

Linux - Evolution

Prerequisites

- Correct setup of the email client [Evolution](#)
- Correct integration of the [certification authorities](#) into the operating system.
- **Valid digital [User certificate](#)**

Configuration

- Start Evolution
- Edit → Settings → Certificates
 - Card “Your certificates” → Import
 - Point to the file you created under “Issue” in the [User certificates](#) section
 - Enter the corresponding password
 - Click on the “OK” button
 - Card “Certification authorities” → Check the required certification authorities
 - T-Systems Enterprise Services GmbH
 - T-TeleSec GlobalRoot Class 2
 - Verein zur Foerderung eines Deutschen Forschungsnetzes (Association for the Promotion of a German Research Network)
 - DFN-Verein Certification Authority 2
 - DFN-Verein Global Issuing CA
- Edit → Settings → E-mail accounts
 - <Your e-mail account> → Edit
 - Security tab, section Secure MIME (S/MIME)
 - Signature Certificate: Select your personal digital user certificate here.
 - Signature algorithm: SHA256
 - Always sign outgoing messages from this account: activated
 - Encryption certificate: Select your personal digital user certificate here.
 - Always encrypt outgoing messages from this account: enabled.

Now you have carried out all the necessary steps to sign every e-mail. Provided you have the public key of your communication partner, you can also encrypt every e-mail.

Use

Sign

- Click on “New” → “New e-mail message” in Evolution and compose it.
- Before sending, check at the top of DeepL access that the message is digitally signed.
 - The button “Sign this message with your S/MIME signing certificate” at the top of the DeepL access is activated by default.
 - The button “Encrypt this message with your S/MIME encryption certificate” at the top of the DeepL access is enabled by default, it must be disabled.

- As soon as you click on “Send”, the e-mail is digitally signed and subsequently sent.
- The communication partner sees the loop symbol as a sign of a digitally signed e-mail.

Encrypt

To encrypt an e-mail, you must first have the communication partner's public key:

- Have your communication partner send you a digitally signed e-mail, for example. Evolution automatically adds the public key to its certificate store.
- Click on “New” → “New e-mail message” in Evolution and compose it.
- Before sending, check at the top of DeepL access that the message is digitally encrypted.
 - The button “Sign this message with your S/MIME signing certificate” at the top of the DeepL access is activated by default.
 - The button “Encrypt this message with your S/MIME encryption certificate” at the top of the DeepL access is activated by default.
- As soon as you click on “Send”, the e-mail is encrypted and then sent.
- The communication partner sees the padlock symbol as a sign of an encrypted e-mail.

From:
<https://hrz-wiki.jade-hs.de/> - **HRZ-Wiki**

Permanent link:
<https://hrz-wiki.jade-hs.de/en/tp/email/security/linux-evolution>



Last update: **2021/11/21 14:04**