fourth step the certificate is generated and installed and in the fifth step the certificate is tested. The full instructions on how to acquire a digital certificate are available at: http://www.trustcenter.de/set_de.htm.

PGP

1. Where can I get a PGP plug-in?

   Versions of PGP are available for free at the web page http://www.pgpi.com. PGP supports a variety of eMail programs:

   - Qualcomm Eudora
   - Microsoft Exchange
   - Microsoft Outlook
   - Microsoft Outlook Express

   A plug-in exists for Lotus Notes which is however not available in a free version.

   The use of the free PGP version in commercial environments is highly restricted and should be investigated in advance. In addition to PGP there is also the product GNUPG, which is also available for free and which includes plug-ins for Eudora, Outlook Express and Outlook.

2. How can I get the PGP key of a BASF employee?

   Contact your communication partner within BASF and request his PGP key. He will send you the public part of his PGP key as well as the PGP key of the Trusted Introducer of BASF.

3. What is a Trusted Introducer?

   A Trusted Introducer is comparable with a certification authority with S/MIME. The Trusted Introducer is an instance which signs the PGP keys of other users. If the Trusted Introducer has been checked (e.g. by comparison of the fingerprint) and has been found to be trustworthy, in the future no keys which have been signed by this Trusted Introducer need to be checked. The Trusted Introducer principle is particularly common at larger companies. The secure eMail gateway at BASF also works with a Trusted Introducer.

4. How can I verify the authenticity of the PGP key of my communication partner?

   The verification will be done indirectly by verifying the fingerprint of the PGP key of the Trusted Introducer (Key ID: 2FF7E7C4) of BASF. You will receive the PGP key of the Trusted Introducer by receiving the PGP key of your communciation partner with BASF or via the web page http://www.basf.de/securemail. Here BASF publishes the PGP key of the Trusted Introducer as well as the corresponding fingerprint.

   If you will import the PGP key of your communication partner afterwards, the key will be marked as trustworthy.

5. Why does the administrator of the BASF gateway need to check my fingerprint?

   In order to ensure that your are the owner of the PGP key whose public part has been stored in the secure eMail gateway, a random check of fingerprints is conducted. The inspection is carried out on a spot-check basis, since it would be difficult to check every key being imported due to the large number of PGP keys to be expected.

6. How can I view the fingerprint of my PGP key?

   If you use PGP, open your key ring, select the key to be inspected, click with the right mouse key and then view the key by selecting "Key Properties". In the dialog box which opens next, the fingerprint of the key is also displayed.