E-Mail - Encryption

09/13/2026 06:38:11

FAQ Article Print

Category:	Kommunikation & Kollaboration::E-Mail	**Votes:**	0
State:	public (all)	**Result:**	0.00 %
Language:	en	**Last update:**	12:11:45 - 11/27/2025

Keywords

Encryption Entry LDAP PKI E-Mail

Solution (public)

TU Dresden uses the public key infrastructure of the DFN-Verein ([1]DFN-PKI) to issue, distribute and verify certificates. S/MIME (Secure/Multipurpose Internet Mail Extensions) is used as a standardized procedure for encrypting and signing emails.

Without a digital signature, any email can be manipulated very easily and the sender's side of the email cannot be verified. The digital signature of an email has the following advantages:
- The recipient of the email can verify that the message originates only from the specified sender.
- The recipient of the email can check that the message has not been tampered with en route. (integrity)

Requirements
- You need a personal certificate to send an encrypted email:
[2]Instructions for requesting a personal certificate

- The certificate must be integrated into the local email client or operating system:
[3]Instructions for integrating the personal certificate

- The recipient's certificate must also be known.
(see section "Receive the recipient's certificate")

Personal Certificate

Note and remember the password for your personal certificate assigned when you applied and save the certificate file on your device. The certificate file can only be downloaded during the application process. It is not possible to use the certificate without the certificate file or the password. In this case, a new one must be requested.

Duration

Certificates are valid for a limited period of 2 years. If a certificate expires, you will receive information by email in good time. You must then apply for a new certificate.

Expired Certificates

Expired certificates and the corresponding passwords should continue to be saved and integrated into the email client. This is the only way to continue decrypting encrypted (older) emails.

Publication

All personal certificates and certificates of functional addresses are automatically provided in the global address book of Exchange and LDAP directory of the DFN-PKI (see below), so that the exchange of encrypted emails is possible.
TU Dresden is legally obliged to provide the information (email address, certificate) for the encryption of employees in a publicly accessible directory. The legal obligation results from § 2 para. 1 sentence 3 of the Saxon E-Government Act (SächsEGovG): “Encryption procedures must be offered and generally used for electronic communication.”

Receive the recipient's certificate Email clients integrated via the Exchange protocol, such as Gnome Evolution or Microsoft Outlook, can access the global address book without any further setup. This allows you to find all members of TU Dresden and the email client automatically retrieves their certificates.
If your mail client is not connected via Exchange or you would like to contact people outside TU Dresden, you can use one of the following options to obtain the certificate.
Variant 1: Exchange of a signed email

To send an encrypted email, the recipient's certificate must be known. To do this, the keys must initially be exchanged via an email signed with the certificate.

Example: Person A sends an email signed with their personal certificate to person B. Person B now knows the certificate of person A and can send them an encrypted email directly.

Variant 2: Integrate directory service DFN PKI LDAP

The DFN PKI offers a public LDAP (Lightweight Directory Access Protocol) directory service which can be used as a DFN-wide email address book for email addresses and certficiates. You can configure this LDAP directory as an address book in your email client in order to find people and their associated

certificates to send them encrypted email. The directory contains all user certificates of the old DFN PKI and all SECTIGO-issued certificates of TU Dresden and several other organisations (mostly Max Planck insitutes). Further organisations might be added in the future.

You can also browse the DFN PKI directory directly using an LDAP browser:

Hostname: ldap.pca.dfn.de
Port: 389 (also with SSL) or with LDAPS 636
Base DN: o=DFN-Verein, c=DE

Setup in the Email Client Depending on the email client used, access to the contacts or certificates is possible, but may require the directory service to be integrated into the program:

Email Client	Contact	Certificates	Automatic Access without Setup
Apple Mail for macOS	✓	-	-
[4]Instructions			
GNOME Evolution for Linux	✓	✓	✓
(only necessary for TUD external contacts)			
Microsoft Outlook for macOS	✓	✓	✓
([5]only necessary for TUD external contacts)			
Microsoft Outlook for Windows	✓	✓	✓
([6]only necessary for TUD external contacts)			
Mozilla Thunderbird	✓	✓	-
[7]Instructions			

[1] https://www.pki.dfn.de/ueberblick-dfn-pki
[2] https://faq.tickets.tu-dresden.de/v/ItemID=1027
[3] https://faq.tickets.tu-dresden.de/s/Keyword=E-Mail,Einrichtung,Zertifikat;LanguageIDs=1
[4] https://faq.tickets.tu-dresden.de/v/ItemID=489
[5] https://faq.tickets.tu-dresden.de/v/ItemID=491
[6] https://faq.tickets.tu-dresden.de/v/ItemID=512
[7] https://faq.tickets.tu-dresden.de/v/ItemID=514