E-Mail Security

Digital, electronic e-mail signatures and the encryption of e-mails can be used to increase security in the e-mail sector.

To be able to use these, a digital user certificate is required. During the creation process, a digital key pair is generated which is confirmed by a certification authority. This key pair consists of 2 parts, the private and the public key:

- Private key: This is password protected and always remains in the possession of the user.
- Public key: This is required by the communication partner and must be made known to them in some way.

Signing

Principle: You use your private key to sign your e-mail. The communication partner can then use your public key to check whether / that data is unchanged.

Encrypt

Principle: You encrypt your e-mail with the help of the communication partner's public key. The communication partner can then decrypt the e-mail using his private key. You must therefore first have the communication partner's public key for encryption.

Prerequisites

A basic prerequisite for use is the correct integration of the certification authorities in the operating system you are using and a valid digital user certificate. Then configure the appropriate application software:

Pages in this namespace:

A

- Apple iOS/iPadOS - Mail
- Apple macOS - Mail

G

- Google Android

L

- Linux - Evolution

M

- Microsoft Outlook 2016/2019

M cont.

- Microsoft Outlook for Mac 2019
- Mozilla Thunderbird

From:
https://hrz-admin-wiki.jade-hs.de/ - **HRZ-Admin-Wiki**

Permanent link:
https://hrz-admin-wiki.jade-hs.de/en/tp/email/security/start

Last update: **2025/07/02 11:45**