Microsoft Outlook 2016/2019

Prerequisites

- Correct setup of the e-mail client Microsoft Outlook 2016/2019
- Correct integration of the Certification authorities into the operating system.
- **Valid digital User certificate** integrated into the operating system.

Configuration

Step 1: Microsoft Outlook needs to know which digital user certificate to use and how:

- Start Microsoft Outlook
- File → Options → Trust Center → Trust Center Settings... → E-mail Security
- Section “Encrypted e-mail messages”
    - Add digital signature to outgoing messages: activated
    - Send signed messages as plain text: activated
    - Select the button “Settings...”
        - Security setting name: DFN-PKI (<your e-mail address>).
        - Cryptography format: S/MIME
        - Default setting for this format of cryptographic messages: activated
        - Default setting for all cryptographic messages: activated
        - Certificates and algorithms
            - Signing certificate / Select... / Select your personal user certificate here.
            - Hashalgorithm: SHA256
            - Encryption certificate / Select... / Select your personal user certificate here.
            - Encryption algorithm: AES (256-bit) (keep default).
            - Add these certificates to signed messages: activated
- Confirm your entries by clicking the “OK” button several times until you are back in the main Microsoft Outlook window.

Step 2: Set up Microsoft Outlook for convenient use of digital signature and encryption:

- In Microsoft Outlook, click on “New Email” and then on the “Options” card.
- Right-click on “Sign” and select “Add to toolbar for DeepL access”.
- Right-click on “Encrypt” and select “Add to DeepL Access Toolbar”.
- Close the window again

You have now completed all the necessary steps to sign each email. Provided you have the public key of your communication partner, you can also encrypt any e-mail.

Use

Sign

- Click on “New e-mail” in Microsoft Outlook and compose it.
- Before sending, check at the top of DeepL access that the message is digitally signed. The button “Digitally sign message” at the top of DeepL access is activated by default.
- As soon as you click on “Send”, the e-mail is digitally signed and then 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. Add the communication partner to your Microsoft Outlook contacts so that his or her public key is stored in your system.

- Click on “New e-mail” in Microsoft Outlook and compose it.
- Before sending, click on “Encrypt” at the top of DeepL access.
- As soon as you click on “Send”, the e-mail is encrypted and then sent.
- The communication partner will see the lock symbol as a sign of an encrypted e-mail.