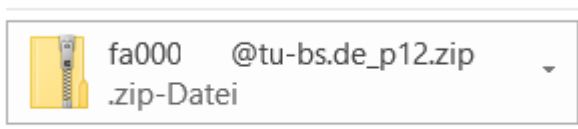


Import zusätzlicher Zertifikate für Funktionsaccounts

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 verwalten

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

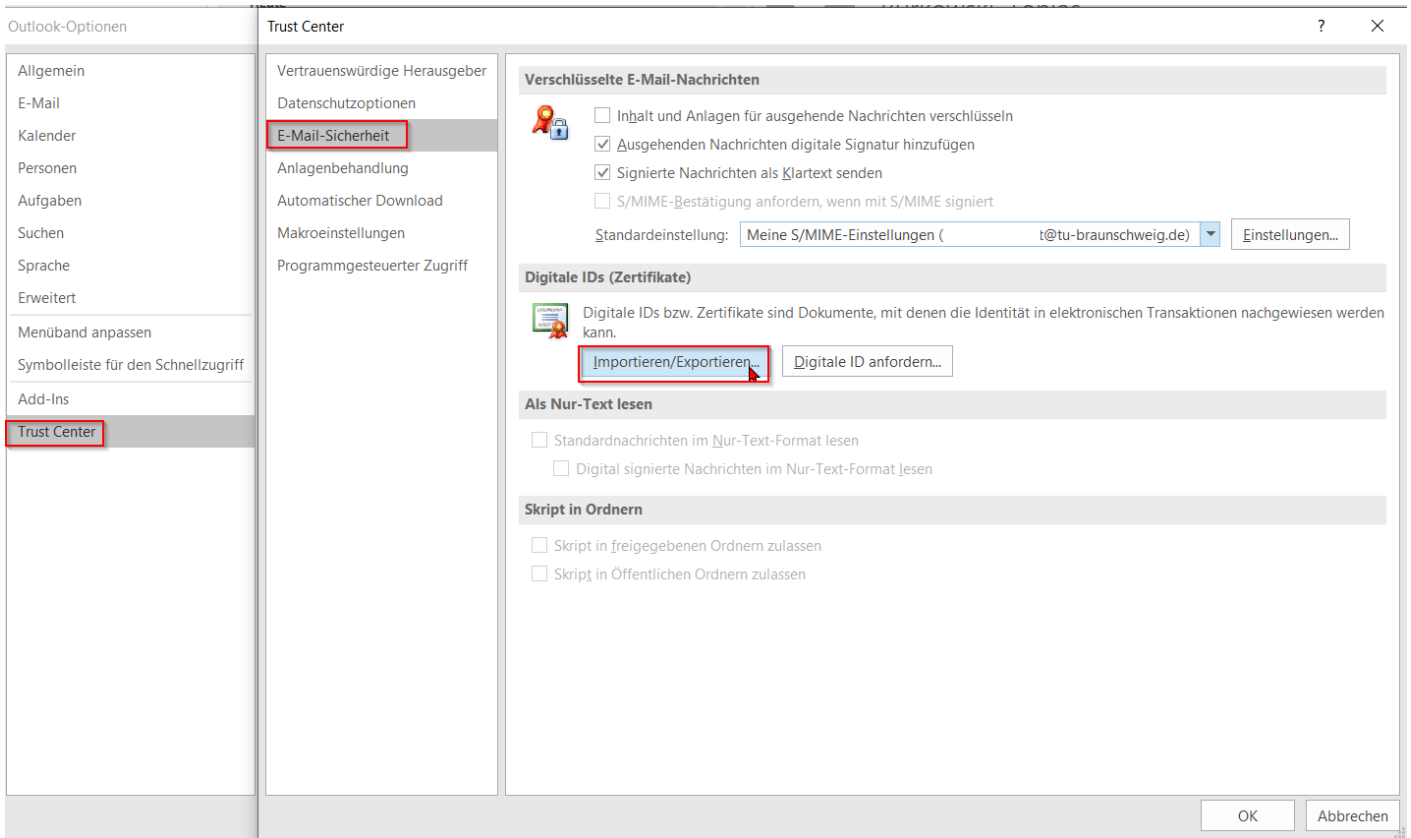
Langsame und deaktivierte COM-Add-Ins

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

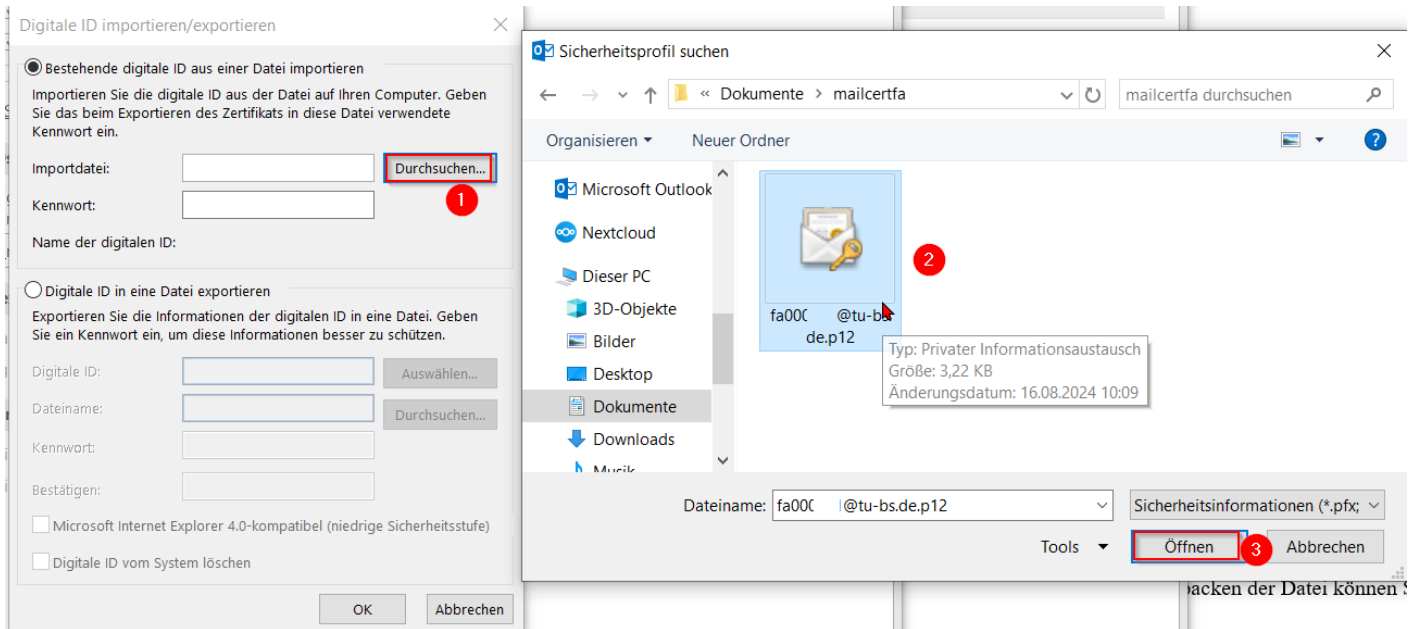
Add-Ins verwalten

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 (1). In the main area, 'E-Mail-Sicherheit' is selected in the left-hand menu with a red circle (2). The 'Verschlüsselte E-Mail-Nachrichten' section is active, and the 'Einstellungen...' button is highlighted with a red circle (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 'Kryptografieformat' is set to 'S/MIME'. The 'Standardinstellung für dieses Format kryptografischer Nachrichten' and 'Standardsicherheitseinstellung für alle kryptografischen Nachrichten' are both checked. The 'Sicherheitskennzeichen...' button has a 'Neu' button highlighted with a red circle (4). The 'Zertifikate und Algorithmen' section shows 'Signaturzertifikat' and 'Verschlüsselungszertifikat' both set to 'Marius'. The 'Verschlüsselungsalgorithmus' is set to 'AES (256-bit)'. The 'OK' and 'Abbrechen' buttons are visible at the bottom of the dialog box.

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:

Sicherheits-einstellungen 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: []

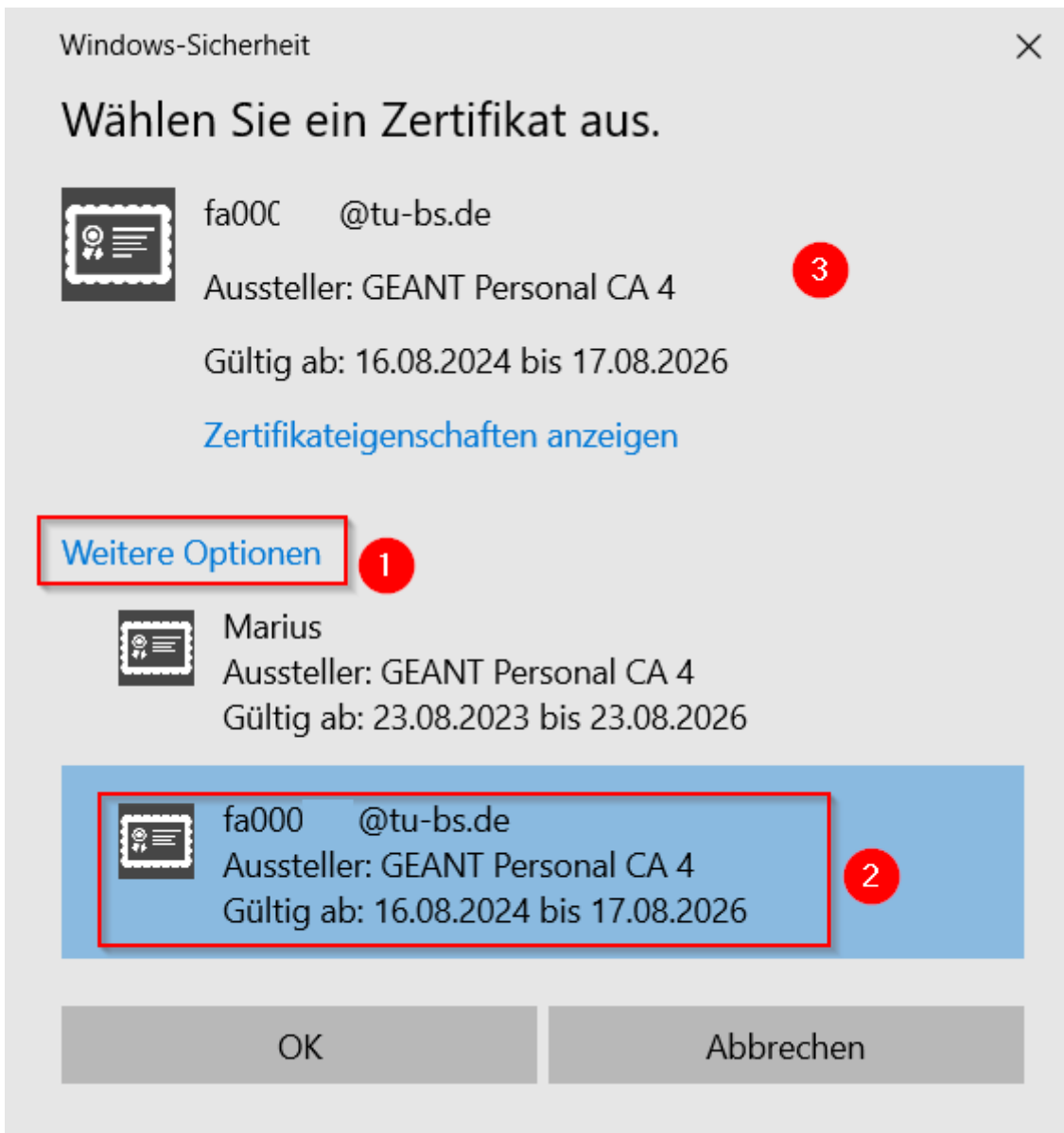
Verschlüsselungszertifikat: [] Auswählen...

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

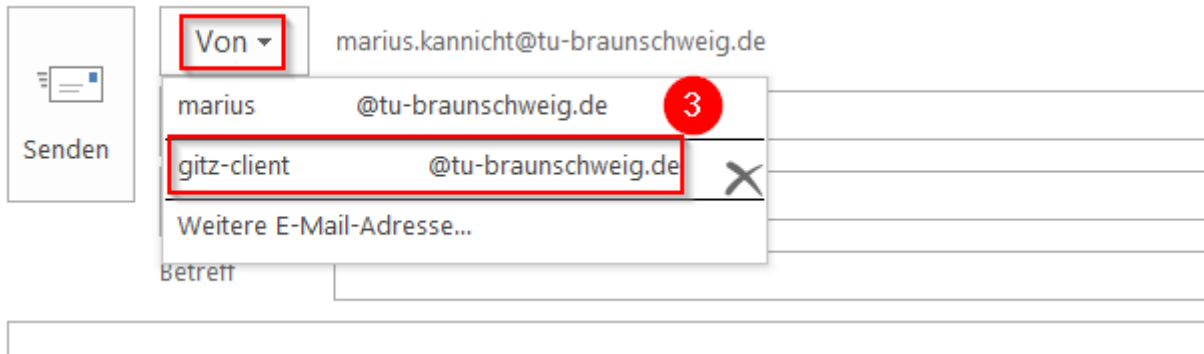
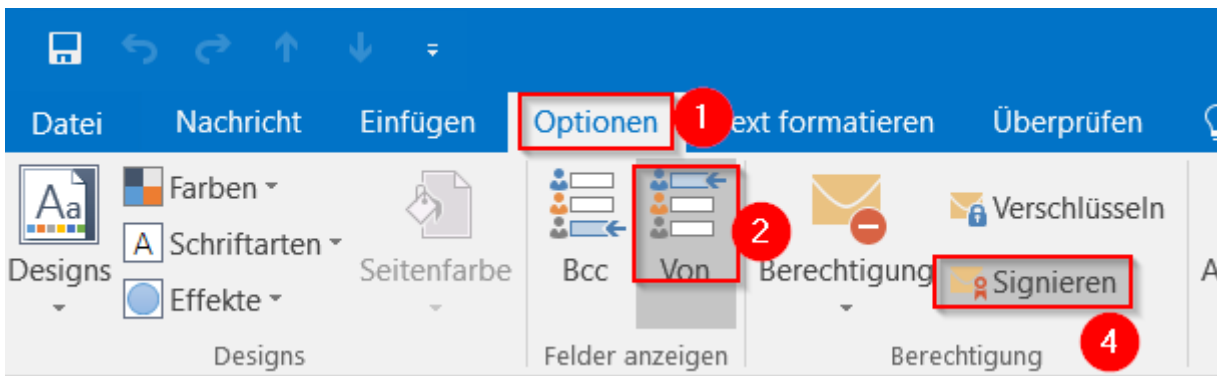
Skript in Ordnern

Skript in freigegebenen Ordnern zulassen
 Skript in Öffentlichen Ordnern zulassen

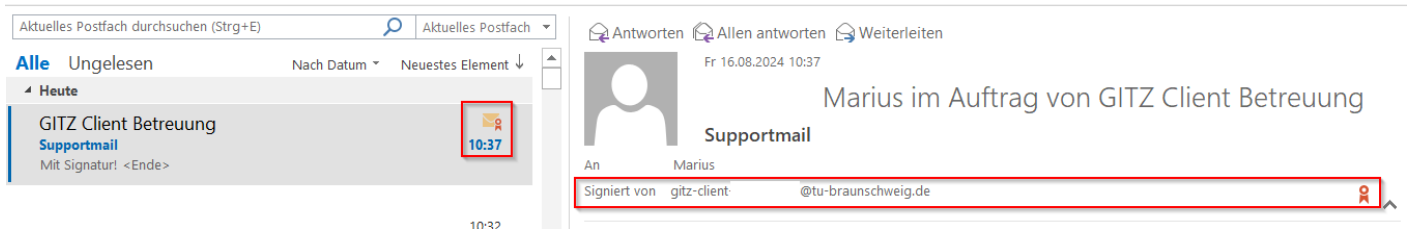
Soll jetzt nun mit "Senden Als" oder "Senden im Auftrag" eine E-Mail signiert werden, wie folgt vorgehen:

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.

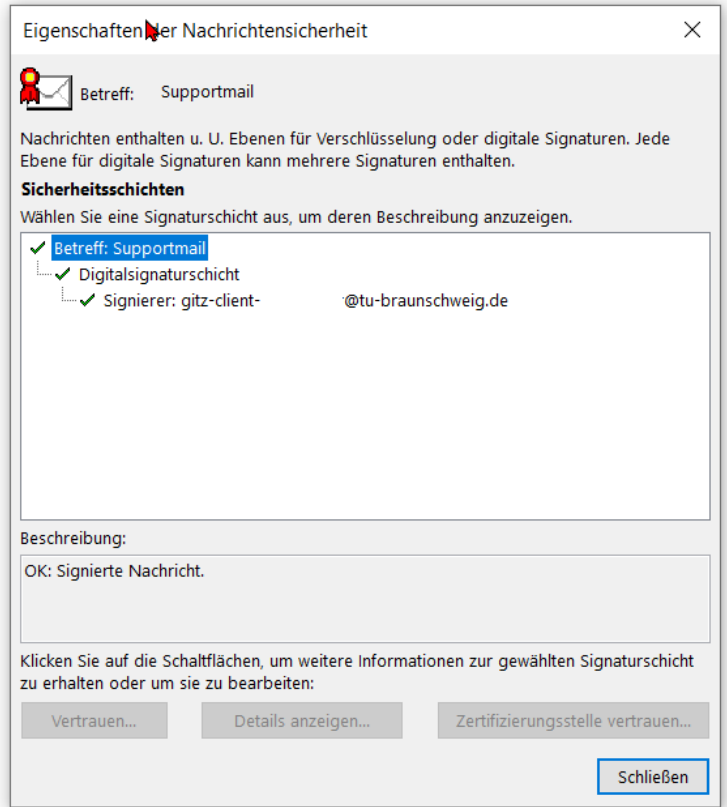
Beim Senden kommt je nach oben gewählter Sicherheitsstufe beim Import dann eine neue Passwortabfrage für den Zugriff über die CryptoAPI auf die hinterlegten Zertifikate. Wurde ein solches festgelegt, ist dieses Passwort bei allen Zugriffen auf die hinterlegten Zertifikate (personenbezogene Accounts oder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



Die so signierte E-Mail wird dann wie folgt bei den Empfängern angezeigt: gesendet durch Person x im Auftrage 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:



Revision #11

Created 2024-08-16 09:20:55 UTC by Marius Kannicht

Updated 2026-05-18 07:07:56 UTC by Jan-Marc Pilawa