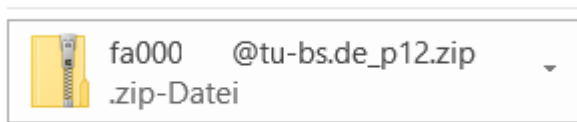


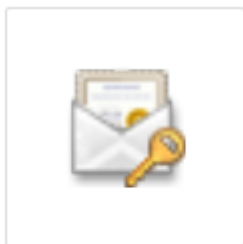
Import zusätzlicher Zertifikate für Funktionsaccounts

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

Posteingang - marius.kannicht@tu-

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.

Tools zum 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.

Informationen

Öffnen und Exportieren

Speichern unter

Anlagen speichern

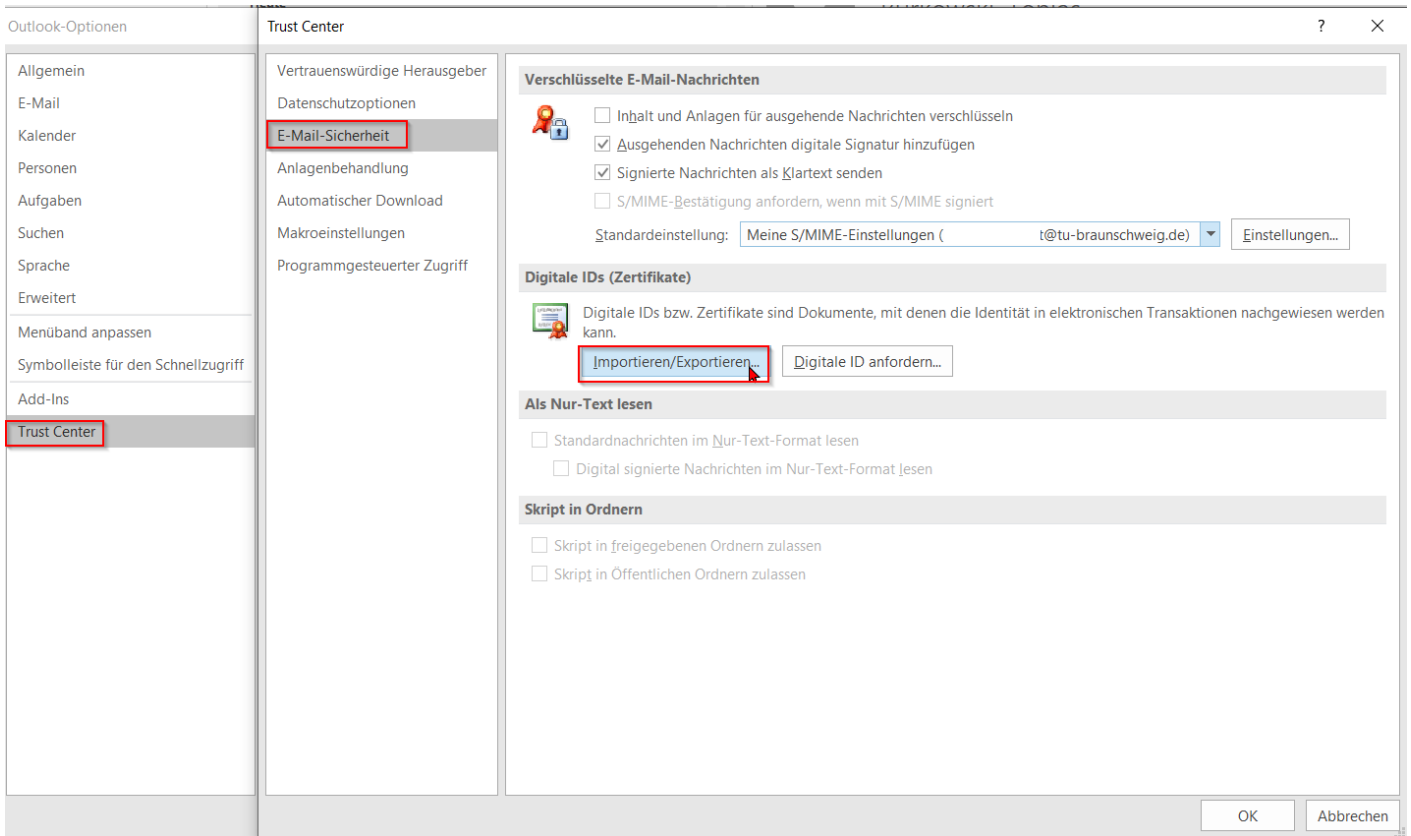
Drucken

Office-Konto

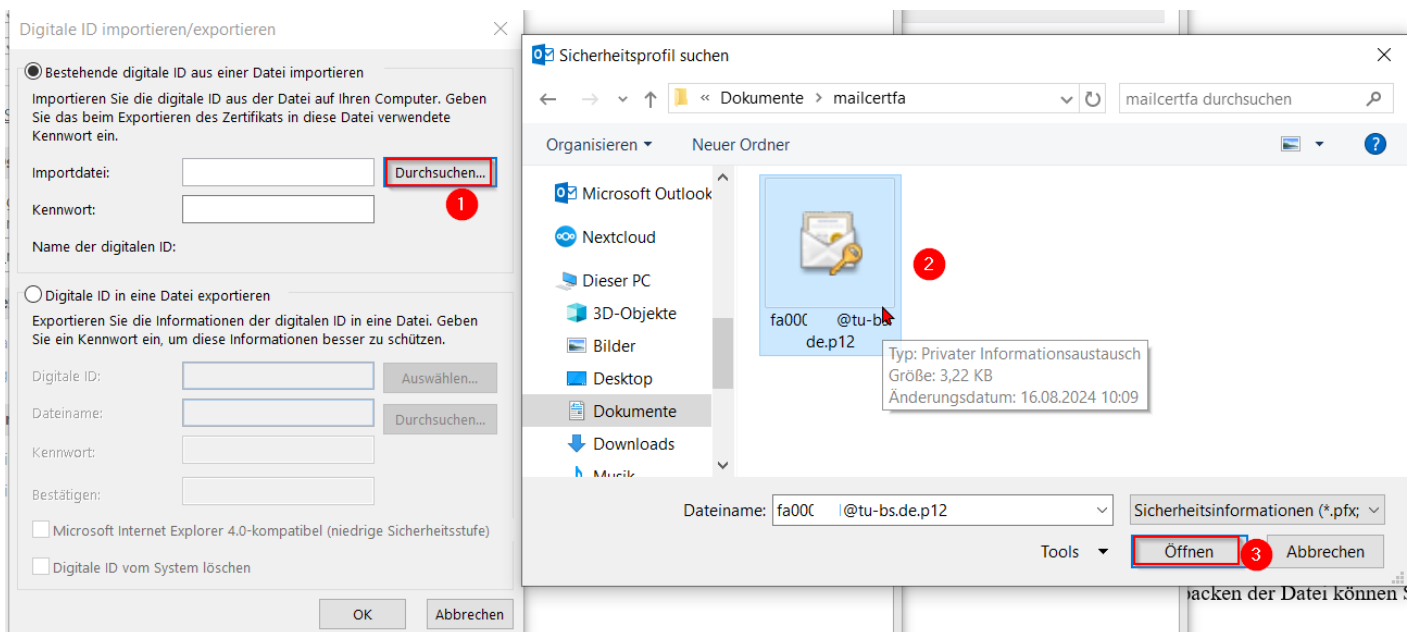
Optionen

Beenden

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

OK

2

Abbrechen

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 Options window with the Trust Center tab selected (1). In the Trust Center, the E-Mail-Sicherheit section is highlighted (2). The 'Verschlüsselte E-Mail-Nachrichten' section shows the 'Einstellungen...' button (3). A dialog box titled 'Sicherheitseinstellungen ändern' is open, showing the 'Neu' button (4) to create a new security profile. The dialog box also shows the 'Standard-Sicherheitseinstellung für alle kryptografischen Nachrichten' checkbox checked.

Outlook-Optionen

Trust Center

Vertrauenswürdige Herausgeber

Datenschutzoptionen

E-Mail-Sicherheit (2)

Anlagenbehandlung

Automatischer Download

Makroeinstellungen

Programmgesteuerter Zugriff

Digitale IDs (Zertifikate)

Digitale IDs bzw. Zertifikate sind Dokumente, die die Identität eines Senders bestätigen können.

Importieren/Exportieren...

Als Nur-Text lesen

Standardnachrichten im Nur-Text-Format

Digital signierte Nachrichten im Nur-Text-Format

Skript in Ordnern

Skript in freigegebenen Ordnern zulassen

Skript in Öffentlichen Ordnern zulassen

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: Meine S/MIME-Einstellungen (marius :@tu-braunschweig.de)

Einstellungen... (3)

Sicherheitseinstellungen ändern

Bevorzugte Sicherheitseinstellungen

Name der Sicherheitseinstellung: Meine S/MIME-Einstellungen (marius :@tu-braunschweig.de)

Kryptografieformat: S/MIME

Standard-Sicherheitseinstellung für dieses Format kryptografischer Nachrichten

Standardsicherheitseinstellung für alle kryptografischen Nachrichten

Sicherheitskennzeichen... (4) Neu Löschen

Zertifikate und Algorithmen

Signaturzertifikat: Marius Auswählen...

Hashalgorithmus: SHA512

Verschlüsselungszertifikat: Marius Auswählen...

Verschlüsselungsalgorithmus: AES (256-bit)

Signierten Nachrichten diese Zertifikate hinzufügen

OK Abbrechen

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: ▼

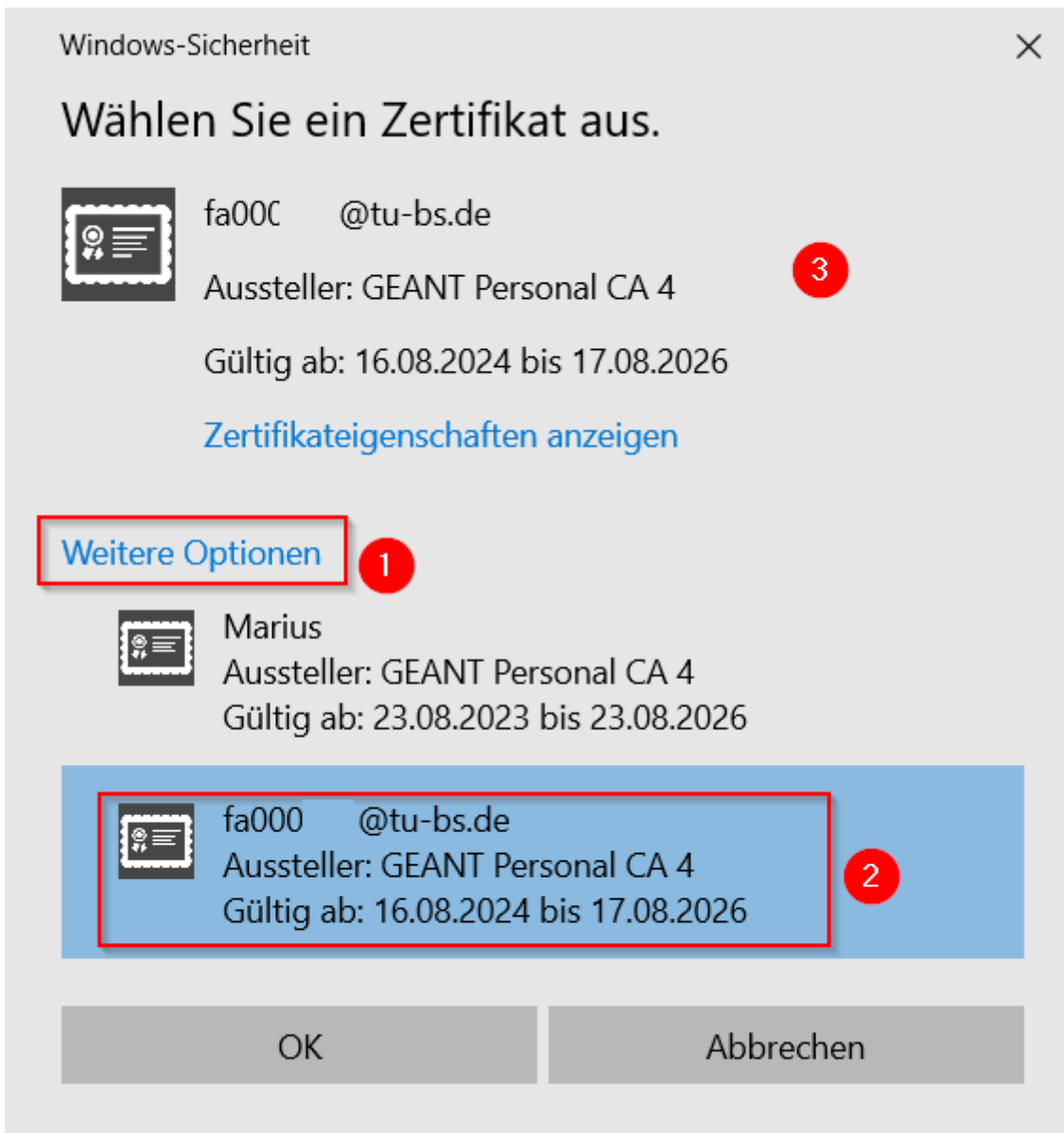
Verschlüsselungszertifikat: Auswählen...

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

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

Vertrauenswürdige Herausgeber

Datenschutzooptionen

E-Mail-Sicherheit


Anlagenbehandlung

Automatischer Download

MakroEinstellungen


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:

gitz-client-@tu-braunschweig.de

Einstellungen...

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

Importieren/Exportieren...

Digitale ID anfordern...

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

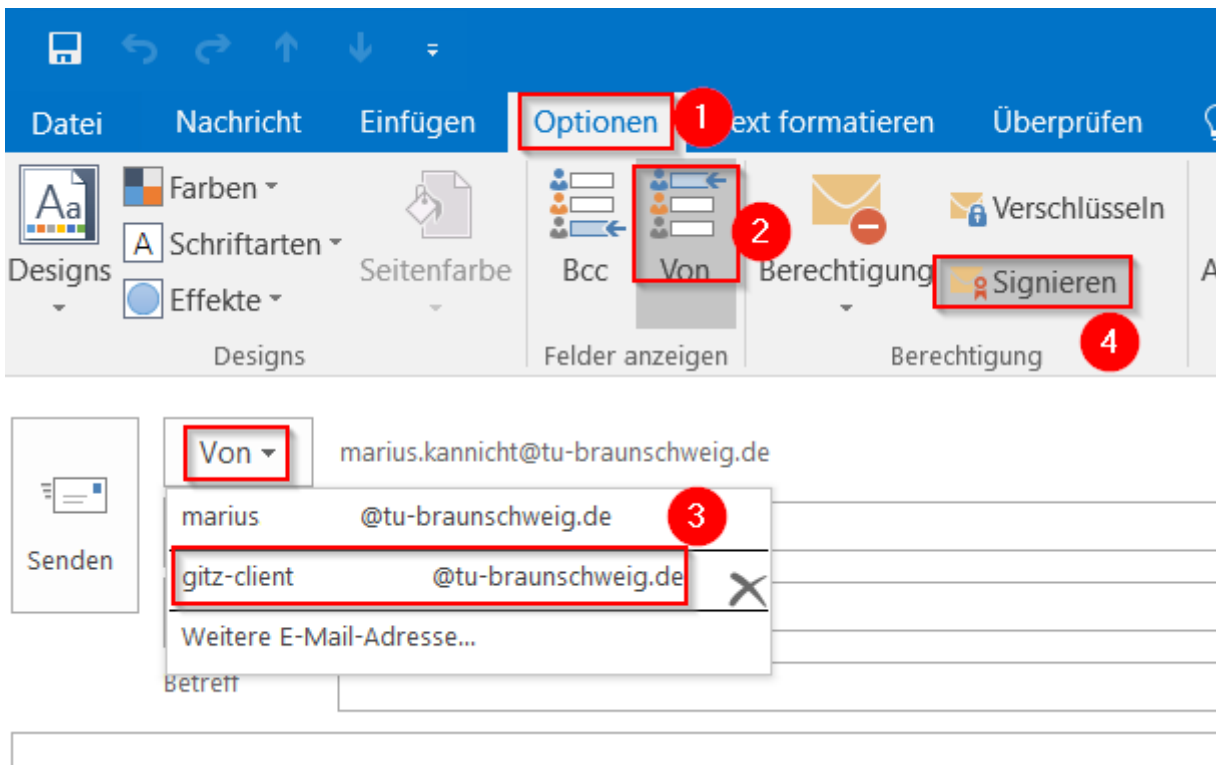
OK

Abbrechen

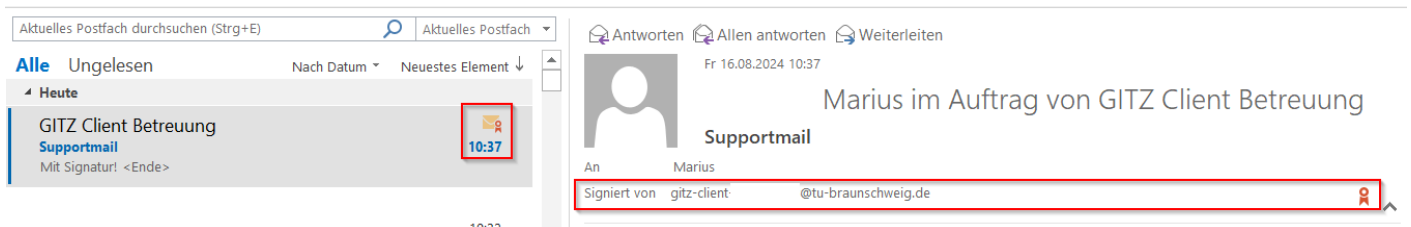
Soll jetzt nun mit "Senden Als" oder "Senden im Auftrag" eine E-Mail signiert werden, wie folgt vorgehen:

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.

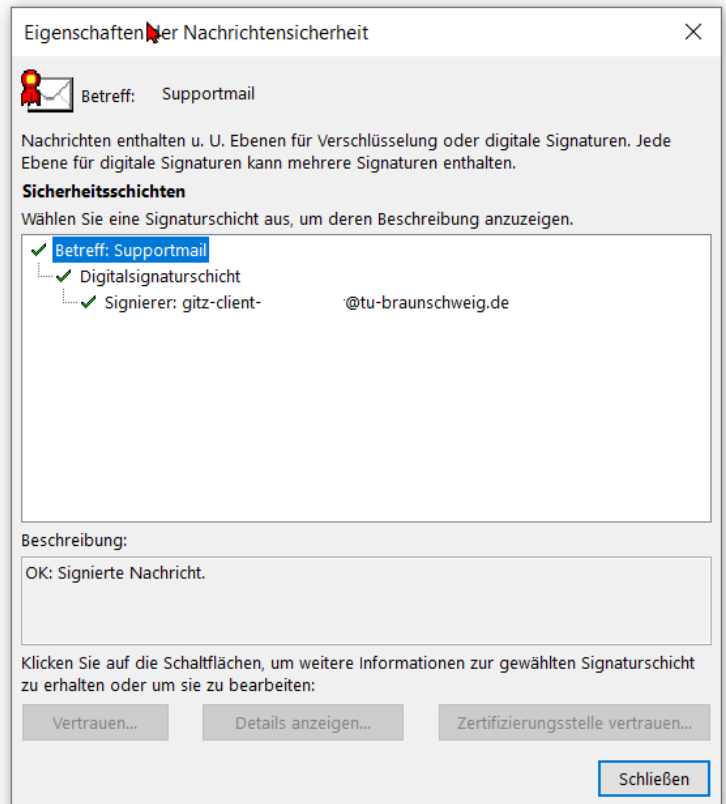
Beim Senden kommt je nach oben gewählter Sicherheitsstufe beim Import dann eine neue Passwortabfrage für den Zugriff über die CryptoAPI auf die hinterlegten Zertifikate. Wurde ein solches festgelegt, ist dieses Passwort bei allen Zugriffen auf die hinterlegten Zertifikate (personenbezogene Accounts oder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



Revision #9

Created 16 August 2024 09:20:55 by Marius Kannicht

Updated 16 August 2024 11:06:19 by Sandra Ulbrich