1. Introduction

BASF relies heavily on email to interact with a large number of business partners. Since confidential information is often exchanged, BASF supports the exchange of encrypted and digitally signed emails.

2. Signing and encrypting

By digitally signing an email, the recipient can verify the integrity of the email message. It proves that the sender signed the contents of the message and that the contents have not been altered during transition.

BASF supports cryptographically secured external communications using standardized S/MIME and PGP methods.

Encrypting outgoing emails that contain business-critical content is mandatory when the recipient's trustworthy public key is available. In this case, BASF prefers to use the S/MIME method rather than PGP.

If confidential content should be sent, but there is no trustworthy key available for the intended recipient, the information is kept on hold and not sent. Instead, the information is made available for 30 days on BASF's securEmail WebApp, where it can be viewed, downloaded and replied to.
3. Initiation of secure email communication with BASF

To start a secure email communication your BASF contact sends you an email which is classified as “Confidential”. If your key is already available on the BASF Secure Mail Gateway you will immediately receive the secured email in your personal mail client.

Otherwise BASF will retain the email that is intended for you. You will receive a notification email signed by the sender with the Subject “BASF Securemail: Respond to Receive an Encrypted Email / Antworten Sie zum Empfangen einer verschlüsselten E-mail” (Fig. 1).

Fig. 1: First Notification Email
4. Possibilities for encrypted email exchange

There are two different possibilities available to enable the secure exchange of emails with BASF:

Option 1: S/Mime or PGP
Option 2: BASF securEmail WebApp

4.1. Option 1: Encryption using S/MIME or PGP

If you are already using S/MIME, simply reply to the notification email and sign it with your S/Mime certificate. Your certificate will be trusted if the issuer certificate authority (CA) is available on the BASF Secure Mail Gateway. Otherwise it will be validated by the BASF administrator timely and as soon as this has been done you will receive the encrypted email in your mailbox. In the rare case the certificate can’t be trusted, you can register for BASF securEmail WebApp (see Option 2).

For BASF employees BASF provides certificates which are signed by the issuer certificates of the BASF PKI. The root certificate and the intermediate certificates can be found at www.basf.com/securemail, where you can download them, install them in your email client and check the fingerprints of the certificates.

If you are already using PGP, please reply to the notification email (fig.1) and attach your public PGP key. Once you provide your PGP key with the reply email it will be automatically stored on the BASF Secure Mail Gateway and become available for future use.

For BASF employees the BASF Secure Mail Gateway issues PGP keys which have been signed by our Trusted Introducer. You will find the PGP key of the BASF Trusted Introducer at www.basf.com/securemail. You can download the key from there and import it to your PGP client or check the fingerprint.

4.2. Option 2: BASF securEmail WebApp

To use the BASF securEmail WebApp system, you need Internet access and a browser. Via the BASF securEmail WebApp, the recipient can also transfer valid public S/MIME or PGP key material to BASF. Preferably, however, a signed email should be sent in reply to the notification email; that email is then used to extract the key material and verify its’ trustworthiness.
Request to register for BASF securEmail WebApp by clicking on the link in the notification email “Request BASF securEmail WebApp registration” (Fig. 1). You will receive an email from Administrator BASF Securemail containing the link to login to BASF securEmail WebApp (Fig. 2).

4.2.1. Registering for BASF securEmail WebApp

By clicking on “REGISTER” you will be directly prompted to insert and confirm a NEW password of your choice. The condition for passwords will be displayed (Fig. 3).
4.2.2 Login to BASF securEmail WebApp

The Login page of BASF securEmail WebApp then appears (Fig. 4). Here you can login and also download PGP keys or S/MIME certificates of BASF employees.

Please log in with your email address and your chosen password. You can log in anytime using https://securemail.basf.com
After logging in you will see the Start page of BASF securEmail WebApp (Fig. 5) which shows the Overview.

Fig. 4: BASF securEmail WebApp Login

Fig. 5: Your BASF securEmail WebApp mailbox
4.2.3. BASF securEmail WebApp mailbox

Select Inbox to show the emails which are stored for you on the secured WebApp server.

Your messages are listed in chronological order in your inbox (Fig. 6). By clicking on the subject line or on the envelope icon, you can open the corresponding message. Messages that have not been read are indicated by a closed envelope.

You can now access the securely sent email in the Inbox (Fig. 7).
As you can see in the menu you can now reply to this email, delete or save the email in diverse formats on your hard drive. It is also possible to export the emails as an *.eml file so that you can import the emails into your email program (e.g. Microsoft Outlook).

Please notice that the mail is kept on the server for 30 days. During this period, you can access the emails at any time via a browser using your user ID (your email address) and password. When a new email arrives in your BASF Secure Email mailbox, you are notified with a message.

When an email contains an attachment, this is indicated by a paper clip shown next to the sender’s name. You can download any file attachments onto your computer.

You can use the “New Message” button to create an email to other BASF employees. This will be sent securely to his/her mailbox.
4.2.4. BASF securEmail WebApp Preferences

Select the “Preferences” button to change your settings. You can change your password here. By selecting “Certificates” you can upload S/MIME or PGP keys in case you prefer one of those encryption methods. Don’t forget to delete outdated keys.

You can also change your User Preferences as shown in Fig. 8.

![User Preferences](image)

Fig. 8: User Preferences

If you want to change the Security Type to S/MIME or PGP you must have uploaded your certificate before. After changing the Security Type to S/MIME or PGP and clicking on Apply Changes you will receive the next encrypted email from a BASF employee in your mailbox and not in BASF securEmail WebApp. Your login information will still be valid.
4.2.5 Responding to an email

Fig. 9: Replying to an email

You can also use the BASF securEmail WebApp interface to send secure messages to BASF. This can be a response to an existing email in your mailbox (Fig. 9), or it can be a new message. You can attach files to any email. The "To:“, "Cc:“ and "Bcc:“ fields only accept valid BASF email addresses. If you want to address multiple people at BASF, their addresses are to be separated by a comma (","), or semicolon (";").

It is not possible to send an email to a non-BASF address; consequently, any message containing such an address will be rejected.

5. Requesting public keys of BASF employees

If you use S/MIME or PGP encryption, you need the public key that your communication partner at BASF uses. This key enables you to establish encrypted communication. You can request the public key from BASF via the following link:

URL: https://securemail.basf.com

BASF won’t provide S/MIME certificates and PGP keys for all employees here. Only keys of users of the Secure Mail Gateway can be downloaded.
Therefore BASF recommends to always initiate secure email communication on the BASF side. Please ask your contact person to send you a confidential email. In that way you will always receive his/her certificates automatically or you can reply using BASF securEmail WebApp.

The procedure for requesting a public key is described in the example provided in Fig. 10 below. In the login page (Fig. 4) don’t log in but select “Request a Public Key”.

Enter your own email address first and in the second line the email address for which you want to request the key, click on “Request a Public Key”. The result of your request will be displayed:
The S/MIME certificate and the PGP key that you requested for your BASF communication partner is then sent to your personal mailbox (see Fig. 12). This is an automated response with the sender address of the person from whom you requested the key.

![Fig. 12: Received email with keys](image)

This mail contains the PGP public key as an .asc attachment and is S/MIME signed by the sender.

If you use an S/MIME certificate or PGP key for email encryption, you will always receive the emails directly in your personal email client. In this case, the encryption/decryption of the messages takes place automatically between your email program and BASF.

In case of problems or questions regarding the BASF Secure Mail service please contact postmaster-securemail@basf.com.