

SHORTGUIDE

EINRICHTUNG EINER DIGITALEN SIGNATUR AM BEISPIEL VON OUTLOOK

FÜR MITGLIEDER UND ANGEHÖRIGE DER RUB

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: <http://www.itsb.ruhr-uni-bochum.de/phishing.html>.

Sie können dies verhindern, indem Sie dem Empfänger 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 und im Shortguide „Beantragung eines persönlichen Nutzerzertifikats“.

Hinweis

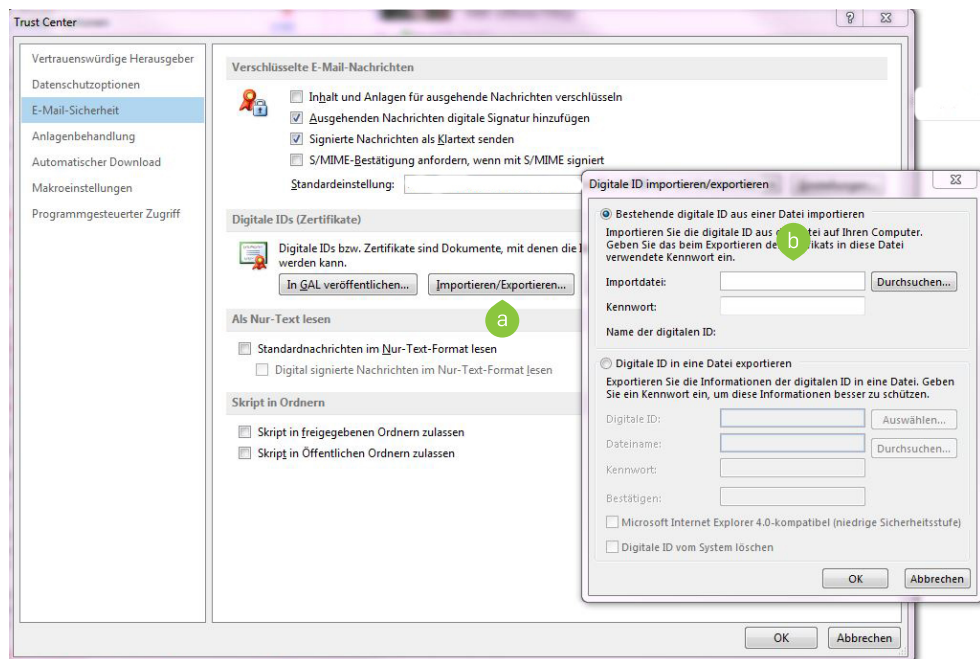
Wenn es Probleme mit der Authentifizierung oder Überprüfung der Signatur gibt, prüfen Sie, ob alle Zertifikate der Vertrauenskette installiert sind. Diese Zertifikatskette finden Sie im DFN-PKI-Portal.

Bei Fragen können Sie Kontakt mit unserer Registrierungsstelle aufnehmen: per E-Mail pki@ruhr-uni-bochum.de oder telefonisch im Servicecenter unter 0234/32-24025.

EINRICHTUNG EINER DIGITALEN SIGNATUR IN OUTLOOK

Manueller Import

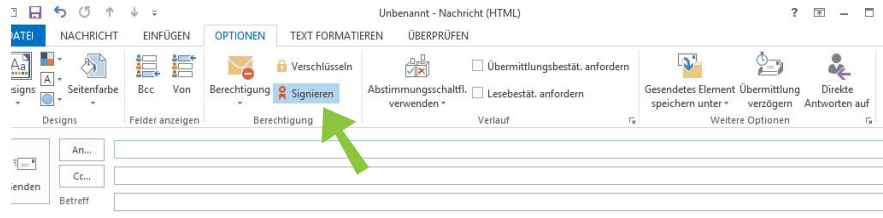
1. Wählen Sie in Outlook in der oberen Menüleiste „Datei“ aus und öffnen Sie „Optionen“.
2. Öffnen Sie unter „Trust Center“ die „Einstellung für das Trust Center...“.
3. Im linken Menü finden Sie „E-Mail-Sicherheit“.
4. Wählen Sie die Importieren-Funktion aus (a) und fügen Sie Ihr Nutzerzertifikat als Importdatei hinzu (b). Das Kennwort haben Sie beim Exportieren des Zertifikats aus dem Browser, mit dem Sie das Zertifikat beantragt haben, festgelegt und müssen es hier verwenden.
5. Bestätigen Sie Ihre Eingaben mit „OK“, um fortzufahren.



Geschafft!

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.

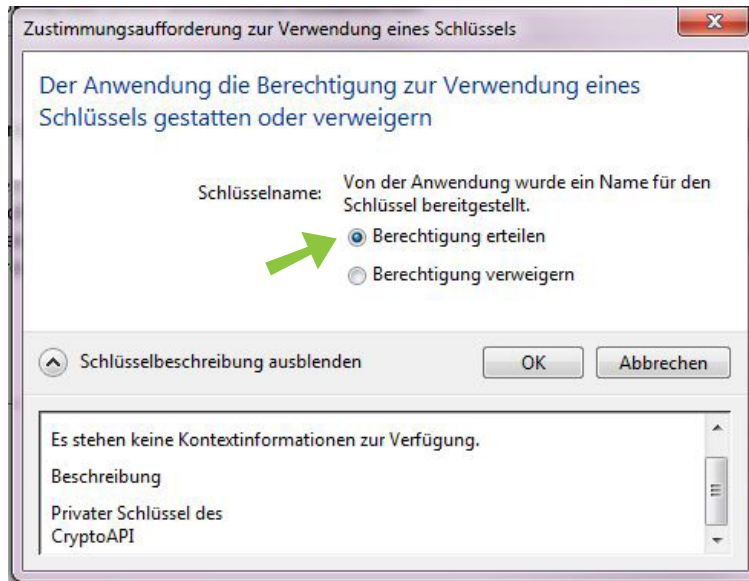
Möchten Sie eine E-Mail unsigniert versenden, können Sie das Feld „Signieren“ manuell deaktivieren.



Zustimmung zur Verwendung des Schlüssels

Eventuell fragt Outlook Sie bei der ersten E-Mail am Tag, ob Sie der Anwendung die Berechtigung zur Verwendung eines Schlüssels gestatten oder verweigern möchten.

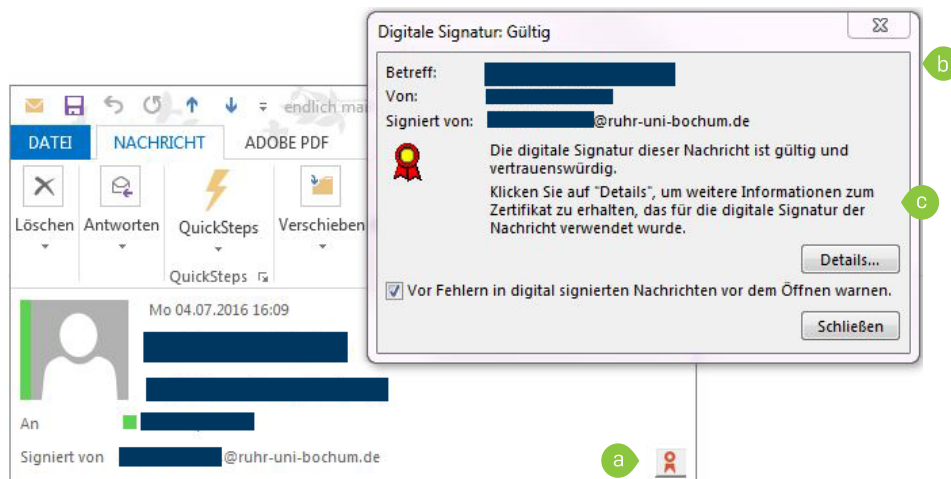
Klicken Sie „Berechtigung erteilen“ an und bestätigen mit „OK“.



Umgang mit signierten E-Mails

Sie können Signaturen von empfangenen E-Mails überprüfen, indem Sie auf das Schleifen-Symbol klicken (a) und sich damit weitere Informationen zum Zertifikat anzeigen lassen (b). Unter „Details“ (c) erhalten Sie weitere Informationen über das Zertifikat.

Wir empfehlen, das Häkchen bei „Vor Fehlern...“ zu setzen. E-Mails mit ungültigen Zertifikaten werden dann nicht direkt geöffnet (siehe nächste Box „Ungültige Signatur“).

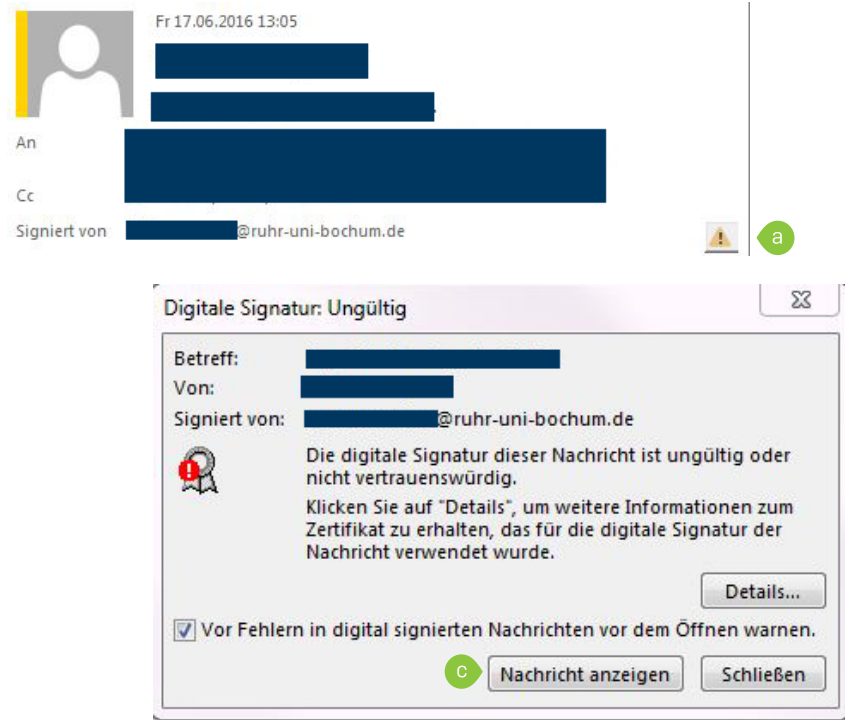


Ungültige Signatur

Ungültige Signaturen erkennen Sie daran, dass in der E-Mail nicht das Schleifensymbol, sondern ein Warndreieck (a) 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 (b). 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“ (c) oder öffnen Sie die E-Mail gegebenenfalls erst nach Rücksprache mit dem Absender.

Möglicherweise ist das Zertifikat lediglich abgelaufen.



Bei Fragen & Problemen

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