Deutsche Bank
Global Transaction Banking

Secure Exchange of Information via Email – Frequently Asked Questions

Last Update, December 2018

Table of Contents

1. Why should I enhance my email security?

Cyber attacks on the systems and data of companies and their clients are on the rise around the globe. Hackers employ sophisticated methods with a view to reading, amending or deleting standard emails. Unauthorised persons can thus read and tamper with any sensitive data not sent in encrypted form.

What's more, you cannot be certain of the sender's identity when you receive a standard email. It may have been sent by fraudsters or crooks under a bogus address.

Deutsche Bank is aware of all these risks. As a bank, we have to deal with particularly sensitive data and comply with strict requirements, and consequently regard it as our duty to ensure ongoing secure communication with our clients and business partners alike.

We therefore wish to encrypt our mutual email communication for the exchange of sensitive information in order to give you the assurance that you are always corresponding with a bona fide Deutsche Bank employee. We also take care by receiving confidential information from you via this secure channel.

Examples of confidential information are product and pricing agreements as well as account or transaction related details. We also set store by receiving confidential information from you via this secure channel.

2. What is an email certificate?

An email certificate is a security feature that proves your identity and provides the assurance that third parties have not tampered with your email. Using your certificate, you can sign the email to prove your identity and using the receiver's certificate, you can encrypt the emails so that only the intended recipient can read the email.

3. Why should my company use digital certificates?

Digital certificates form the basis of secure email communication. These digital documents identify senders and recipients as the bona fide holders of their email addresses. Certificates are only issued following verification of identity.

Deutsche Bank has to deal with particularly sensitive data and comply with strict regulatory requirements, and consequently regard it as our duty to ensure ongoing secure communication with our clients and business partners alike. We therefore wish to encrypt our mutual email communication for the exchange of sensitive information in order to give you the assurance that you are always corresponding with a bona fide Deutsche Bank employee.

4. What type of email certificates do I need?

An email certificate is a security feature, so it is essential that your identity is verified beyond doubt. Encrypted email communication with Deutsche Bank calls for certificates based on the encryption standards: Pretty Good Privacy (PGP), or Secure/Multipurpose Internet Mail Extensions (S/MIME).

The following types of certificates are supported:

1. Organisation-validated email certificates: Proof of the certificate holder's organisation or company is required in addition to proof of his or her identity. The certificate contains both the name of the certificate holder and that of his or her organisation or company

2. Identity-validated email certificates: The identity of the certificate holder is proven by means of an ID card. His or her identity is visible to the email recipient.

5. Who issues and administers email certificates?

The following options are available:

1. Your IT department issues the certificate. It verifies your identity internally before sending you the certificate

2. You request the certificate with verification of your identity from a public issuer such as Digicert, Global Sign, Swiss Sign, Comodo, QuoVadis, D-Trust, A-Trust, Entrust or Volksverschlüsselung/Frauenhofer

6. Where can I get a certificate for myself or my company?

Individual certificates can be purchased through global certificate provider such as Verisign, Digicert, etc. Please check with your company's IT department whether your company already has its own root certificate in place.

7. Which certificates are automatically trusted by Deutsche Bank?

Most of the global certificate providers' certificates are automatically trusted. If your company is enrolled in EBCA (European Bridge Certificate Authority), your company's root certificates are automatically trusted as well. PGP and S/MIME are both email industry encryption standards. The support varies by product; however, popular programs like Outlook and Thunderbird natively support S/MIME.

8. What if my company issues its own certificates – how can mutual trust be established with Deutsche Bank?

If you would like Deutsche Bank to trust automatically on your company's root certificate, a form needs to be filled out and our key management team will verify.

9. Where can I seek help?

Please contact your IT administrator or the support service of a public issuer of email certificates if you have any questions regarding the purchase, administration or installation of certificates. Further information on secure email communication and certificates is available on our website http://cib.db.com/insights-and-initiatives/initiatives/security_at_deutsche_bank.htm

10. What should I do with the email certificate once I have received it?

You should provide Deutsche Bank with the certificate as soon as it has been installed. This merely involves sending an email bearing your signature to any Deutsche Bank staff member or group email box. Your certificate is then saved for all your communication partners at Deutsche Bank. Your Deutsche Bank communication partners will also send you their certificate via a signed email. This process enables you to send and read the encrypted emails you have exchanged with each other.

11. Does a digital certificate work with every email program?

PGP and S/MIME are both email industry encryption standards. The support varies by product; however, popular programs like Outlook and Thunderbird natively support S/MIME.

12. We prefer not to use certificates to communicate with Deutsche Bank – what other options are there?

dbSecureEmail provides for a webmail portal (https://securewebmail.db.com) that allows users to read and send encrypted emails without having certificates.

13. Does Deutsche Bank support Transport Layer Security (TLS) as well?

Yes, in case you prefer to use TLS this can be arranged via your Deutsche Bank service representative as well.