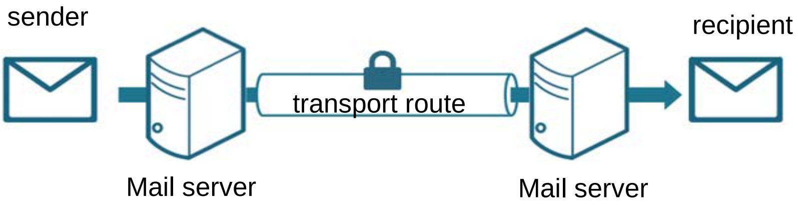
Data protection in e-mail traffic – encryption at FAIR Audit

FAIR Audit supports the following encryption techniques:

1. Transport Encryption – TLS (Transport Layer Security)

By default, FAIR Audit transmits messages via TLS – in this case the transport route between the mail servers is encrypted at the time of e-mail transmission.

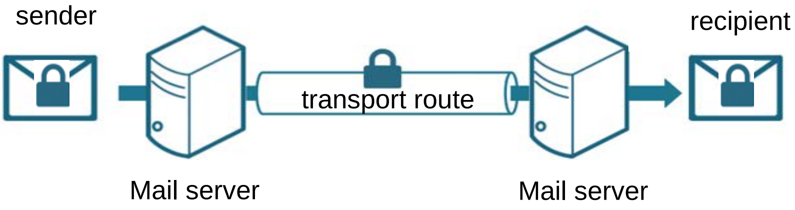


It is required that sender and recipient offer TLS encryption, otherwise the e-mail is sent using an unsecured connection.

When using mail programs such as Outlook, you may first have to activate TLS with your mail server – you may need to contact your administrator. Mail programs such as GMX automatically encrypt the transport route when retrieved via the browser or an app.

2. End-to-End Encryption – S/MIME

In this process, the contents of an e-mail are encrypted against unauthorized access. The sender and recipient must have digital keys. At the same time, S/MIME digitally signs e-mails to verify the legitimate sender of a message as such.



FAIR Audit uses digital keys issued by the trusted service provider SwissSign.

3. There are the following possibilities:

- **You also use end-to-end encryption:**

  Each e-mail we send contains verified digital keys. Save the key of each sender of our office from the signature certificate once and also send a signed email with your key. From this point onwards, all mail traffic between you and the respective contact at FAIR Audit is securely encrypted.

- **You do not use end-to-end encryption:**

  In this case, the encryption of the transport route should be done via TLS (see 1.). If this procedure is also not activated, the e-mail traffic with FAIR Audit is unencrypted.

Please feel free to ask any questions you may have.

FAIR Audit
Geries Harder Stubley PartG mbB
Wirtschaftsprüfungsgesellschaft

As of July 2018