

Zertifikatsimport S/MIME Outlook

Erfolgreiches Signieren und Verschlüsseln von E-Mails mit dem Exchange-E-Mail-Konto der TU Braunschweig.

- [Voraussetzungen](#)
- [Import des Nutzerzertifikats](#)
- [Import zusätzlicher Zertifikate für Funktionsaccounts](#)
- [Verwendung](#)
- [Erkennen von korrekt signierten Nachrichten](#)
- [Wichtige Hinweise](#)

Voraussetzungen

Sie benötigen zum Signieren und oder Verschlüsseln von E-Mails Ihres Kontos an der TU Braunschweig ein gültiges Nutzerzertifikat, wie es nach folgender Anleitung beantragt werden kann: [Nutzerzertifikate](#). Bitte beachten Sie die [wichtigen Hinweise](#).

Import des Nutzerzertifikats

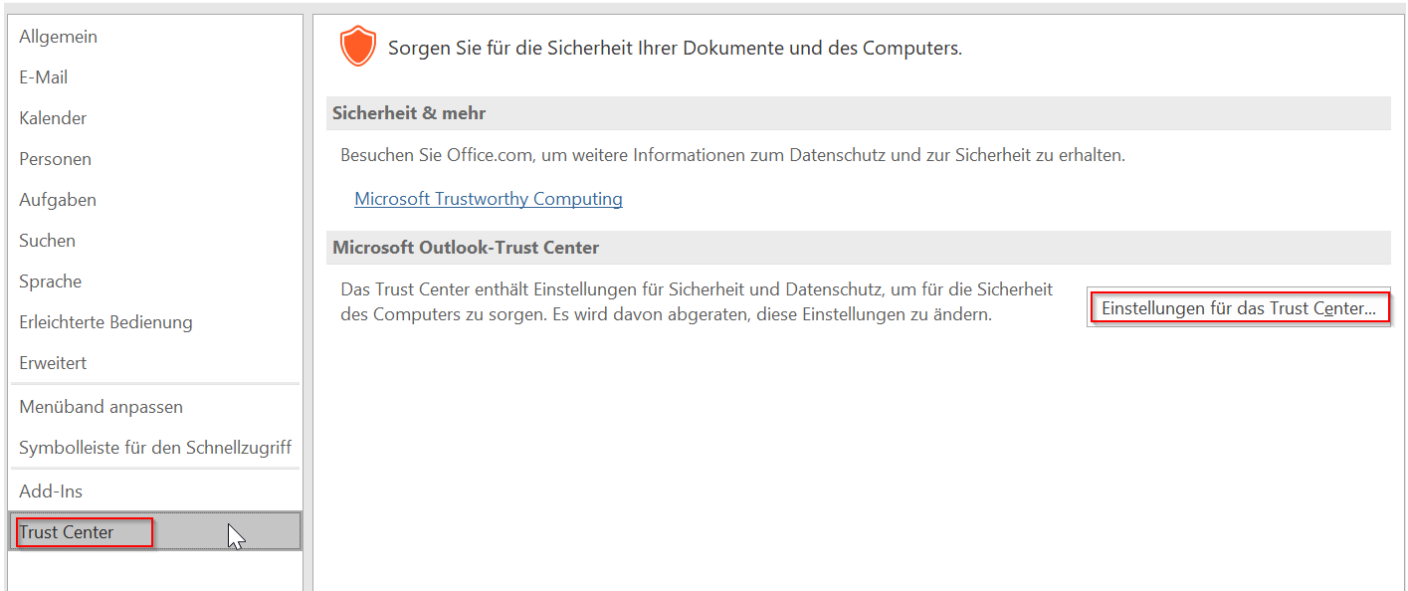
Das beantragte Nutzerzertifikat haben Sie nach der Beantragung direkt heruntergeladen.

Die erhaltene **pkcs#12 (.p12) Zertifikatsdatei** muss entpackt und im Trust-Center von Outlook eingebunden werden.

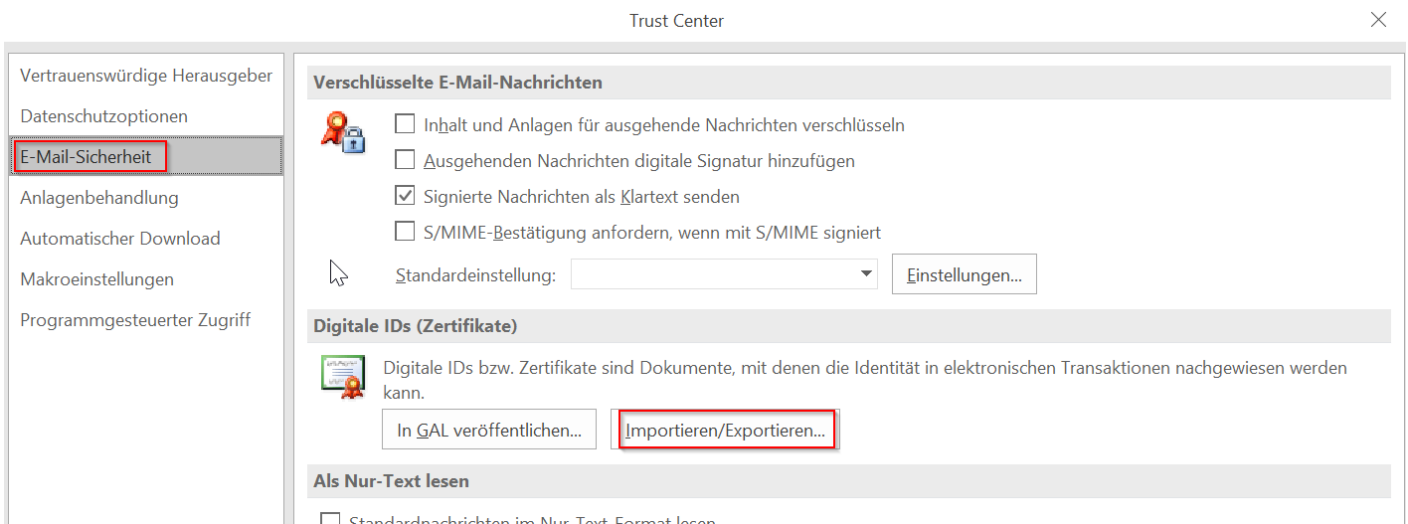
Zum Hinzufügen des Nutzerzertifikats öffnen Sie die Outlook **[Optionen]** (Datei < Optionen).

The screenshot displays the Outlook interface for account management. On the left, a blue sidebar contains navigation options: 'Informationen', 'Öffnen und Exportieren', 'Speichern unter', 'Anlagen speichern', 'Drucken', 'Office-Konto', 'Optionen' (highlighted with a red box), and 'Beenden'. The main area is titled 'Kontoinformationen' and shows the account '@tu-braunschweig.de' on Microsoft Exchange. Below this, there is a '+ Konto hinzufügen' button. Two main sections are visible: 'Kontoeinstellungen' (Account Settings) with a sub-description 'Ändern der Einstellungen für dieses Konto oder Einrichten weiterer Verbindungen.' and a list of options including 'Zugriff auf dieses Konto im Internet' (with a link to <https://mail.tu-braunschweig.de/owa/>) and 'Die Outlook-App für iPhone, iPad, Android oder Windows 10 Mobile herunterladen.'; and 'Automatische Antworten (Außer Haus)' (Automatic Replies) with a sub-description 'Mit automatischen Antworten können Sie andere über Ihre Abwesenheit benachrichtigen bzw. mitteilen, dass Sie auf E-Mail-Nachrichten nicht antworten können.' A profile picture placeholder is also present with an 'Ändern' (Change) link.

Wählen Sie in den Optionen unter dem Reiter **[Trust Center]** die **[Einstellungen für das Trust Center]** aus.



Wählen Sie die Kategorie **[E-Mail-Sicherheit]** aus und klicken Sie unter dem Aspekt Digitale IDs auf **[Importieren/Exportieren]**.



In dem sich geöffneten Fenster müssen Sie nun die Zertifikatsdatei auswählen. Klicken Sie auf **[Durchsuchen]**.

Digitale ID importieren/exportieren ×

Bestehende digitale ID aus einer Datei importieren

Importieren Sie die digitale ID aus der Datei auf Ihren Computer. Geben Sie das beim Exportieren des Zertifikats in diese Datei verwendete Kennwort ein.

Importdatei:

Kennwort:

Name der digitalen ID:

Digitale ID in eine Datei exportieren

Exportieren Sie die Informationen der digitalen ID in eine Datei. Geben Sie ein Kennwort ein, um diese Informationen besser zu schützen.

Digitale ID:

Dateiname:

Kennwort:

Bestätigen:

Microsoft Internet Explorer 4.0-kompatibel (niedrige Sicherheitsstufe)

Digitale ID vom System löschen

Wählen Sie die passende Datei aus und geben Sie das Transportpasswort ein, welches Sie beim Beantragen des Nutzerzertifikates (s.o.) im BDD eingegeben haben.

Bestehende digitale ID aus einer Datei importieren

Importieren Sie die digitale ID aus der Datei auf Ihren Computer. Geben Sie das beim Exportieren des Zertifikats in diese Datei verwendete Kennwort ein.

Importdatei:

Kennwort:

Name der digitalen ID:

Digitale ID in eine Datei exportieren

Exportieren Sie die Informationen der digitalen ID in eine Datei. Geben Sie ein Kennwort ein, um diese Informationen besser zu schützen.

Digitale ID:

Dateiname:

Kennwort:

Bestätigen:

Microsoft Internet Explorer 4.0-kompatibel (niedrige Sicherheitsstufe)

Digitale ID vom System löschen

Klicken Sie nun auf **[OK]**. Anschließend erscheint das Modul zum Import und Verwaltung des Zertifikats und des enthaltenen Schlüssels. Klicken Sie auf **[Sicherheitsstufe]**.

Import des privaten Austauschschlüssels



Eine Anwendung erstellt ein geschütztes Objekt.



Privater Schlüssel des CryptoAPI

Sie haben die mittlere
Sicherheitsstufe gewählt.

Sicherheitsstufe...

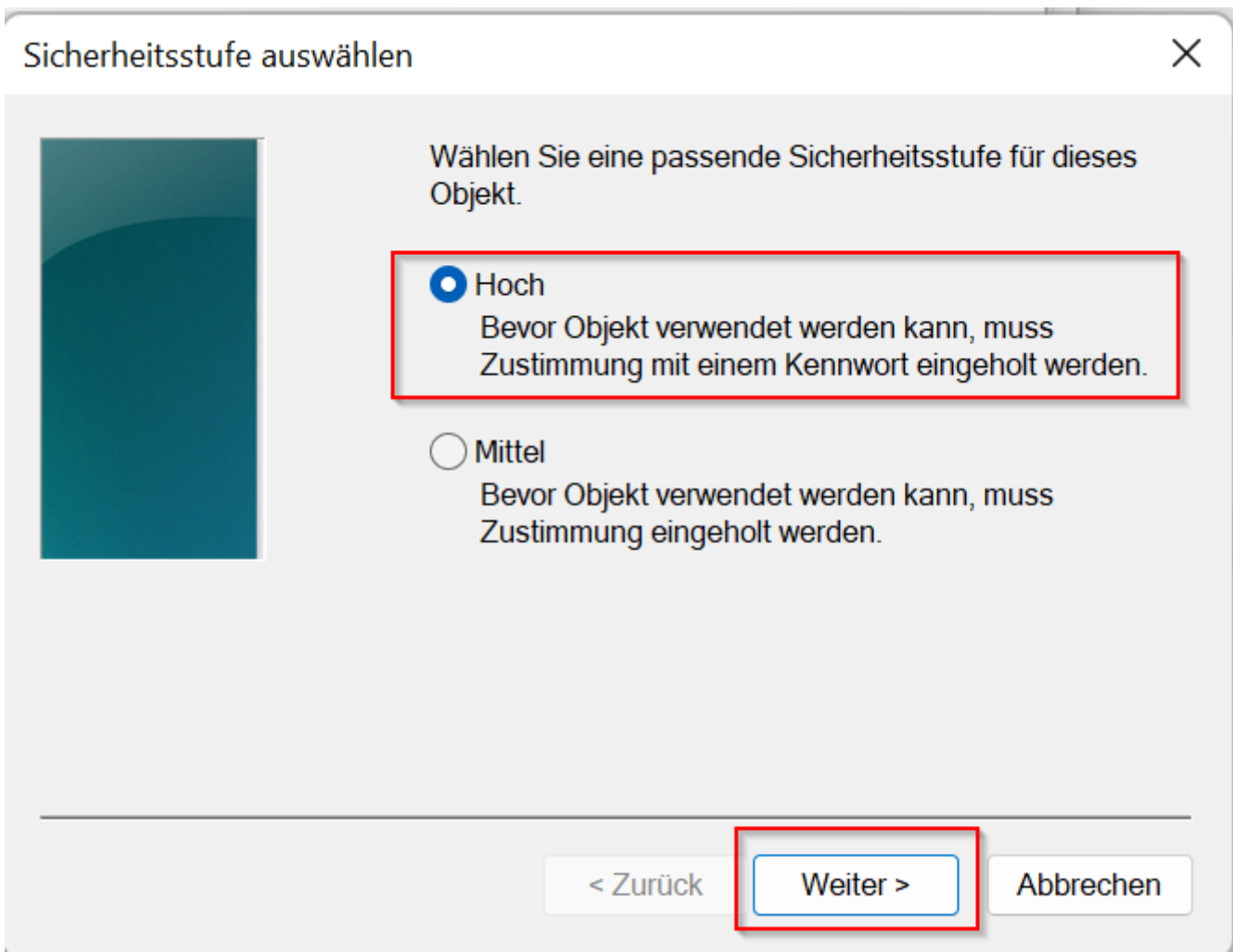
OK

Abbrechen

Details...

Der Autor empfiehlt die Sicherheitsstufe Hoch, diese hat zur Folge, dass beim Signieren oder Verschlüsseln der Zugriff auf das Zertifikat und den enthaltenen Schlüssel nur über eine Passwortabfrage möglich ist. Wählen Sie die für Ihre Sicherheit notwendige Sicherheitsstufe aus.

Nach Klick auf **[Weiter]** und Abschluss des Imports können nun die eigentlichen Einstellungen zur Verwendung des Nutzerzertifikats zum Signieren und Verschlüsseln vorgenommen werden; Punkte 1 bis 3 ist das von uns empfohlene Alltagsverhalten.



In den Einstellungen müssen anschließend noch folgende Parameter angepasst werden:

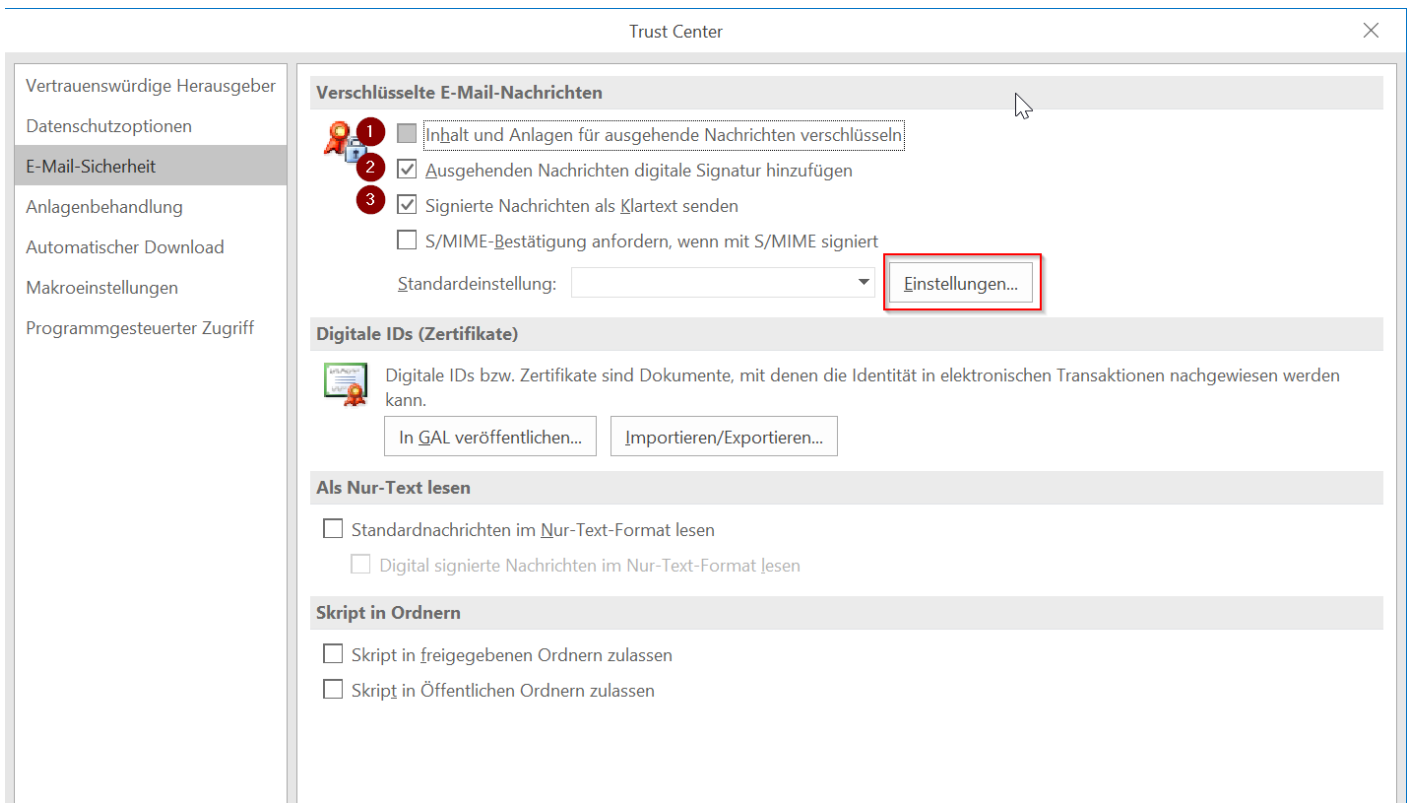
(1) Es darf bzw. sollte **kein** Haken bei **[Inhalt und Anlagen für ausgehende Nachrichten verschlüsseln]** gesetzt werden.

Hintergrund: es handelt sich primär um Signaturzertifikate.

(2) Es muss ein Haken bei **[Ausgehenden Nachrichten digitale Signatur hinzufügen]** gesetzt werden.

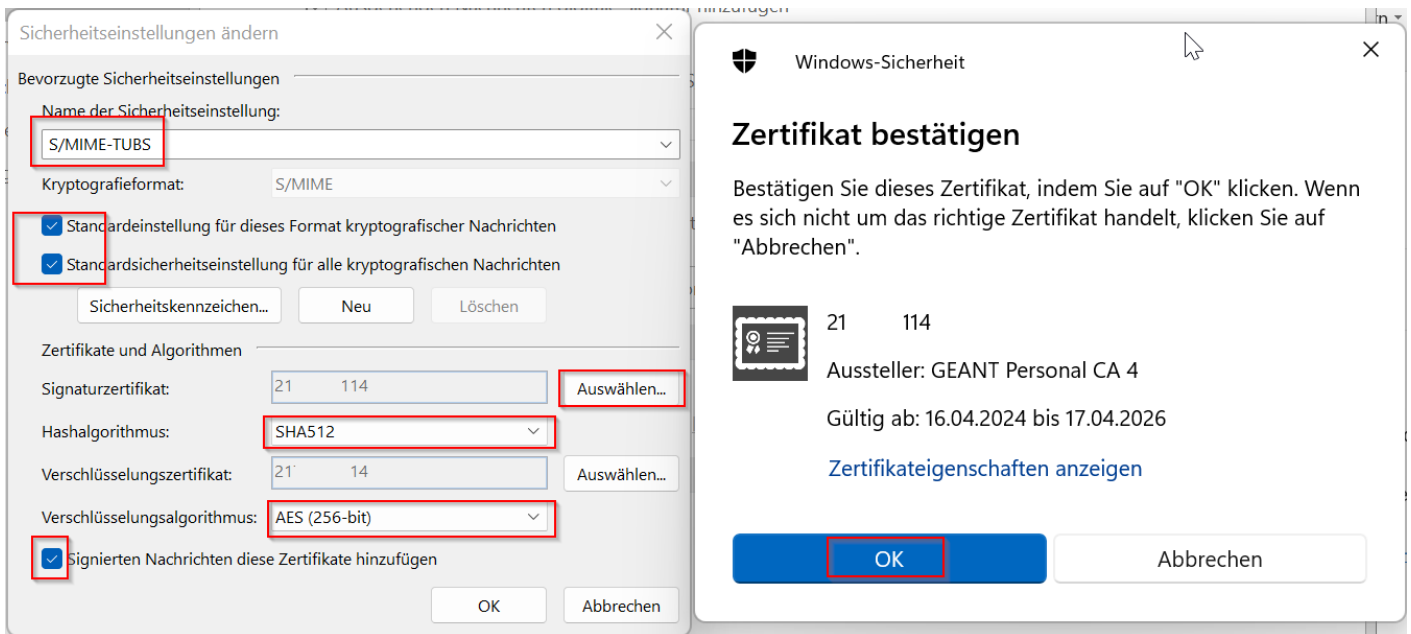
(3) Es muss ein Haken bei **[Signierte Nachricht als Klartext senden]** gesetzt werden.

Klicken Sie anschließend auf **[Einstellungen]**.



Vergeben Sie in dem neuen Fenster einen Namen für diese Sicherheitseinstellung (wenn noch nicht automatisch erzeugt). Setzen Sie die entsprechenden Häkchen wie im folgenden Bild und wählen Sie das Signaturzertifikat. Bestätigen Sie mit **[OK]**.

Wichtig: Ändern Sie nach Hinzufügen den Hashalgorithmus von SHA-1 auf mindestens SHA-256 und vergewissern Sie sich bitte, dass der Verschlüsselungsalgorithmus auf AES 256-bit eingestellt ist.



Wurde nun mit **[OK]** bestätigt, wird nun im Trust-Center das aktive S/MIME Profil angezeigt.

Sie können nun das Trust-Center und die Einstellungen schließen.

Verschlüsselte E-Mail-Nachrichten



- Inhalt und Anlagen für ausgehende Nachrichten verschlüsseln
- Ausgehenden Nachrichten digitale Signatur hinzufügen
- Signierte Nachrichten als Klartext senden
- S/MIME-Bestätigung anfordern, wenn mit S/MIME signiert

Standardeinstellung: S/MIME-TUBS

Einstellungen...

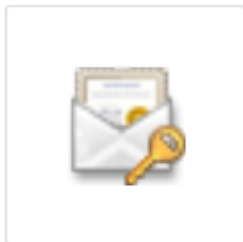
Import zusätzlicher Zertifikate für Funktionsaccounts

Nach Beantragung eines Zertifikats für einen Ihnen zugeordneten Funktionsaccount im BDD können Sie ähnlich dem Import der personenbezogenen Zertifikate verfahren.

Sie erhalten das Zertifikat als komprimierte .p12:



Entpacken als .p12 in einen Ordner:



fa000 @tu-bs.
de.p12

Anschließend in Outlook unter Datei -> Optionen

←

Informationen

Öffnen und Exportieren

Speichern unter

Anlagen speichern

Drucken

Office-Konto

Optionen

Beenden

Kontoinformationen

@tu-braunschweig.de

Microsoft Exchange

Konto hinzufügen

Kontoeinstellungen

Ändern der Einstellungen für dieses Konto oder Einrichten weiterer Verbindungen.

- Zugriff auf dieses Konto im Internet. <https://mail.tu-braunschweig.de/owa/>

Ändern

Automatische Antworten (Außer Haus)

Mit automatischen Antworten können Sie andere über Ihre Abwesenheit benachrichtigen bzw. mitteilen, dass Sie auf E-Mail-Nachrichten nicht antworten können.

Postfach aufräumen

Verwalten der Größe Ihres Postfachs durch Leeren des Ordners "Gelöschte Elemente" und Archivierung.

7,28 GB frei von 10 GB

Regeln und Benachrichtigungen

Mithilfe von Regeln und Benachrichtigungen können Sie eingehende E-Mail-Nachrichten organisieren und Aktualisierungen empfangen, wenn Elemente hinzugefügt, geändert oder entfernt werden.

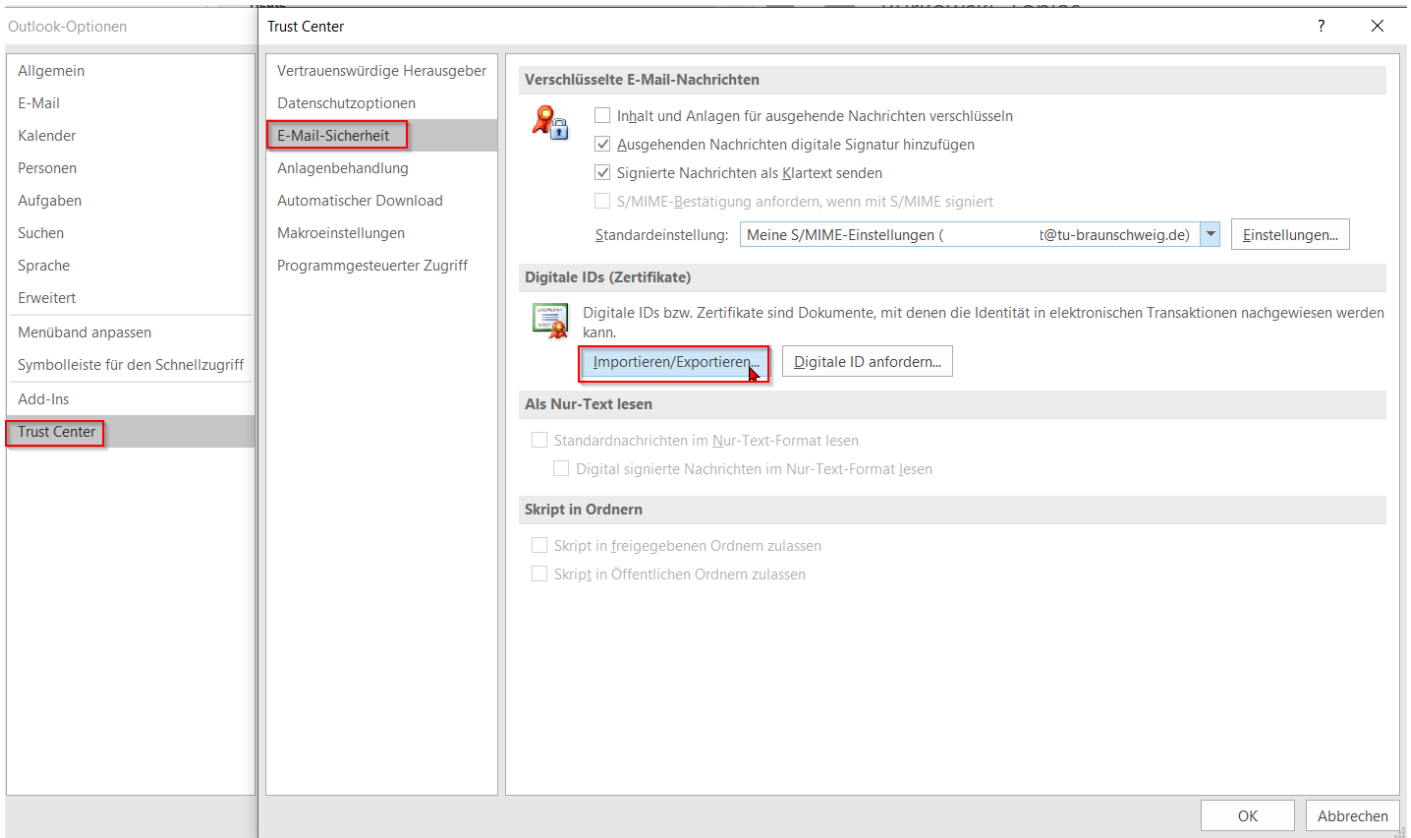
Langsame und deaktivierte COM-Add-Ins

COM-Add-Ins verwalten, die Ihre Outlook-Benutzererfahrung betreffen.

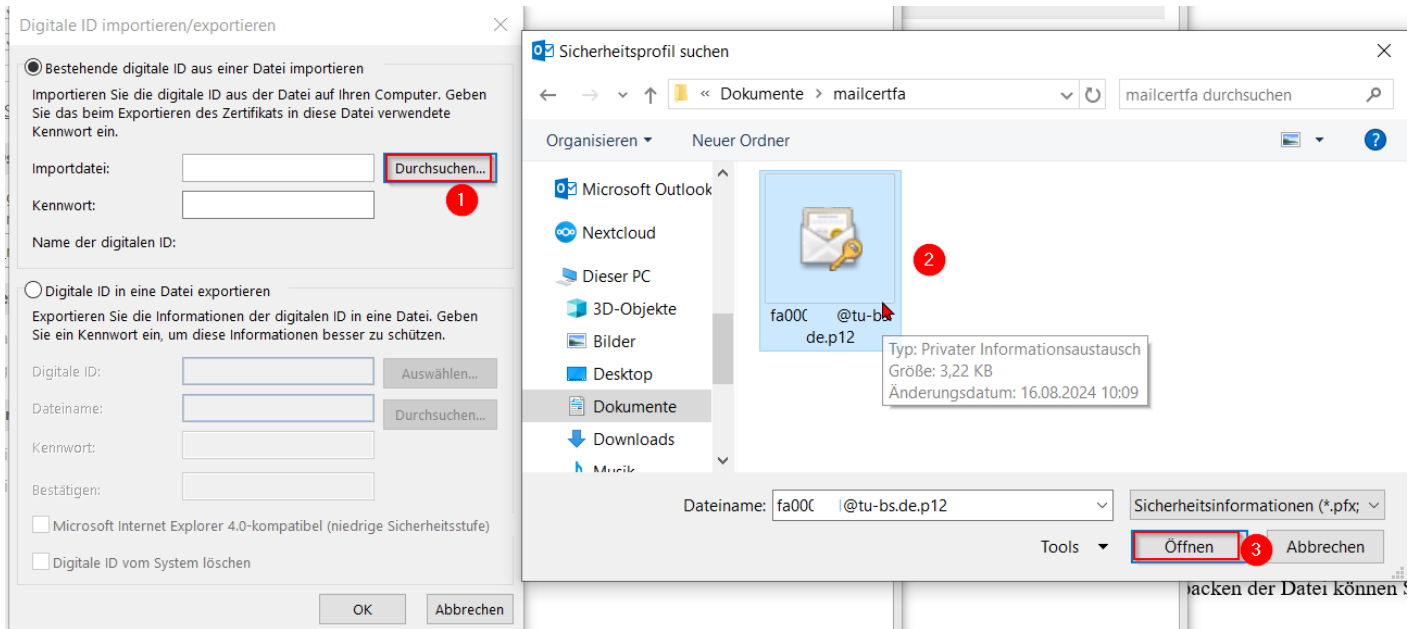
Add-Ins verwalten

Web-Add-Ins für Outlook verwalten und kaufen.

Im Trust Center unter E-Mail-Sicherheit das zusätzliche Zertifikat importieren:



Bitte dazu die Importdatei mit Klick auf Durchsuchen (1) im entsprechenden Ordner auswählen (2) und öffnen (3).



Anschließend das Transportkennwort eingeben (1) und mit (2) bestätigen.

Digitale ID importieren/exportieren



Bestehende digitale ID aus einer Datei importieren

Importieren Sie die digitale ID aus der Datei auf Ihren Computer. Geben Sie das beim Exportieren des Zertifikats in diese Datei verwendete Kennwort ein.

Importdatei:

Kennwort: **1**

Name der digitalen ID:

Digitale ID in eine Datei exportieren

Exportieren Sie die Informationen der digitalen ID in eine Datei. Geben Sie ein Kennwort ein, um diese Informationen besser zu schützen.

Digitale ID:

Dateiname:

Kennwort:

Bestätigen:

Microsoft Internet Explorer 4.0-kompatibel (niedrige Sicherheitsstufe)

Digitale ID vom System löschen

2

In diesem Fenster kann die Sicherheitsstufe (z.B. Passwort für den Zugriff auf dieses Zertifikat) wieder entsprechend angepasst werden. Anschließend mit OK bestätigen:

Import des privaten Austauschschlüssels



Eine Anwendung erstellt ein geschütztes Objekt.

Privater Schlüssel des CryptoAPI

Sie haben die mittlere Sicherheitsstufe gewählt

Sicherheitsstufe...

OK

Abbrechen

Details...

Damit ist das Zertifikat importiert, nun muss es noch für die Verwendung konfiguriert werden. Dazu bitte im Trust Center (1) unter E-Mail-Sicherheit (2) mit Klick auf Einstellungen (3) ein Neu(4)es Profil anlegen:

The screenshot shows the Outlook Trust Center interface. On the left, the 'Trust Center' option is highlighted with a red circle and the number 1. In the main area, 'E-Mail-Sicherheit' is selected in the left-hand menu with a red circle and the number 2. The 'Verschlüsselte E-Mail-Nachrichten' section is active, and the 'Einstellungen...' button is highlighted with a red circle and the number 3. A dialog box titled 'Sicherheitseinstellungen ändern' is open, showing the 'Name der Sicherheitseinstellung' dropdown menu with 'Meine S/MIME-Einstellungen (marius @tu-braunschweig.de)' selected. The 'Neu' button is highlighted with a red circle and the number 4. The dialog box also shows options for 'Kryptografieformat' (S/MIME), 'Standardinstellung für dieses Format kryptografischer Nachrichten' (checked), 'Standardsicherheitseinstellung für alle kryptografischen Nachrichten' (checked), and 'Zertifikate und Algorithmen' (Signature certificate: Marius, Hash algorithm: SHA512, Encryption certificate: Marius, Encryption algorithm: AES (256-bit)).

Dies öffnet folgenden Dialog, dort bitte unter (1) eine passende Beschreibung auswählen (es empfiehlt sich die dazugehörige E-Mail-Adresse) und dann mit (2) das Signaturzertifikat auswählen:

Sicherheitseinstellungen ändern ×

Bevorzugte Sicherheitseinstellungen

Name der Sicherheitseinstellung: gitz-client-@tu-braunschweig.de 1

Kryptografieformat: S/MIME

Standardeinstellung für dieses Format kryptografischer Nachrichten

Standardsicherheitseinstellung für alle kryptografischen Nachrichten

Sicherheitskennzeichen... Neu Löschen

Zertifikate und Algorithmen

Signaturzertifikat: Auswählen... 2

Hashalgorithmus:

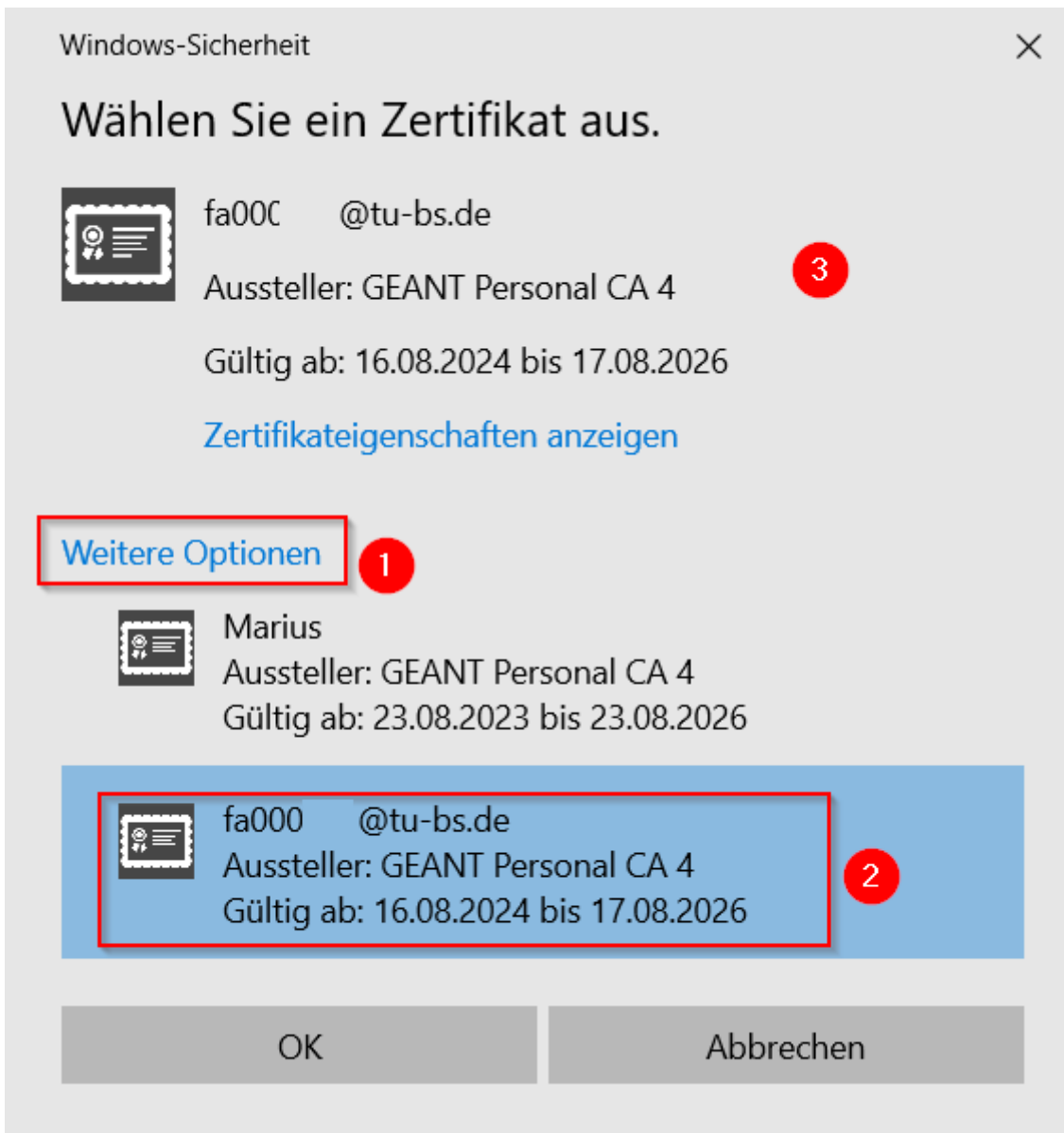
Verschlüsselungszertifikat: Auswählen...

Verschlüsselungsalgorithmus:

Signierten Nachrichten diese Zertifikate hinzufügen

OK Abbrechen

Im folgenden Auswahldialog auf Weitere Optionen (1) klicken und das eben importierte Zertifikat für den Funktionsaccount auswählen (2), daraufhin aktualisiert sich (3) und es kann mit OK bestätigt werden:



Nun muss sichergestellt werden, dass das Zertifikat (1) passt, der Hashalgorithmus auf SHA-512 geändert (2) und ggf. Verschlüsselungsalgorithmus auf AES256 angepasst wird, das ganze mit Klick auf OK (4) bestätigen.

Hinweis: die Verwendung als Verschlüsselungszertifikat wird offiziell nicht empfohlen, da es zu Datenverlust führen wird, sollte das Zertifikat und Passwort nicht sicher aufbewahrt werden!

Sicherheitseinstellungen ändern



Bevorzugte Sicherheitseinstellungen

Name der Sicherheitseinstellung: gitz-client- j@tu-braunschweig.de

Kryptografieformat: S/MIME

Standardeinstellung für dieses Format kryptografischer Nachrichten

Standardsicherheitseinstellung für alle kryptografischen Nachrichten

Sicherheitskennzeichen... Neu Löschen

Zertifikate und Algorithmen

Signaturzertifikat: fa000 @tu-bs.de 1 Auswählen...

Hashalgorithmus: SHA512 2 ✓

Verschlüsselungszertifikat: fa000 @tu-bs.de Auswählen...

Verschlüsselungsalgorithmus: AES (256-bit) 3 ✓

Signierten Nachrichten diese Zertifikate hinzufügen


OK 4 Abbrechen

Der Haken bei „**Standardeinstellung für dieses Format kryptografischer Nachrichten**“ und „**Standardsicherheitseinstellung für alle kryptografischen Nachrichten**“ werden von Outlook ggf. automatisch gesetzt.

Anschließend sind beide Zertifikatsprofile hinterlegt und das Trust Center kann mit Klick auf OK geschlossen werden.


Vertrauenswürdige Herausgeber
Datenschutzoptionen
E-Mail-Sicherheit
Anlagenbehandlung
Automatischer Download
Makroinstellungen
Programmgesteuerter Zugriff

Verschlüsselte E-Mail-Nachrichten

 Inhalt und Anlagen für ausgehende Nachrichten verschlüsseln
 Ausgehenden Nachrichten digitale Signatur hinzufügen
 Signierte Nachrichten als Klartext senden
 S/MIME-Bestätigung anfordern, wenn mit S/MIME signiert

Standardeinstellung:

Digitale IDs (Zertifikate)

 Digitale IDs bzw. Zertifikate sind Dokumente, mit denen die Identität in elektronischen Transaktionen nachgewiesen werden kann.

Als Nur-Text lesen

Standardnachrichten im Nur-Text-Format lesen
 Digital signierte Nachrichten im Nur-Text-Format lesen

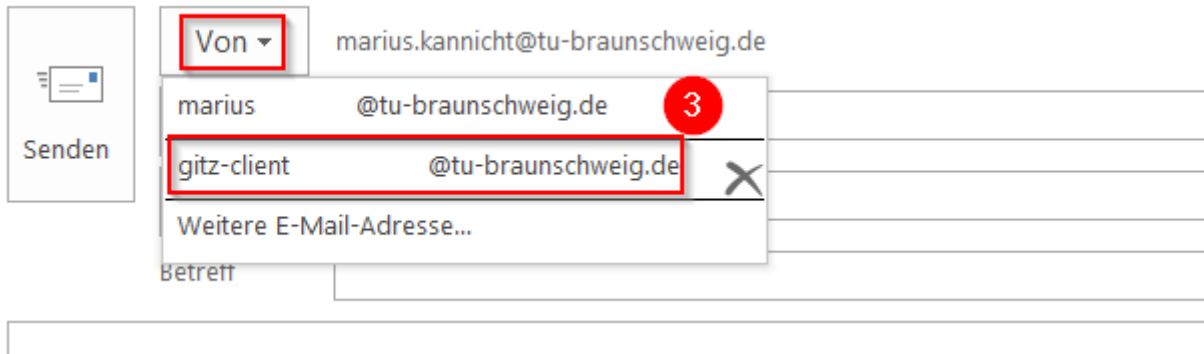
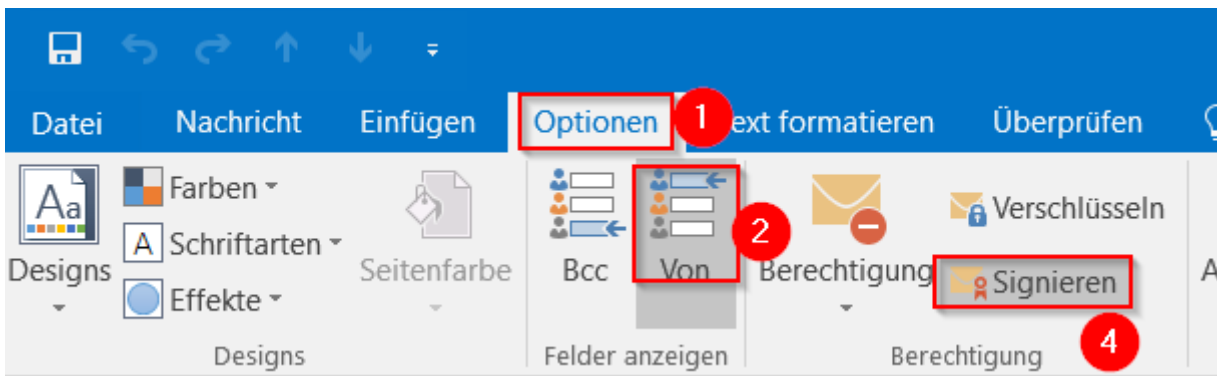
Skript in Ordnern

Skript in freigegebenen Ordnern zulassen
 Skript in Öffentlichen Ordnern zulassen

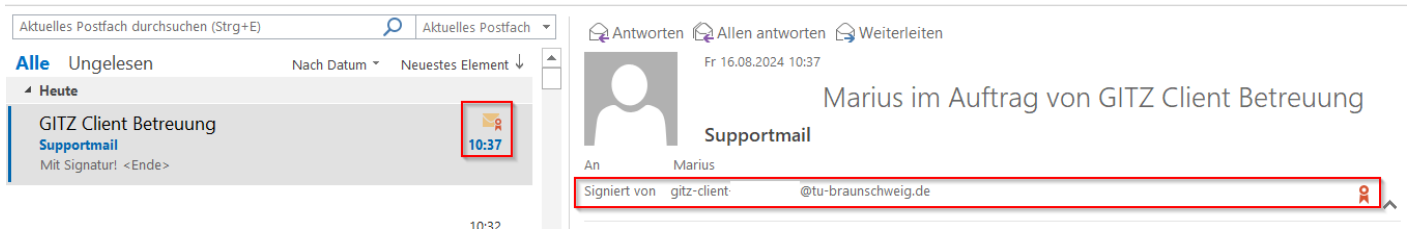
Soll jetzt nun mit "Senden Als" oder "Senden im Auftrag" eine E-Mail signiert werden, wie folgt vorgehen:

Neue E-Mail schreiben, mit Klick auf Optionen (1) und Von (2) die entsprechende Funktions-E-Mail-Adresse auswählen (3) und sicherstellen, dass das Signieren (4) ausgewählt ist. Wie gewohnt mit dem Verfassen fortfahren.

Beim Senden kommt je nach oben gewählter Sicherheitsstufe beim Import dann eine neue Passwortabfrage für den Zugriff über die CryptoAPI auf die hinterlegten Zertifikate. Wurde ein solches festgelegt, ist dieses Passwort bei allen Zugriffen auf die hinterlegten Zertifikate (personenbezogene Accounts oder Funktionsaccounts) identisch.



Die so signierte E-Mail wird dann wie folgt bei den Empfängern angezeigt: gesendet durch Person x im Auftrag der Funktionsadresse (oder direkt als dieser Account bei "Senden Als" Rechten) und signiert durch das Zertifikat des Accounts.



Mit Klick auf die Schleife können die Signaturdetails überprüft werden:

Digitale Signatur: Gültig


Betreff: Supportmail
Von: Marius
Signiert von: gitz-client-@tu-braunschweig.de

 Die digitale Signatur dieser Nachricht ist gültig und vertrauenswürdig.
Klicken Sie auf "Details", um weitere Informationen zum Zertifikat zu erhalten, das für die digitale Signatur der Nachricht verwendet wurde.

Details...

Schließen

Eigenschaften der Nachrichtensicherheit

 Betreff: Supportmail

Nachrichten enthalten u. U. Ebenen für Verschlüsselung oder digitale Signaturen. Jede Ebene für digitale Signaturen kann mehrere Signaturen enthalten.

Sicherheitsschichten
Wählen Sie eine Signaturschicht aus, um deren Beschreibung anzuzeigen.

- ✓ **Betreff: Supportmail**
 - ✓ Digitalsignaturschicht
 - ✓ Signierer: gitz-client-@tu-braunschweig.de

Beschreibung:
OK: Signierte Nachricht.

Klicken Sie auf die Schaltflächen, um weitere Informationen zur gewählten Signaturschicht zu erhalten oder um sie zu bearbeiten:

Vertrauen... Details anzeigen... Zertifizierungsstelle vertrauen...

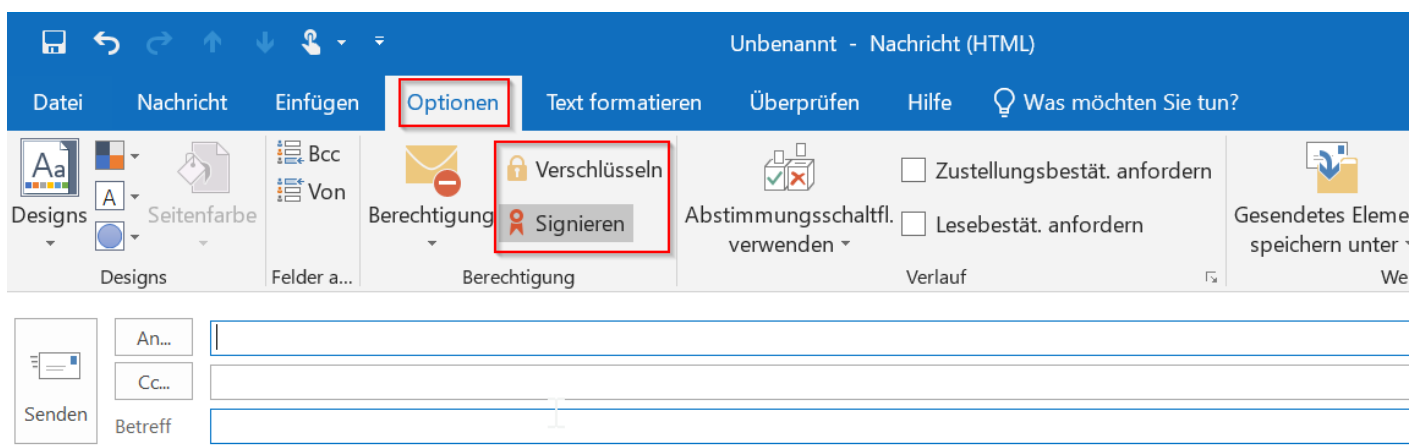
Schließen

Verwendung

Beim Verfassen einer neuen E-Mail oder beim Beantworten ist durch die im Trust-Center vorgenommenen Einstellungen nun standardmäßig das Signieren aktiviert worden. Sollte die hohe Sicherheitsstufe für die Verwendung gewählt worden sein, wird nun z.B. beim Absenden einer Signierten Nachricht das gewählte Passwort abgefragt. Das Signieren kann aber auch in jeder Kommunikation deaktiviert oder auch das zusätzliche Verschlüsseln aktiviert werden.

Bewahren Sie Passwörter, private Schlüssel und auch abgelaufene Zertifikate immer sorgfältig auch, um Datenverlust zu vermeiden, siehe auch [wichtige Hinweise](#).

Zum Anpassen der Optionen bitte in der geöffneten E-Mail **[Optionen]** auswählen und die gewünschten Einstellungen vornehmen:



Die oben genannte Passwortabfrage unterscheidet sich von der Exchange oder Windows-Domänen-Passwortabfrage und sieht wie folgt aus:



Anmeldeinformationen erforderlich

Geben Sie das Kennwort ein, um der App Zugriff auf Ihren privaten Schlüssel zu gewähren:

Schlüsselbeschreibung : Privater Schlüssel des
CryptoAPI



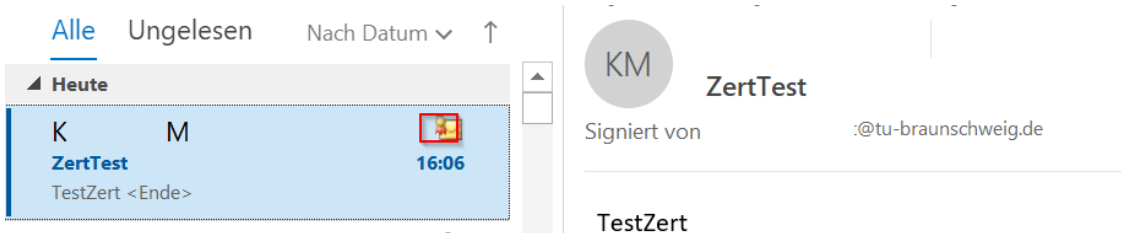
Kennwort

Zulassen

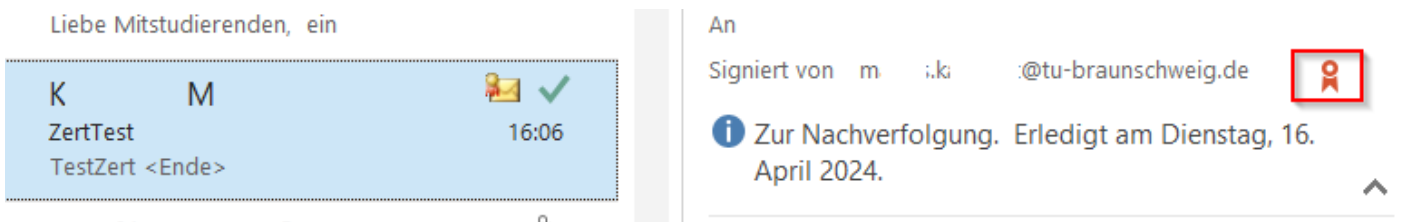
Nicht zulassen

Erkennen von korrekt signierten Nachrichten

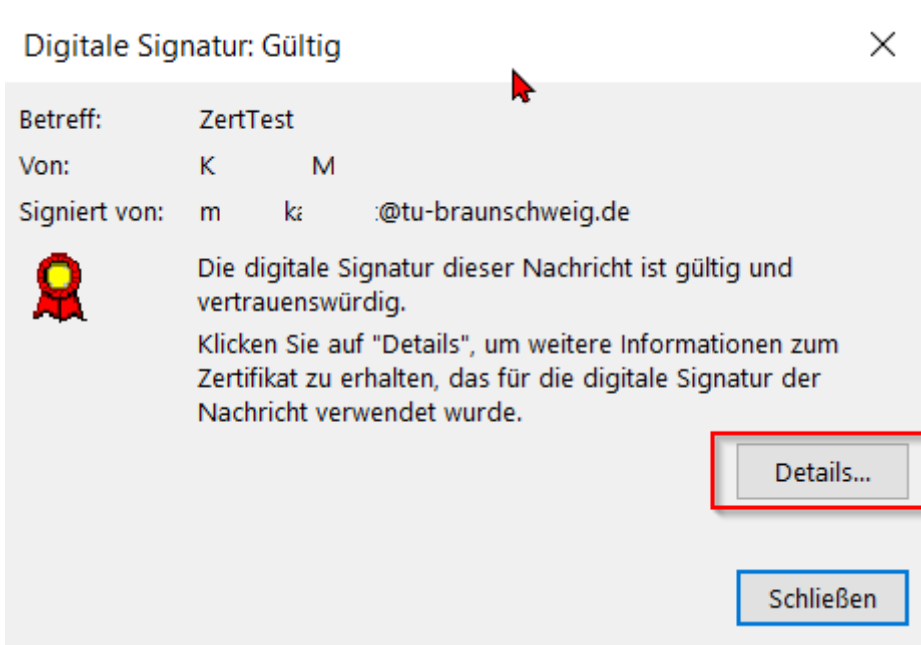
Eine signierte Nachricht erkennen Sie am "Schleifchen" des E-Mail-Symbols.



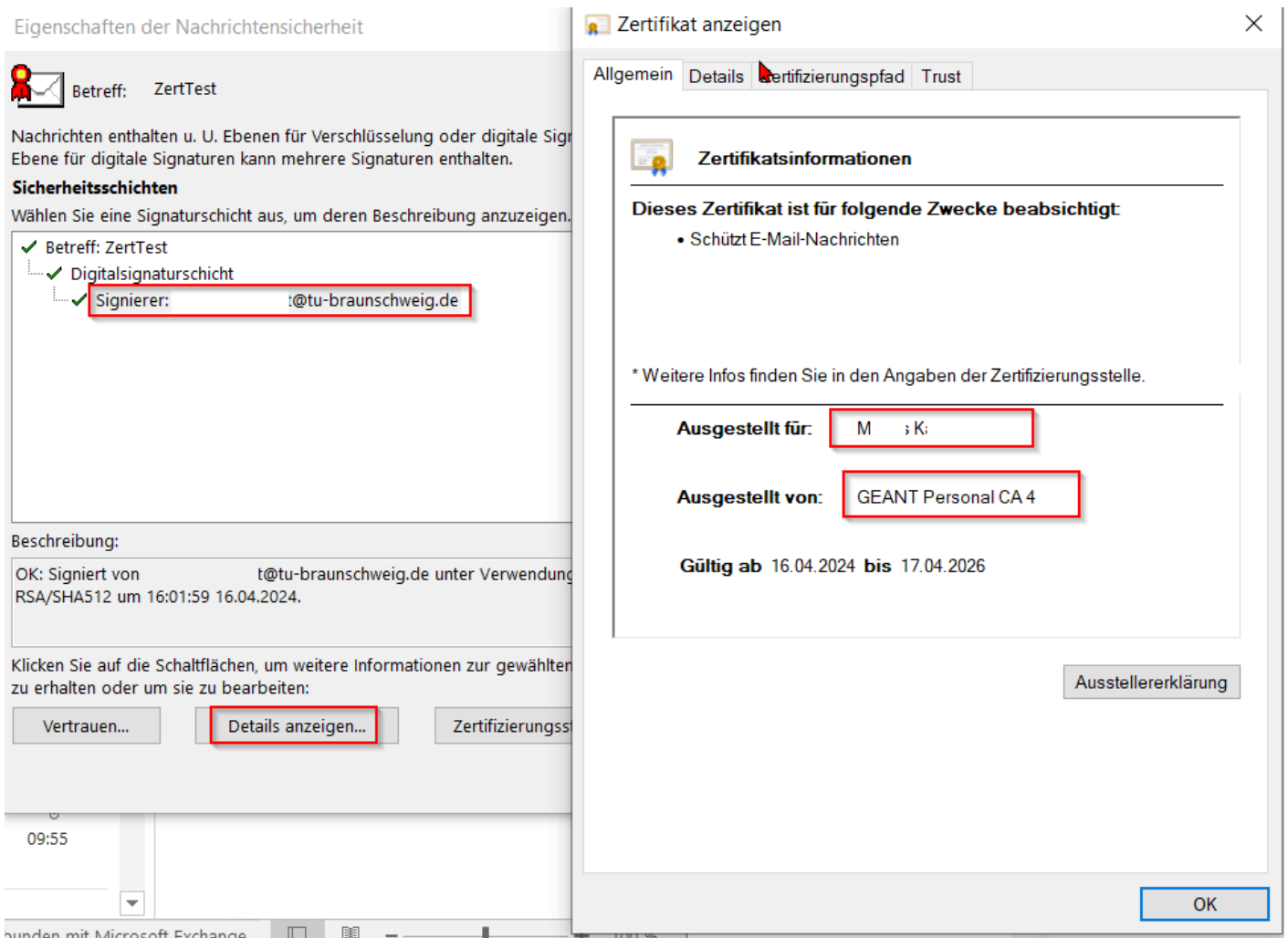
Im Nachrichtenkopf können Sie mit Klick auf das **[Schleifchen]** die Signatur überprüfen.



Es öffnet sich ein neues Fenster, in welchem weitere Informationen zur Signatur stehen. In diesem können Sie sich mit einem Klick auf **[Details]** weitere Informationen bezüglich des Zertifikates anzeigen lassen.



Es öffnet sich ein weiteres Fenster, in welchem unter anderem die ausstellende Einheit steht und für welche Person das Zertifikate ausgestellt worden ist.



Wichtige Hinweise

- **Bewahren Sie Ihre Passwörter und ggf. privaten Schlüssel getrennt und sicher auf**, etwa in einem vertrauenswürdigen Passwortmanager oder in verschlüsselten Containern. Legen Sie zusätzlich eine offline gesicherte Kopie auf einem verschlüsselten Medium (zum Beispiel einem USB-Stick im Tresor) an, um im Notfall darauf zugreifen zu können.
- **Verlust von Passwörtern oder privaten Schlüsseln führt zum unwiederbringlichen Datenverlust!** Bereits verschlüsselte E-Mails lassen sich ohne den privaten Schlüssel oder die korrekte Passphrase nicht mehr entschlüsseln.
- **Löschen Sie niemals abgelaufene Zertifikate!** Auch abgelaufene Zertifikate werden zum Entschlüsseln älterer Nachrichten benötigt, bei Verlust ist eine Entschlüsselung nicht mehr möglich.
- **Richten Sie eine klare Backup- und Wiederherstellungsstrategie ein**, erstellen Sie regelmäßige, ebenfalls verschlüsselte Sicherungen von den verwendeten Passwörtern, privaten Schlüsseln und Zertifikaten und testen Sie die Wiederherstellung in festgelegten Abständen, um im Ernstfall vorbereitet zu sein.