ANLEITUNG

EINRICHTUNG EINER DIGITALEN SIGNATUR AM BEISPIEL VON OUTLOOK

ALLGEMEINES

Wofür benötige ich eine digitale Signatur?

Bei E-Mails besteht grundsätzlich die Gefahr, dass Unbefugte den Inhalt und/oder die Absenderadresse manipulieren können. Damit könnten kriminelle Hacker in Ihrem Namen schadhafte Inhalte versenden. Nähere Informationen zum sogenannten Phishing bietet die Stabstelle IT-Sicherheit der RUB: https://www.itsb.ruhr-uni-bochum.de/themen/email_betrug.html.

Sie können dies verhindern, indem Sie dem/der Empfänger*in eindeutig und fälschungssicher nachweisen, dass die verschickte E-Mail tatsächlich von Ihnen stammt, indem Sie eine digitale Signatur benutzen. Technisch wird dies über ein persönliches Nutzerzertifikat realisiert, das IT.SERVICES allen Mitgliedern und Angehörigen der RUB zur Verfügung stellt.

Voraussetzung für die digitale Signatur

Voraussetzung für die Einrichtung einer digitalen Signatur ist ein persönliches Nutzerzertifikat, das Sie bei IT.SERVICES beantragen können. Informationen dazu finden Sie auf unserer Webseite.

HINWEIS

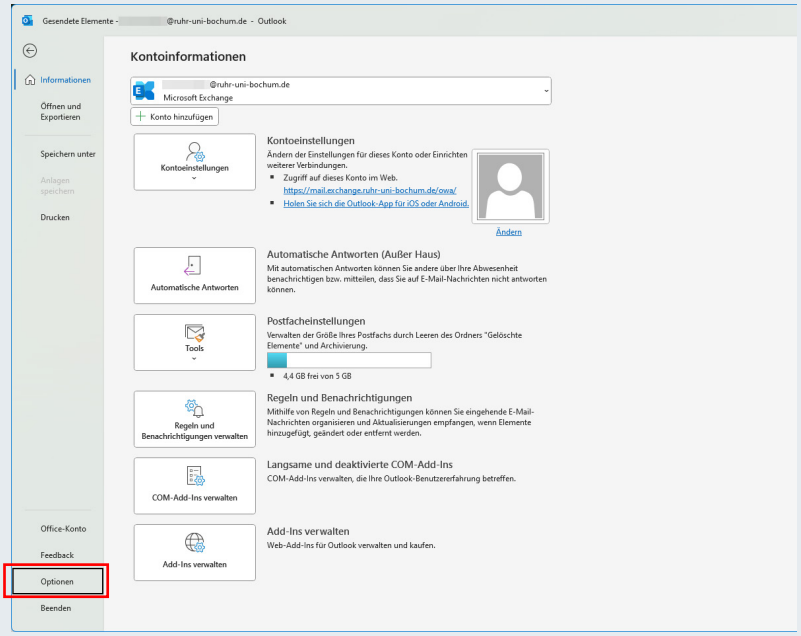
Wenn es Probleme mit der Authentifizierung oder Überprüfung der Signatur gibt, prüfen Sie, ob alle Zertifikate der Vertrauenskette installiert sind. Diese Zertifikatskette finden Sie hier.

Bei Fragen können Sie unsere Registrierungsstelle per E-Mail an pki@ruhr-uni-bochum.de oder telefonisch im Servicecenter unter 0234/32-24025 erreichen.

MANUELLER IMPORT

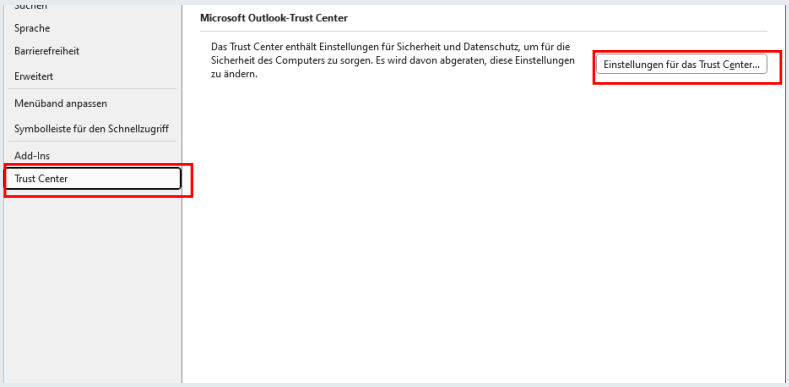
Schritt 1

Starten Sie Outlook. Gehen Sie in der oberen Menüleiste auf "Datei" und dann auf "Optionen".



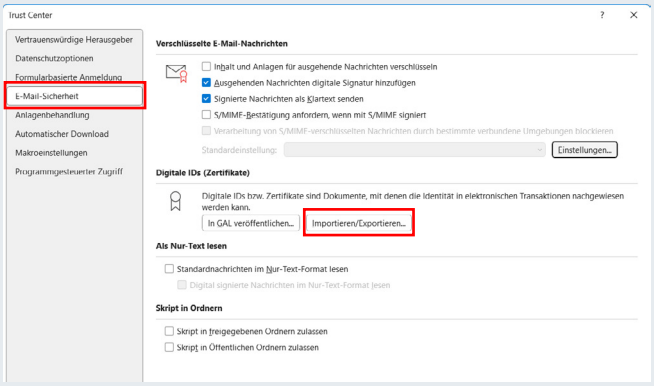
Schritt 2

Klicken Sie nun auf "Trust Center" und anschließend auf "Einstellungen für das Trust Center".



Schritt 3

Klicken Sie nun auf "E-Mail-Sicherheit" in der linken Menüleiste und anschließend auf "Importieren/Exportieren...".

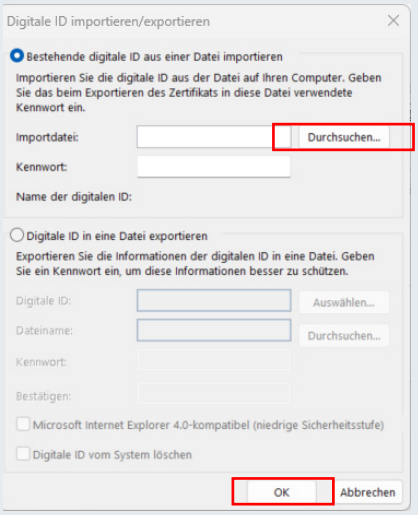


Schritt 4

Fügen Sie nun über "Durchsuchen" Ihr Nutzerzertifikat als Importdatei hinzu.

Geben Sie in das Eingabefeld „Kennwort“ das Passwort ein, welches Sie bei der Beantragung (im Zertifikatsmanager) festgelegt haben.

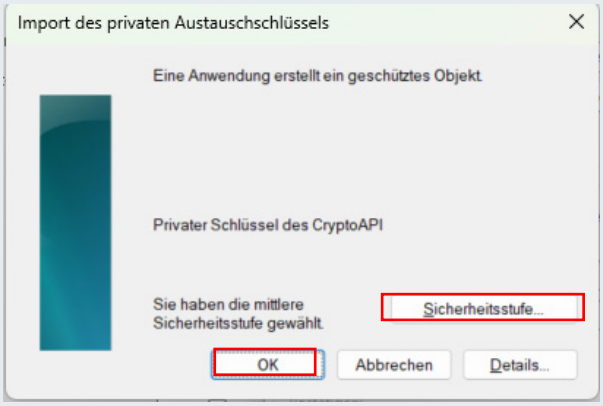
Klicken Sie „OK“ um das Zertifikat zu Importieren.



Schritt 5

Nun öffnet sich ein Fenster mit dem Titel „Import des privaten Austauschschlüssels“.

Wählen Sie hier die gewünschte Sicherheitsstufe aus oder belassen Sie diese auf „mittlere Sicherheitsstufe“ und bestätigen Sie mit „OK“.

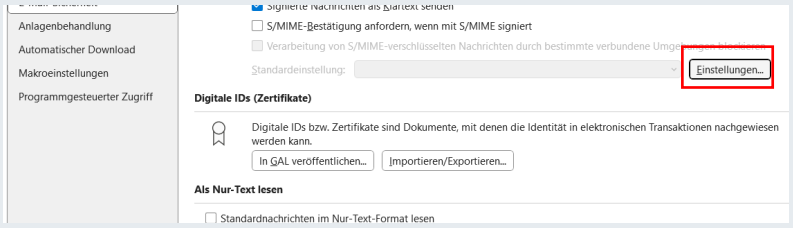


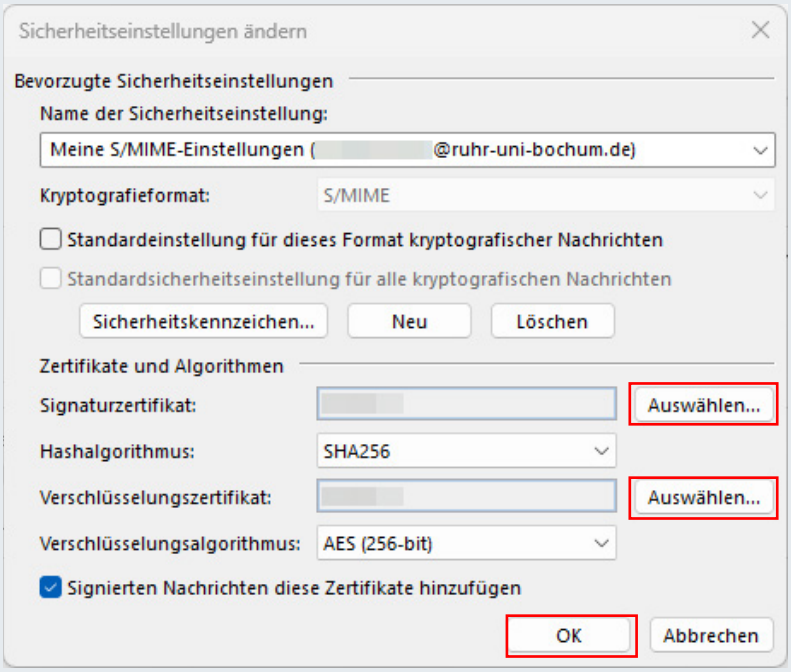
Schritt 6

Klicken Sie nun auf die Schaltfläche „Einstellungen...“.

Anschließend klicken Sie auf „Auswählen...“ neben „Signaturzertifikat“ und wählen hier Ihr zuletzt importiertes Zertifikat aus. Gehen Sie genauso für „Verschlüsselungszertifikat“ vor.

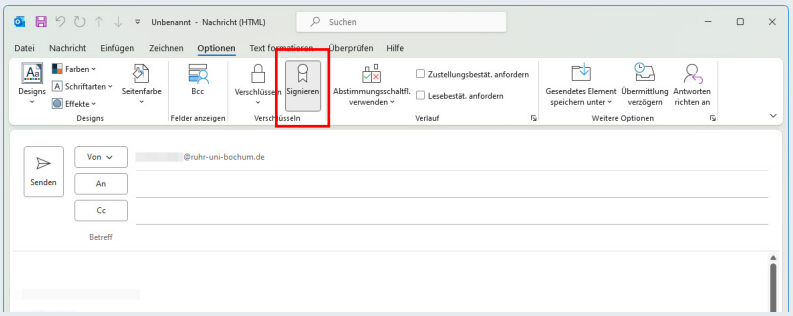
Wählen Sie im aktuellen Einstellungsfenster dann als Hashalgorithmus „SHA256“ und als Verschlüsselungsalgorithmus „AES (256-bit)“. Bestätigen Sie zuletzt alle Einstellungen mit „OK“.





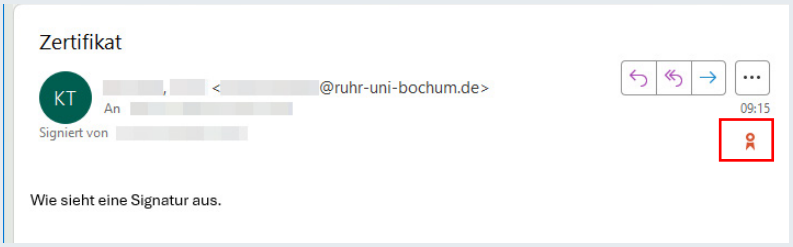
Schritt 7

Um zu prüfen, ob Ihre E-Mails signiert werden, erstellen Sie eine neue E-Mail und überprüfen, ob unter „Optionen“ das Feld „Signieren“ aktiv ist. Möchten Sie eine E-Mail unsigniert versenden, können Sie das Feld „Signieren“ manuell deaktivieren.



UMGANG MIT SIGNIERTEN E-MAILS

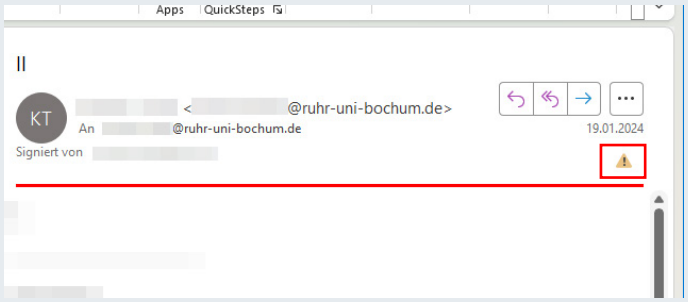
Sie können Signaturen von empfangenen E-Mails überprüfen, indem Sie auf das Schleifen-Symbol klicken und sich damit weitere Informationen zum Zertifikat anzeigen lassen.



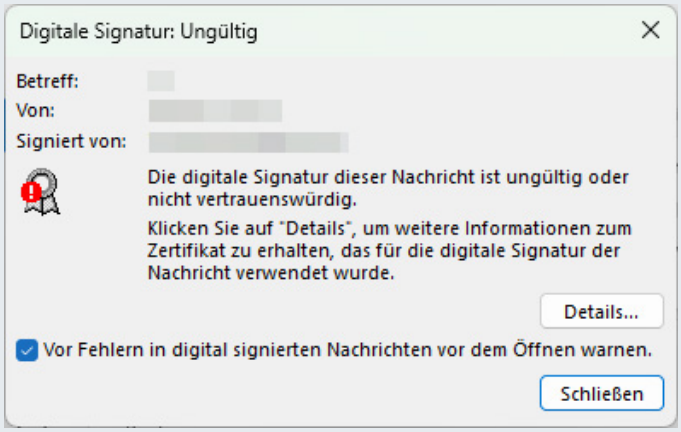
Unter „Details“ erhalten Sie weitere Informationen über das Zertifikat. Wir empfehlen, das Häkchen bei „Vor Fehlern [...] warnen“ zu setzen. E-Mails mit ungültigen Zertifikaten werden dann nicht direkt geöffnet (siehe nächster Abschnitt „Ungültige Signatur“).

UNGÜLTIGE SIGNATUREN

Ungültige Signaturen erkennen Sie daran, dass in der E-Mail nicht das Schleifensymbol, sondern ein Warndreieck angezeigt wird. Haben Sie, wie auf der vorherigen Seite empfohlen, das Häkchen bei „Vor Fehlern…“ gesetzt, werden diese E-Mails nicht direkt geöffnet, sondern zunächst die Informationen zur Signatur. Dies schützt Sie davor E-Mails mit schadhaftem Inhalt (Drive-by-Attacken) zu öffnen.



Prüfen Sie den Fehler genau und klicken erst dann auf „Nachricht anzeigen“ oder öffnen Sie die E-Mail gegebenenfalls erst nach Rücksprache mit dem Absender. Möglicherweise ist das Zertifikat lediglich abgelaufen.



KONTAKT & HILFE:

Bei Fragen und Problemen wenden Sie sich an unseren Helpdesk unter: its-helpdesk@ruhr-uni-bochum.de