

Sicherheit

Zur Erhöhung der Sicherheit im E-Mail Bereich bieten sich digitale, elektronische E-Mail-Signaturen und die Verschlüsselung von E-Mails an.

Um diese nutzen zu können wird ein digitales Nutzerzertifikat benötigt. Bei der Erstellung wird ein digitales Schlüsselpaar erzeugt, welches durch eine Zertifizierungsstelle bestätigt wird. Dieses Schlüsselpaar besteht aus 2 Teilen, dem privaten und dem öffentlichen Schlüssel:

- Privater Schlüssel: Dieser ist passwortgeschützt und verbleibt immer im Besitz des Benutzers
- Öffentlicher Schlüssel: Dieser wird vom Kommunikationspartner benötigt und muss diesem in irgendeiner Weise bekannt gemacht werden.

Signieren

Prinzip: Mit Hilfe Ihres privaten Schlüssels signieren Sie Ihre E-Mail. Der Kommunikationspartner kann dann mit Hilfe Ihres öffentlichen Schlüssels prüfen, ob / dass Daten unverändert vorliegen.

Verschlüsseln

Prinzip: Mit Hilfe des öffentlichen Schlüssels des Kommunikationspartners verschlüsseln Sie Ihre E-Mail. Der Kommunikationspartner kann mit Hilfe seines privaten Schlüssels die E-Mail dann entschlüsseln. Sie müssen also zur Verschlüsselung zunächst den öffentlichen Schlüssel des Kommunikationspartners besitzen.

Voraussetzungen

Eine grundsätzliche Voraussetzung zur Nutzung ist die korrekte Einbindung der [Zertifizierungsstellen](#) in ihr verwendetes Betriebssystem und ein gültiges digitales [Nutzerzertifikat](#). Konfigurieren Sie dann die entsprechende Anwendungssoftware:

Seiten in diesem Namensraum:

A

- [Apple iOS/iPadOS - Mail](#)
- [Apple macOS - Mail](#)

G

- [Google Android](#)

L

- [Linux - Evolution](#)

M

- [Microsoft Outlook 2016/2019](#)

M (Fortsetzung)

- [Microsoft Outlook für Mac 2019](#)
- [Mozilla Thunderbird](#)

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

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

Last update: **2024/03/04 14:26**

