

[MS-OUT] Microsoft Outlook E-Mail-Sicherheit [Signieren+ Verschlüsseln E-Mail mittels Zertifikate]

Autor: Hans G. Zeger
Version 2.2 / 6. Juli 2023
<http://www.globaltrust.eu/static/outlook-anleitung.pdf>

© e-commerce monitoring GmbH 2023

Redaktioneller Hinweis: Das vorliegende Dokument ist mit einer Signatur versehen. Das Datum der Signatur kann aus verschiedenen rechtlichen und organisatorischen Gründen vom Datum des Gültigkeitsbeginns des Dokuments abweichen. Die Signatur gibt keine Auskunft über den Gültigkeitsbeginn des Dokuments, sondern bestätigt nur die Unversehrtheit des Inhalts.

Urheberrechtshinweis: Das Dokument unterliegt dem Urheberrecht und wird nur im Rahmen der Zertifizierungsdienste zur Verfügung gestellt. Eine darüber hinausgehende Verwendung, eine vollständige oder auszugsweise Übermittlung an Dritte oder die Veröffentlichung des Dokuments durch Dritte bedarf der vorherigen Zustimmung des Autors/der Autoren und des Zertifizierungsdiensteanbieters.

Inhalt

1	Grundlagen	4
1.1	Ziele des Dokuments.....	4
1.2	Definitionen und Kurzbezeichnungen	4
1.3	Änderungshistorie.....	5
1.3.1	V1.1 Stammfassung.....	5
1.3.2	V2.0 Fassung für Outlook 2016	5
1.3.3	Version 2.2 Ergänzung Microsoft Security-Verwaltung	5
2	Kurzfassung Zertifikatsinstallation Outlook 2016	5
3	Einrichten des Zertifikates (E-Mail Sicherheit) in OUTLOOK 2016	6
3.1	Beschaffung der PKCS#12-Datei	6
3.2	Installation PKCS#12-Datei in Outlook 2016.....	8
4	GLOBALTRUST-Zertifikate in Outlook 2016 nutzen.....	16
4.1	Mail signiert versenden	16
4.2	signiertes Mail prüfen.....	18
4.3	E-Mail verschlüsselt verschicken	25
4.3.1	Fall 1: vorgesehener Empfänger hat ein signiertes E-Mail geschickt.....	25
4.3.2	Fall 2: Empfänger in LDAP-Server suchen	27
5	GLOBALTRUST LDAP-Server ldap.globaltrust.eu verwenden	31
5.1	LDAP-Server ldap.globaltrust.eu einrichten.....	31
5.2	Personensuche mittels LDAP-Server ldap.globaltrust.eu	35
5.3	optionale Anpassung des Outlook-Adressbuches	37
6	Einrichten Outlook 2016 - E-Mail-Account.....	39
6.1	Outlook 2016 "Standard"	39
6.2	Outlook 2016 "Professional"	47
7	Troubleshooting Outlook 2016.....	49
7.1	Fehlermeldungen und Warnhinweise.....	49
7.1.1	Scheinbares Fehlen des Zertifikates.....	49
7.1.2	Zertifikat wird von Microsoft nicht zur eMail-Signatur akzeptiert.....	50
	STEP 1: Prüfen Stammzertifikate in Zertifikate	52
	STEP 1a: Import Stammzertifikat (nur bei fehlenden Zertifikaten erforderlich)	52
	STEP 2: Prüfen Stammzertifikate in Vertrauenswürdige Herausgeber.....	54
	STEP 3: Prüfen Einstellungen in Outlook Trust Center	55
7.1.3	Fehlerhafte Zertifikats-Kette bei einem eingehenden E-Mail.....	58
7.2	Hilfsmassnahmen	60
7.2.1	Prüfen Laufzeit des Zertifikates.....	60
7.2.2	Prüfen Widerrufsstatus	63
7.2.3	Prüfen Zertifikatskette.....	65
8	Frühere Outlook Versionen.....	66
8.1	Outlook 2013 – Zertifikat installieren und verwenden	66
8.1.1	Zertifikat installieren	66
	8.1.1.1 Zertifikat in Windows installieren	66
	8.1.1.2 Outlook 2013 Menü	70
8.1.2	Signierte E-Mail Verfassen und Versenden.....	73
8.1.3	E-Mails verschlüsseln	73

8.1.3.1	Methode I - Signatur erkennen und antworten.....	74
8.1.3.2	Methode II - Kontakt öffnen	75
8.1.4	LDAP-Server einrichten.....	78
8.1.4.1	Kurzfassung	78
8.1.4.2	Installation des LDAP Verzeichnisses	79
8.1.5	LDAP Verzeichnis verwenden	85
8.2	Outlook 2007/2010 – Zertifikat installieren und verwenden.....	86
8.2.1	Zertifikat installieren	86
8.2.2	Outlook konfigurieren - Vertrauensstellungcenter öffnen	88
8.2.3	E-Mails signieren und/oder verschlüsseln	91

1 GRUNDLAGEN

1.1 ZIELE DES DOKUMENTS

Diese Anleitung ist optimiert für die Installation und Nutzung von Zertifikaten mit Microsoft Outlook 2016 zum signieren und verschlüsseln von E-Mails:

- ⇒ 2 Kurzfassung Zertifikatsinstallation Outlook 2016 (p5)
- ⇒ 3 Einrichten des Zertifikates (E-Mail Sicherheit) in OUTLOOK 2016 (p6)
- ⇒ 4 GLOBALTRUST-Zertifikate in Outlook 2016 nutzen (p16)

Zusätzliche Informationen:

- einrichten des GLOBALTRUST-LDAP-Servers ldap.globaltrust.eu (⇒ 5 GLOBALTRUST LDAP-Server ldap.globaltrust.eu verwenden p31)
- einrichten eines Outlook 2016 - Accounts wenn Anmeldenamen und E-Mail-Adresse des Mailservers abweichen (⇒ 6 Einrichten Outlook 2016 - E-Mail-Account p39)
- Troubleshooting Outlook 2016 (⇒ 7 Troubleshooting Outlook 2016 p49)
- Informationen zu den älteren Outlookversionen (⇒ 8 Frühere Outlook Versionen p66)

Hinweis:

Diese Anleitung wurde für Microsoft Windows erstellt. Für Outlook auf Mac OS wurde diese Anleitung nicht getestet. Die verwendeten Screenshots sind als Symbolbilder zu verstehen und können auf Grund von Sprachvarianten, Patchversionen und sonstigen Besonderheiten von Ihrer konkreten Installation abweichen.

Die verwendeten E-Mail-Adressen und Personenbezeichnungen können zwischen den verschiedenen Screens variieren.

1.2 DEFINITIONEN UND KURZBEZEICHNUNGEN

CA (Certificate Authority)

Zertifikat, das berechtigt ist andere Zertifikate auszustellen. Man unterscheidet oberste Zertifikate (RootCAs) und Zwischenzertifikate (SubCAs). Damit ein Endkunden-Zertifikat als echt anerkannt wird, muss die Zertifikatskette zwischen einer RootCA und dem Endkunden-Zertifikat geschlossen sein.

eIDAS-Verordnung

EU-Rechtsrahmen, der die Verwendung von Zertifikaten innerhalb der EU regelt. GLOBALTRUST ist ein Anbieter der eIDAS-konform ist (<https://webgate.ec.europa.eu/tl-browser/#/tl/AT/4>)

LDAP

Öffentlicher Verzeichnisdienst von Zertifikaten

PKCS#12-Datei

Datei die das Benutzerzertifikat, den privaten Schlüssel und alle notwendigen CA-Zertifikate enthält, meist wird die Endung .p12 oder .pfx verwendet

Ribbon

Menüleiste in Microsoft Office Produkten ab Version 2007

1.3 ÄNDERUNGSHISTORIE

1.3.1 V1.1 STAMMFASSUNG

Redaktionsschluss: 21. Mai 2015

1.3.2 V2.0 FASSUNG FÜR OUTLOOK 2016

Wesentliche Änderungen

- Dokumentation von Outlook 2016
- Installation des LDAP-Servers
- Informationen zum Zertifikats-Troubleshooting

Redaktionsschluss: 3. März 2020

1.3.3 VERSION 2.2 ERGÄNZUNG MICROSOFT SECURITY-VERWALTUNG

Wesentliche Änderungen

- Beschreibung Einstellung "Vertrauenswürdige Herausgeber"

Redaktionsschluss: 6. Juli 2023

2 KURZFASSUNG ZERTIFIKATSINSTALLATION OUTLOOK 2016

Diese Kurzfassung wendet sich an Benutzer, die schon Erfahrung mit der Installation und Verwendung von Zertifikaten haben und deckt nur die wesentlichen Schritte (ohne Erklärung) ab.

installieren Zertifikat:

- PKCS#12-Datei von GLOBALTRUST herunterladen und mit Doppelklick in der Windows-Zertifikatsverwaltung installieren
- In den Outlook-Optionen die Einstellungen für das Trust Center auswählen
- Unter „E-Mail-Sicherheit“ bei „Verschlüsselte E-Mail-Nachrichten“ die "Einstellungen..." auswählen
- Signatur- und Verschlüsselungszertifikat auswählen, Hashalgorithmus auf "SHA256" umstellen

Signieren/Verschlüsseln:

- Neue Nachricht verfassen
- Optionen-Ribbon anzeigen lassen
- Button Signieren bzw. Verschlüsseln drücken ⇒ Senden
- Um eine Nachricht zu verschlüsseln wird ein Zertifikat des Empfängers benötigt. (⇒ 4.3 E-Mail verschlüsselt verschicken p25)

3 EINRICHTEN DES ZERTIFIKATES (E-MAIL SICHERHEIT) IN OUTLOOK 2016

Diese Dokumentation setzt einen bestehenden Outlook 2016 Account mit genau jener E-Mail-Adresse voraus, die im Zertifikat eingetragen ist.

Verfügen Sie noch nicht über einen Outlook-Account, kontaktieren Sie bitte Ihren Workstation- bzw. Computer-Betreuer. Für Benutzer von Mail-Accounts, die nicht von Microsoft oder Google verwaltet werden findet sich im Abschnitt ⇒ 6 Einrichten Outlook 2016 - E-Mail-Account (p39) eine Installationshilfe (am Beispiel des GLOBALTRUST-Mailserver).

Hinweis!

Dieser Abschnitt beschreibt das Einrichten eines Software-Zertifikates, sollten Sie Zertifikate auf Smartcard oder Token verwenden, kontaktieren Sie bitte GLOBALTRUST.

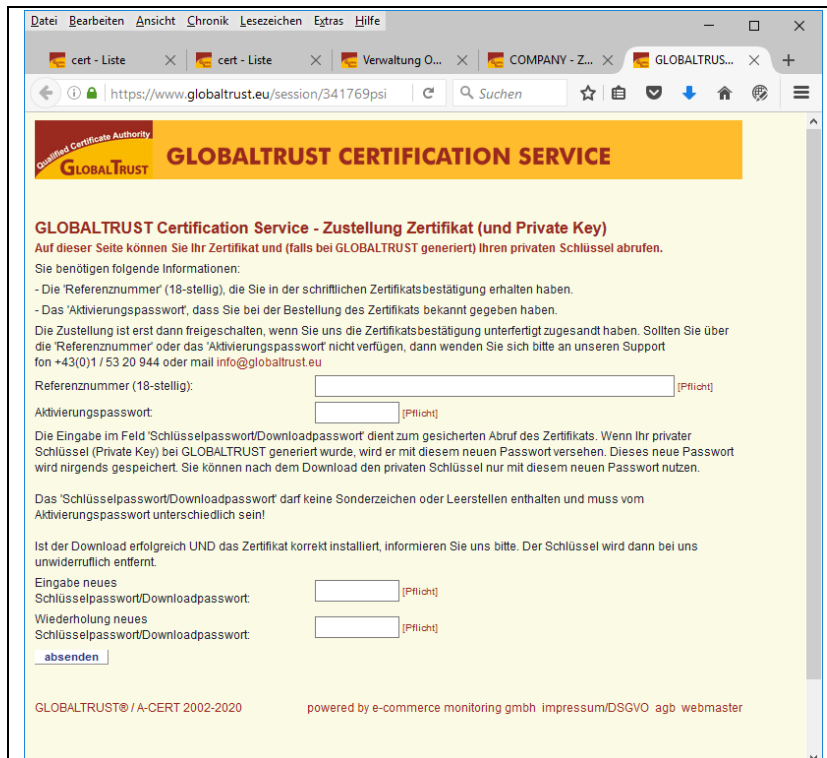
3.1 BESCHAFFUNG DER PKCS#12-DATEI

Je nach Vereinbarung mit GLOBALTRUST und seinen Partnern existieren verschiedene Methoden der Zustellung der PKCS12-Datei.

Die häufigste Methode ist der Download der PKCS12-Datei von der GLOBALTRUS-Website (den Link dazu finden Sie in den zugestellten GLOBALTRUST-Unterlagen).

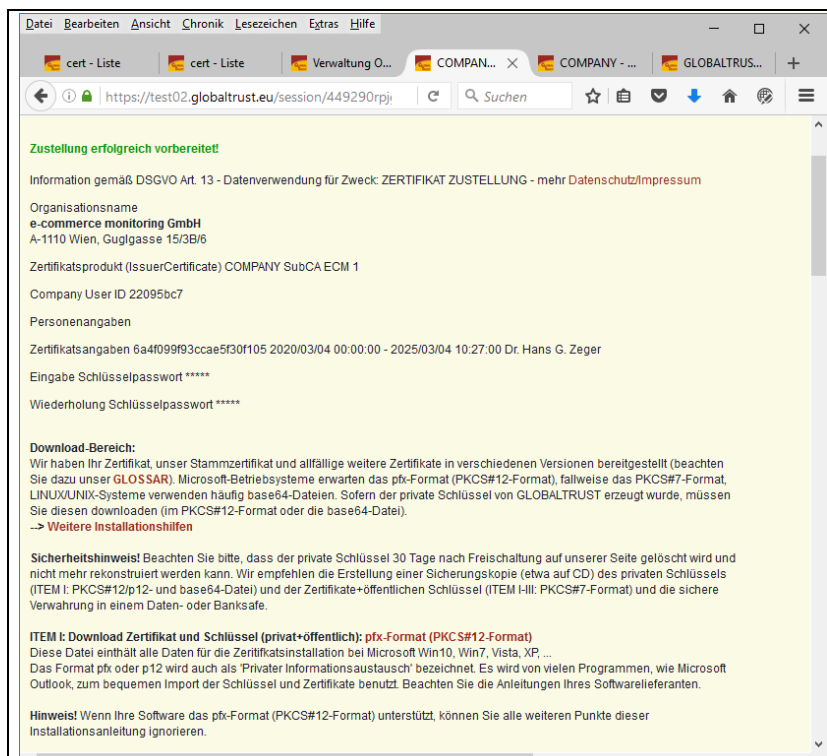
Erforderliche Daten für den Download:

- Referenznummer (18-stellig): wird per Post oder E-Mail zugestellt
- Aktivierungspasswort: wurde vom Kunden bei der Bestellung vergeben (alphanummerische Zeichen sind erlaubt, keine Sonderzeichen)
- ein vom Kunden frei vergebenes Schlüsselpasswort: dieses Passwort schützt die PKCS12-Datei beim Transport und wird bei der Installation in der Zertifikatsverwaltung benötigt



The screenshot shows a web browser window with the URL <https://www.globaltrust.eu/session/341769psi>. The page title is "GLOBALTRUST CERTIFICATION SERVICE". The main heading is "GLOBALTRUST Certification Service - Zustellung Zertifikat (und Private Key)". Below this, there is a paragraph explaining the process and a list of required information: the 18-digit reference number and the activation password. The form includes input fields for the reference number and activation password, both marked as mandatory. There is also a section for a new download password, which must be different from the activation password and not contain special characters or spaces. The form has an "absenden" button. At the bottom, it says "GLOBALTRUST® / A-CERT 2002-2020" and "powered by e-commerce monitoring gmbh".

Screen 1: GLOBALTRUST Einstiegsmaske für Download PKCS12-Datei



The screenshot shows a web browser window with the URL <https://test02.globaltrust.eu/session/449290rpji>. The page title is "Zustellung erfolgreich vorbereitet!". Below this, there is a paragraph explaining the process and a list of required information: the 18-digit reference number and the activation password. The form includes input fields for the reference number and activation password, both marked as mandatory. There is also a section for a new download password, which must be different from the activation password and not contain special characters or spaces. The form has an "absenden" button. At the bottom, it says "GLOBALTRUST® / A-CERT 2002-2020" and "powered by e-commerce monitoring gmbh".

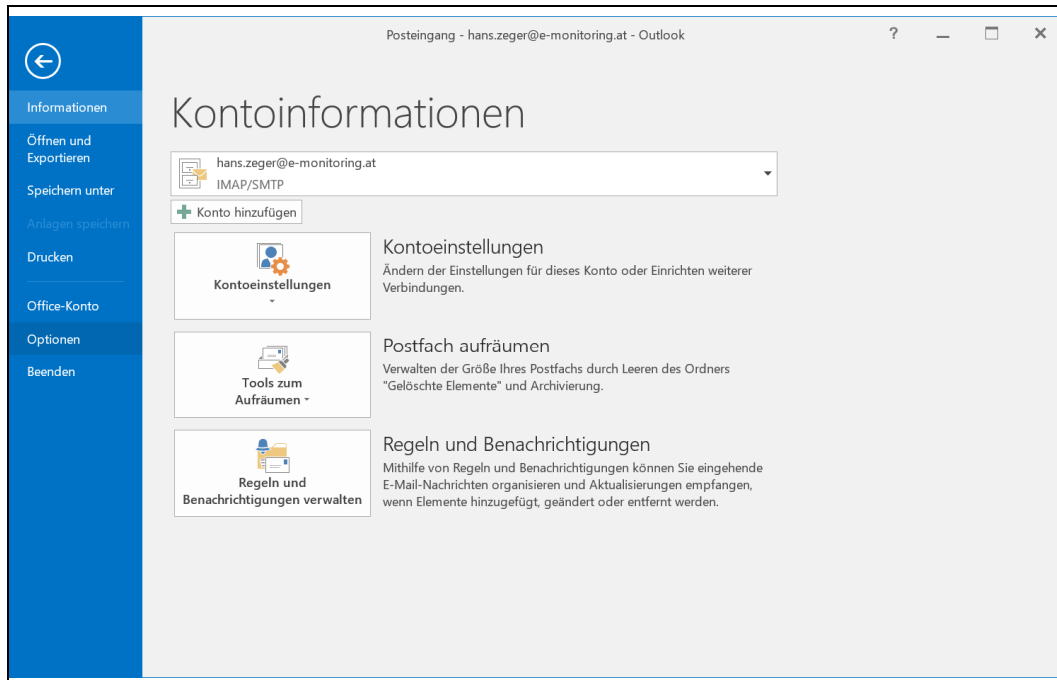
Screen 2: Download PKCS12 Datei

Download der PKCS12-Datei durch Doppelklick auf Link "**pfx-Format (PKCS#12-Format)**"

Die PKCS12-Datei ist an einem geeigneten Speicherort für die spätere Installation in Outlook abzulegen. Alle anderen Downloadoptionen können im Fall von Microsoft Outlook ignoriert werden.

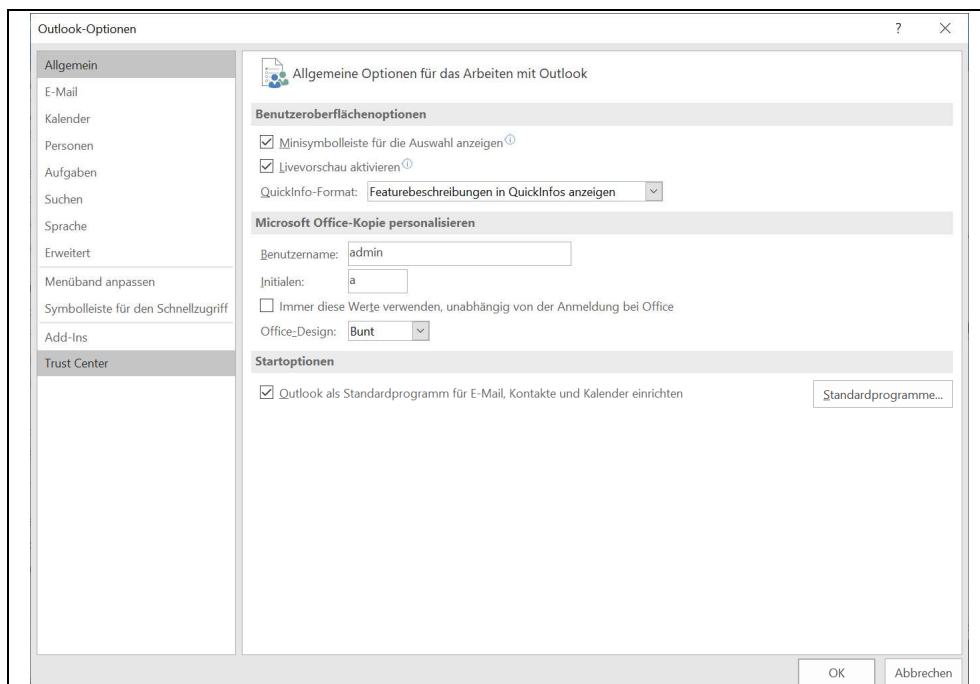
3.2 INSTALLATION PKCS#12-DATEI IN OUTLOOK 2016

Öffnen Outlook 2016 ⇒ Datei ⇒



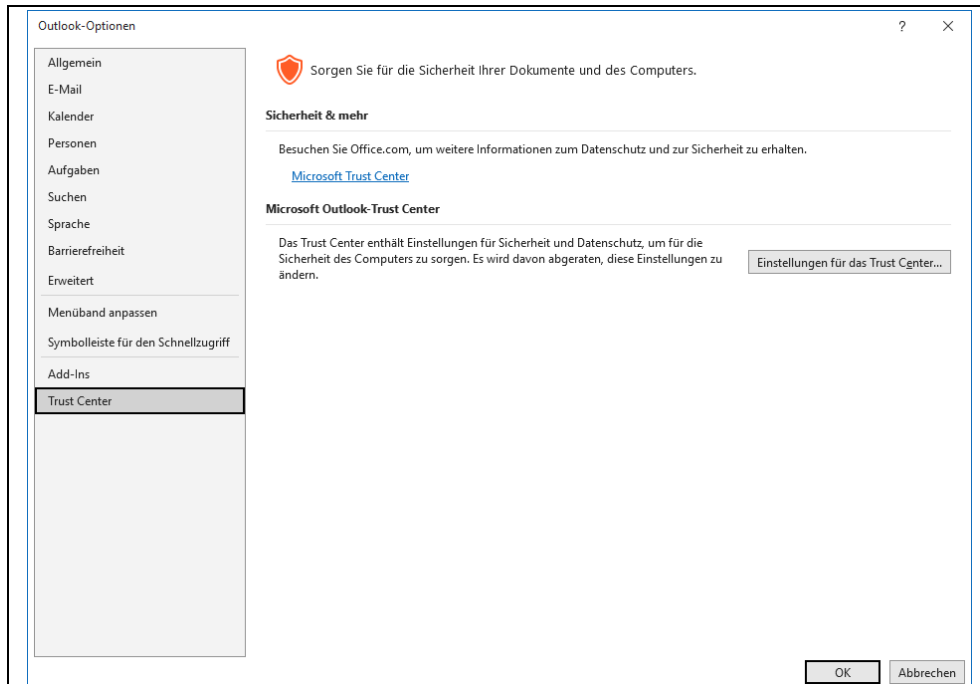
Screen 3: Öffnen Outlook 2016 Datei-Übersicht

Optionen ⇒



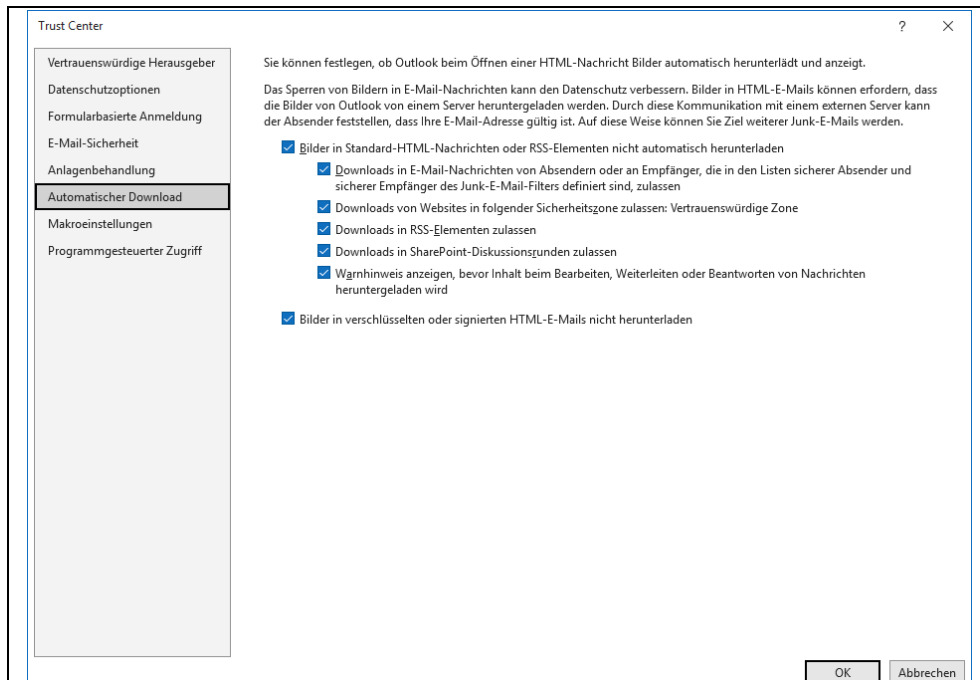
Screen 4: Übersicht Optionen

Trust Center ⇨



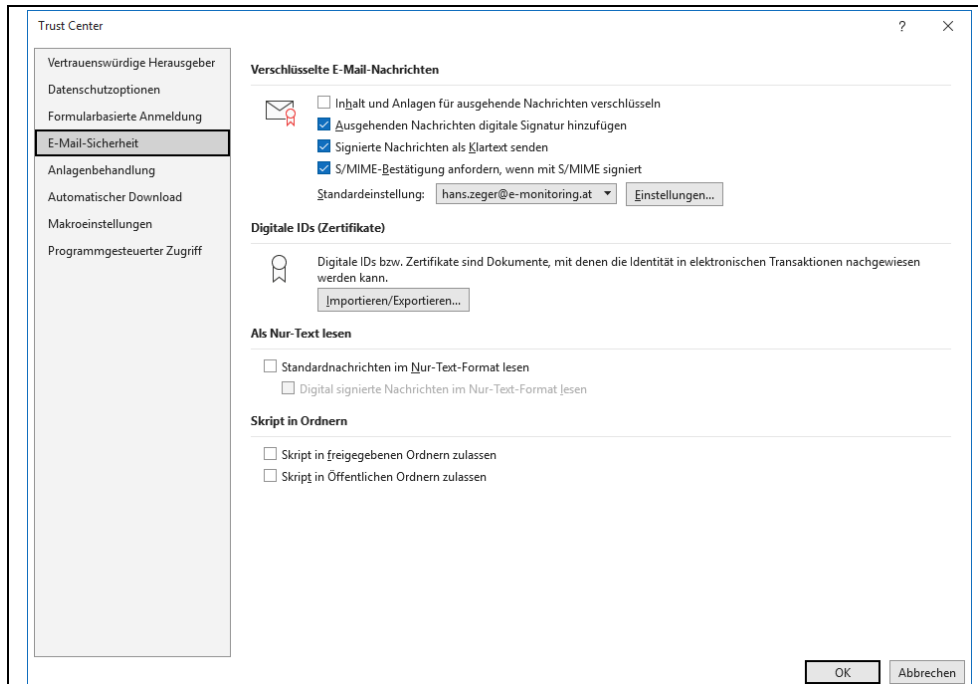
Screen 5: Übersicht Trust Center

Einstellungen für das Trust Center... ⇨



Screen 6: Übersicht Trust Center II

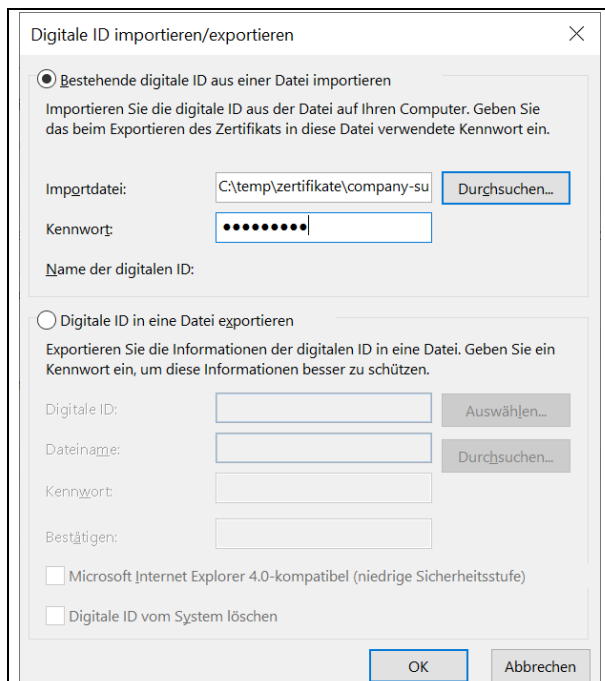
E-Mail-Sicherheit ⇨



Screen 7: Übersicht E-Mail Sicherheit

Digitale IDs (Zertifikate) Importieren

Importieren/Exportieren... ⇨



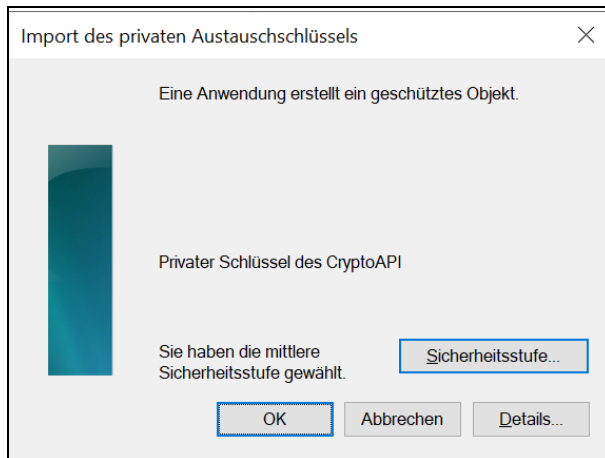
Screen 8: Importmenü für PKCS12-Datei

Importdatei: hier ist die gespeicherte PKCS12-Datei einzutragen

Kennwort: hier ist das Kennwort, dass beim Download der PKCS12-Datei vergeben wurde einzutragen

OK ⇒

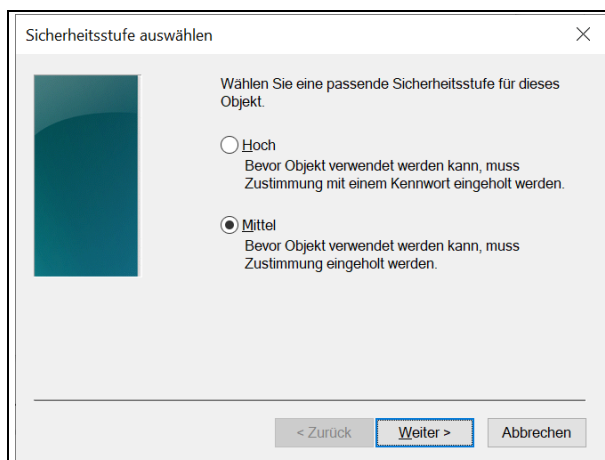
Informationsdialog zu den Sicherheitseinstellungen



Screen 9: Sicherheitsstufe

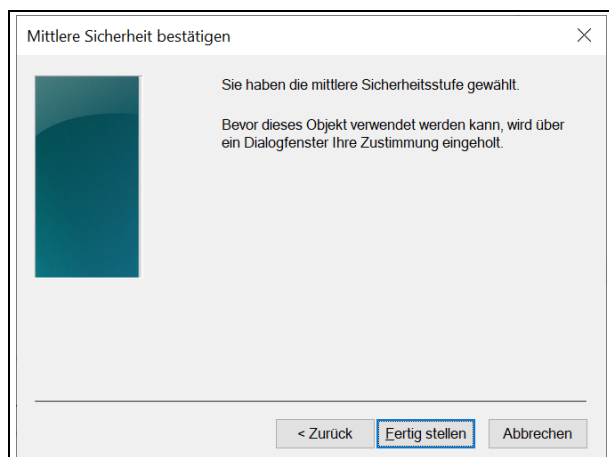
Sicherheitsstufe ⇒

Empfohlen wird mittlere Sicherheitsstufe, aus betriebsinternen Gründen kann auch "Hoch" gewählt werden, bei Unklarheiten kontaktieren Sie Ihren IT-Betreuer.



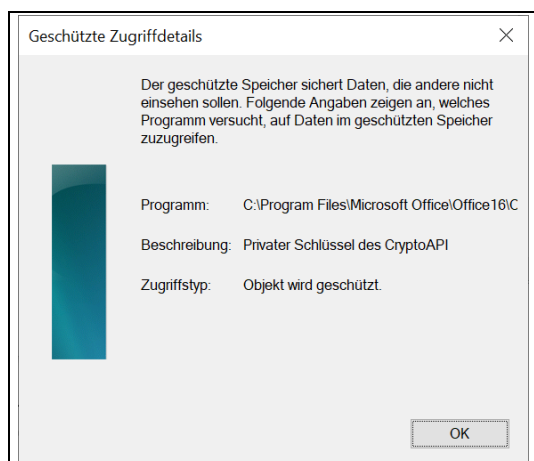
Screen 10: Anzeige der Sicherheitsstufe I

Weiter ⇨



Screen 11: Anzeige der Sicherheitsstufe II

Fertig stellen ⇨

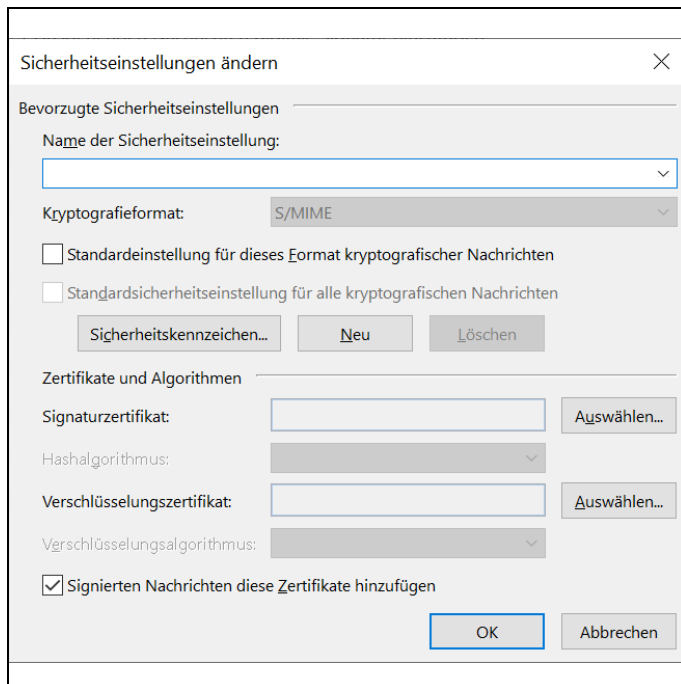


Screen 12: Details zur Sicherheitsstufe mittel

OK ⇨

Damit das Zertifikat tatsächlich genutzt werden kann müssen die Einstellungen zum E-Mail-Konto konfiguriert werden.

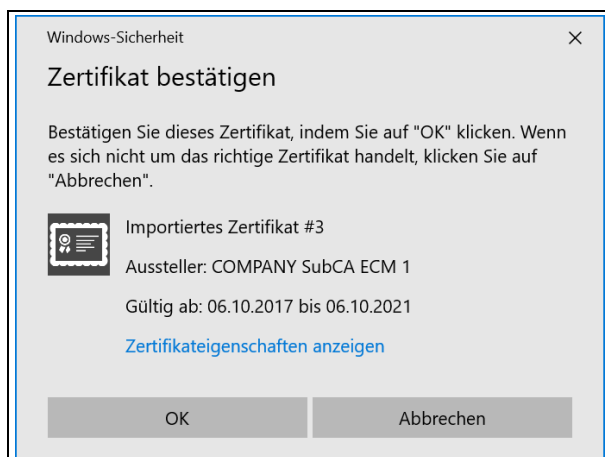
Optionen ⇒ Trust Center ⇒ E-Mail-Konto ⇒ Einstellungen... ⇒



Screen 13: Sicherheits-einstellungen ändern

- **Name der Sicherheits-einstellung:** Es können zu jedem E-Mail-Konto unterschiedliche Zertifikate gewählt werden, es wird empfohlen den Namen der Sicherheits-einstellung mit der zugeordneten E-Mail-Adresse zu bezeichnen.
- **Signaturzertifikat:** es ist das gewünschte aus dem Zertifikatsspeicher auszuwählen, ist nur eines eingetragen, kann nur dieses ausgewählt werden
- **Hash-Algorithmus:** es ist mindestens SHA256 einzutragen (kann erst nach ausgewähltem Signaturzertifikat eingetragen werden)
- **Verschlüsselungszertifikat:** ist in der Regel ident zum Signaturzertifikat
- **Verschlüsselungsalgorithmus:** es kann der vorgeschlagene Algorithmus beibehalten werden

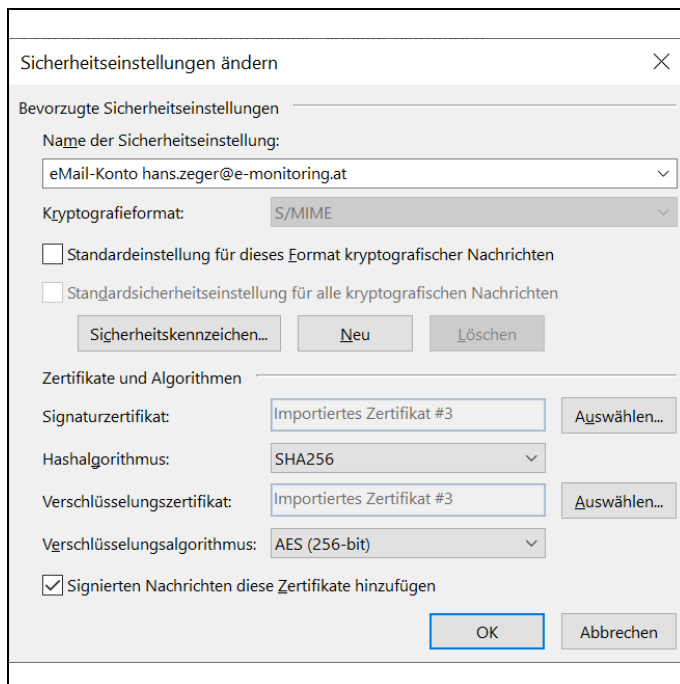
Signaturzertifikat: ⇒ Auswählen... ⇒



Screen 14: Signaturzertifikate anzeigen

Abhängig von der installierten Anzahl wird entweder ein Zertifikat angezeigt oder das erste Zertifikat + der Möglichkeit mittels Optionen andere auszuwählen.

geeignetes Sicherheitszertifikat auswählen ⇒ OK ⇒



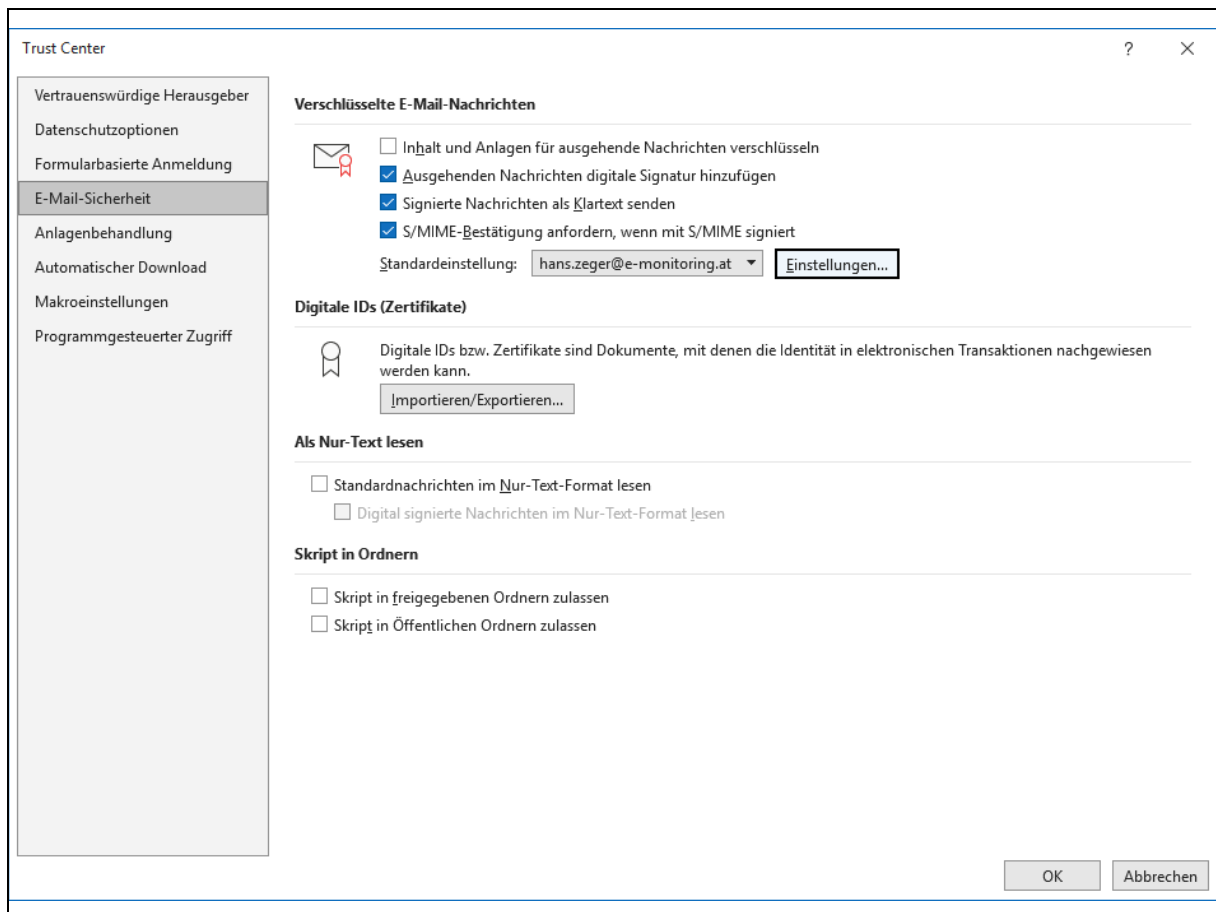
Screen 15: empfohlene Sicherheitseinstellungen nach Übernahme des Zertifikates

OK ⇒

Im Menu können unter "**Verschlüsselte E-Mail-Nachrichten**" zusätzliche Konfigurationen gesetzt werden

optionale Konfigurationsmaßnahmen

- ☐ **Inhalt und Anlagen für ausgehende Nachrichten verschlüsseln:** ist diese Option ausgewählt, wird per Default JEDES E-Mail verschlüsselt. Diese Option ist nur sinnvoll, wenn man von den meisten E-Mail-Empfängern ebenfalls das Zertifikat im Outlook-Adressbuch eingetragen hat oder mittels LDAP abrufen kann (⇒ 4.3.2 Fall 2: Empfänger in LDAP-Server suchen p27).
Empfehlung: NICHT anhacken
- ☒ **Ausgehenden Nachrichten digitale Signatur hinzufügen:** ist diese Option ausgewählt, wird per Default JEDES E-Mail signiert, das lästige Auswählen im Einzelfall entfällt
Empfehlung: anhacken
- ☒ **Signierte Nachrichten als Klartext senden:**
Empfehlung: anhacken
- ☒ **S/MIME Bestätigung anfordern:** ist diese Option ausgewählt, wird bei jedem verschickten Mail der Empfänger gefragt, ob Sie eine Prüfbestätigung erhalten sollen
Empfehlung: anhacken



Screen 16: Konfiguration der E-Mail Sicherheit

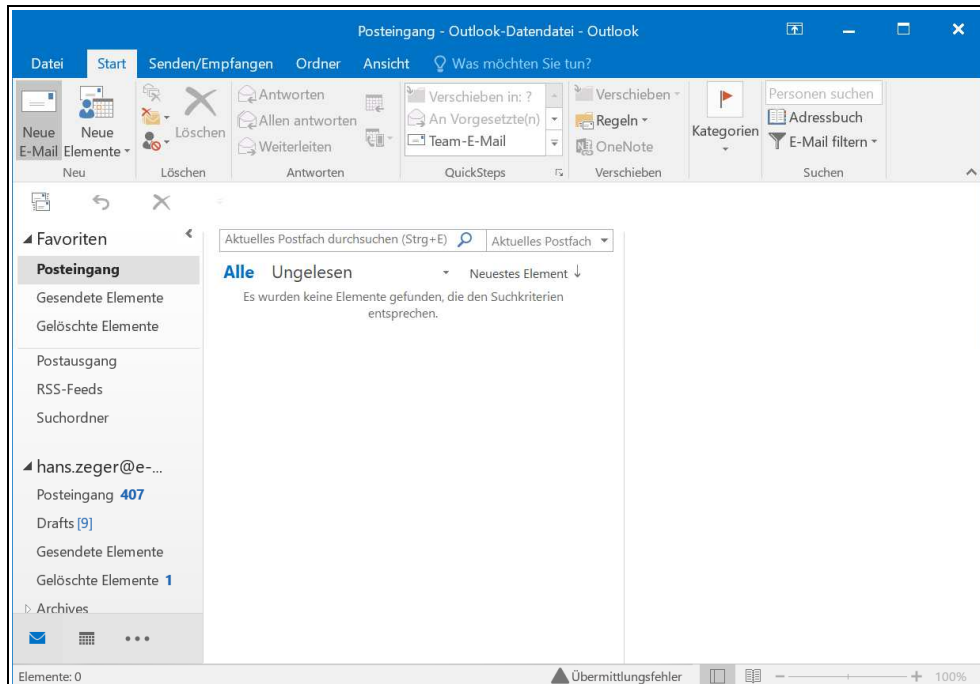
OK ⇒ OK ⇒

Outlook ist zur Signatur und Verschlüsselung von E-Mails konfiguriert.

4 GLOBALTRUST-ZERTIFIKATE IN OUTLOOK 2016 NUTZEN

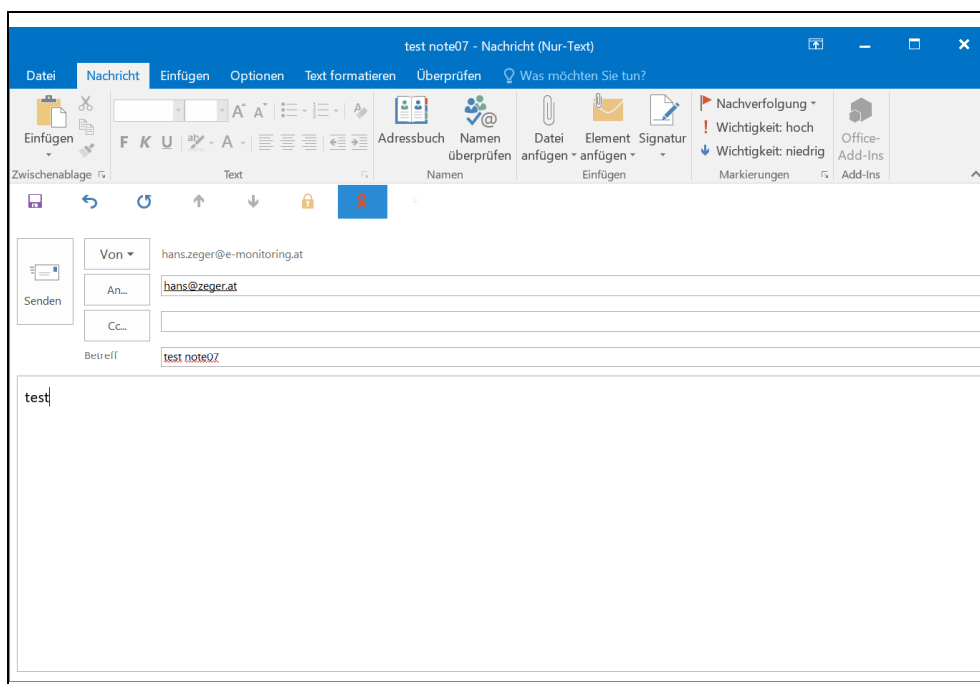
4.1 MAIL SIGNIERT VERSENDEN

Öffnen Outlook 2016 ⇒



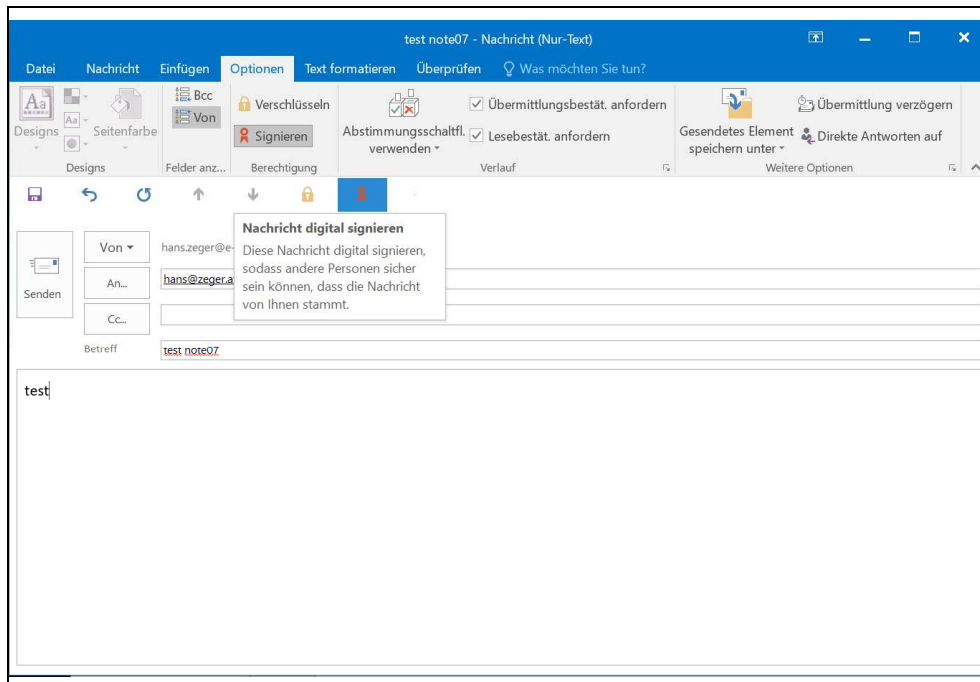
Screen 17: Outlook 2016 Einstiegsseite

Neue E-Mail ⇒ wie gewohnt E-Mail verfassen ⇒



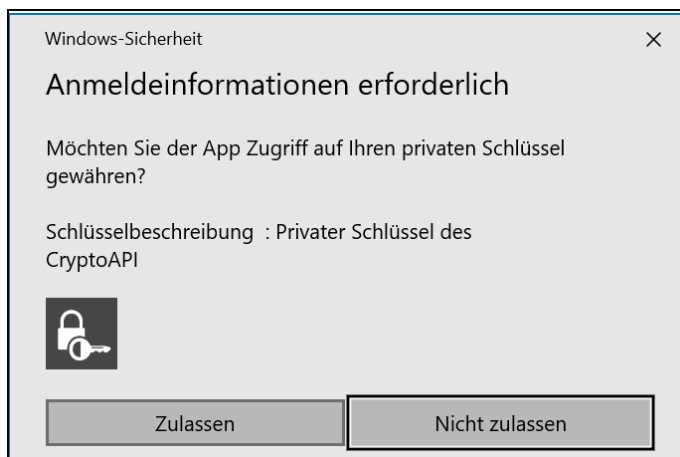
Screen 18: Outlook E-Mail versenden

Optionen ⇒ Signieren auswählen ⇒
(kann auch voreingestellt sein ⇒ siehe optionale Konfigurationsmaßnahmen, p14)



Screen 19: Outlook E-Mail versenden II

Nachricht versenden ⇒ Senden ⇒



Screen 20: Bestätigung Nutzung Zertifikat

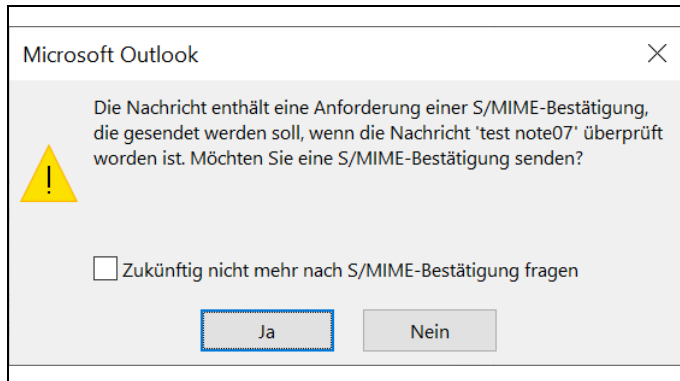
Zulassen ⇒

Hinweis!

Schlägt der e-Mail-Versand fehl ⇒ 7 Troubleshooting Outlook 2016 (p49)

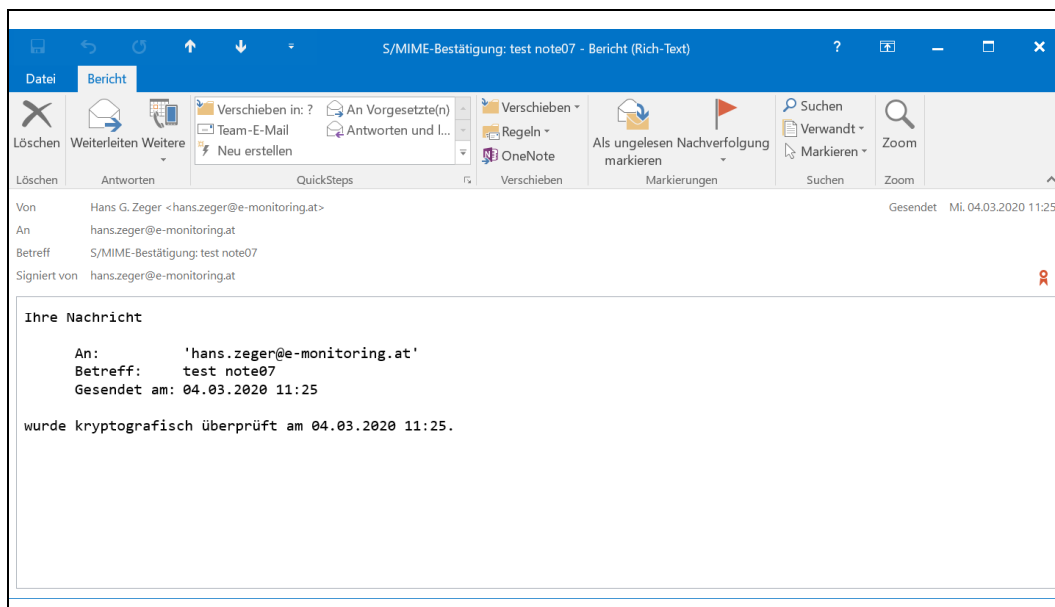
4.2 SIGNIERTES MAIL PRÜFEN

Abhängig von den Einstellungen des Absenders (⇒ siehe optionale Konfigurationsmaßnahmen, p14) kann beim Öffnen folgende Nachricht erscheinen:




Screen 21: Nachfrage S/MIME Bestätigung

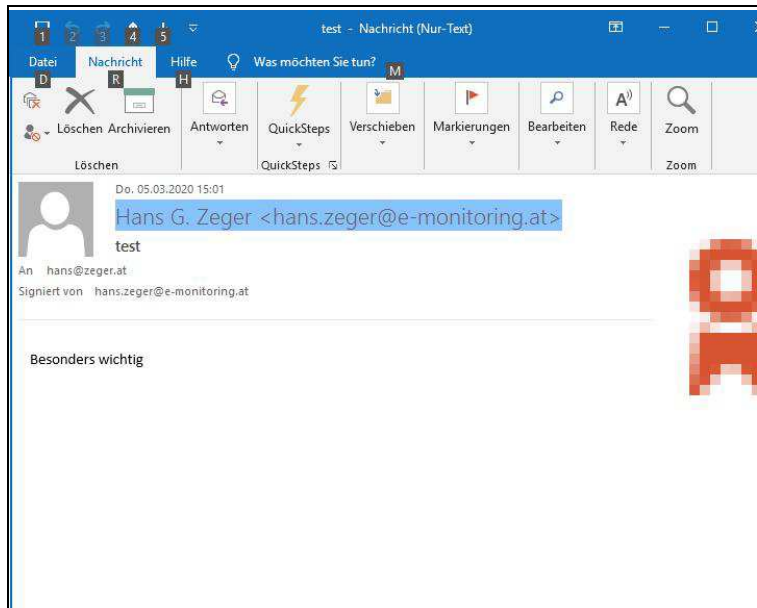
Wird die Option "Ja" gewählt, erhält der Absender eine Benachrichtigung dieser Art



Screen 22: Nachricht auf Grund S/MIME Bestätigung

Ansonsten unterscheidet sich das signierte E-Mail von einem unsignierten nur durch das  Symbol.

Erscheint statt dem Siegel-Symbol ein Warnzeichen ⇒ 7 Troubleshooting Outlook 2016 (p49)



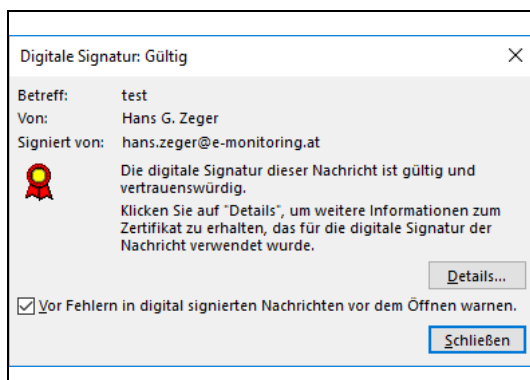
Screen 23: signierte Nachricht (Signatursymbol wurde vergrößert)

Hinweis!

Der nachfolgende Abschnitt beschreibt die verschiedenen Meldungen von Outlook zum Zertifikat. Im Regelfall ist **keine** detaillierte Prüfung erforderlich, der Empfänger einer signierten Nachricht kann jedoch auf diesen Weg Details zur Gültigkeit einer Signatur erfahren

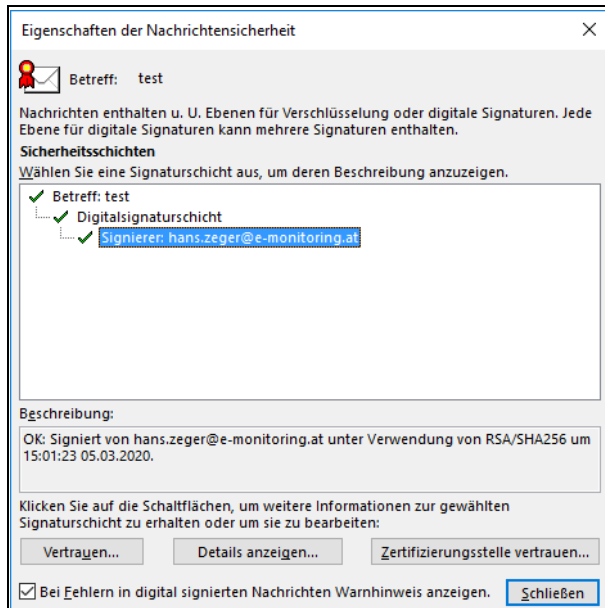
Prüfen des Absenders

Doppelklick auf Signatursymbol ⇒



Screen 24: Signaturprüfung I

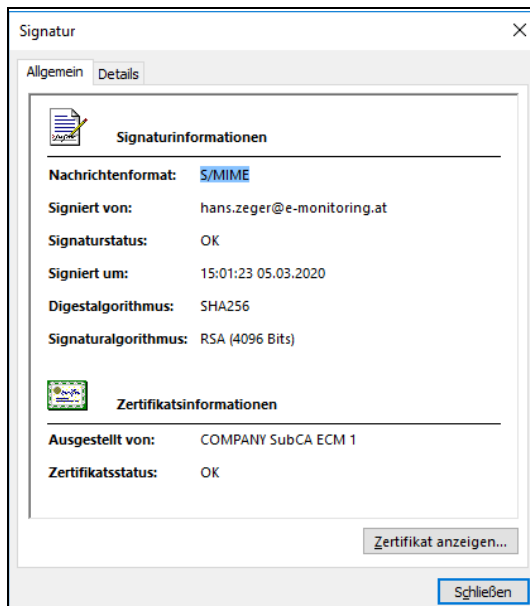
Details... ⇨



Screen 25: Signaturprüfung II

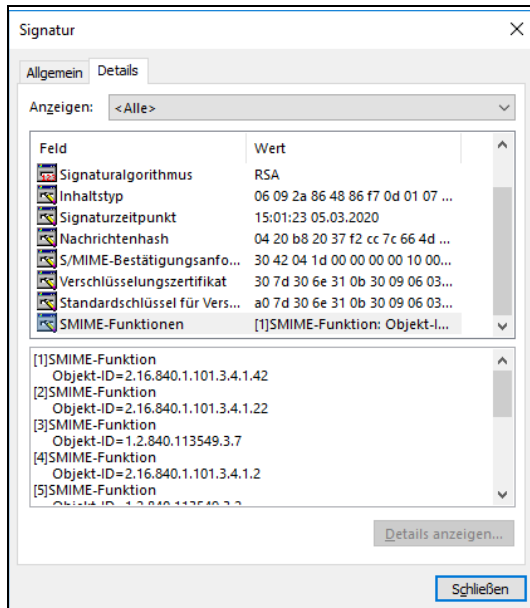
Wird "Signierer" ausgewählt, dann können erweiterte Signaturdaten aufgerufen werden

Signierer ⇨ Details anzeigen ⇨ Reiter "Allgemein" ⇨



Screen 26: Signaturprüfung III

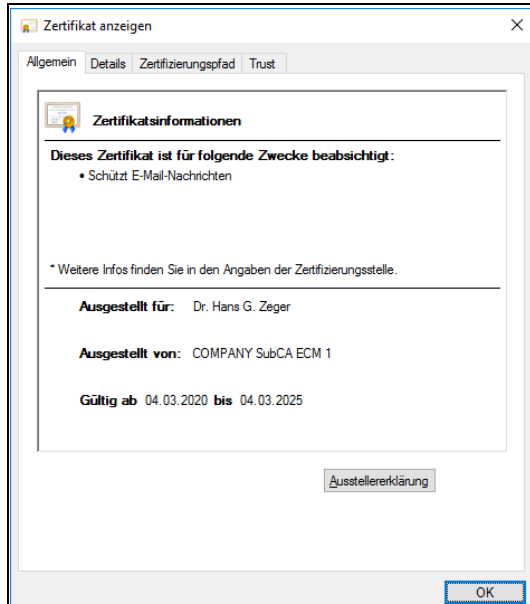
Reiter "Details" ⇒



Screen 27: Signaturprüfung IV

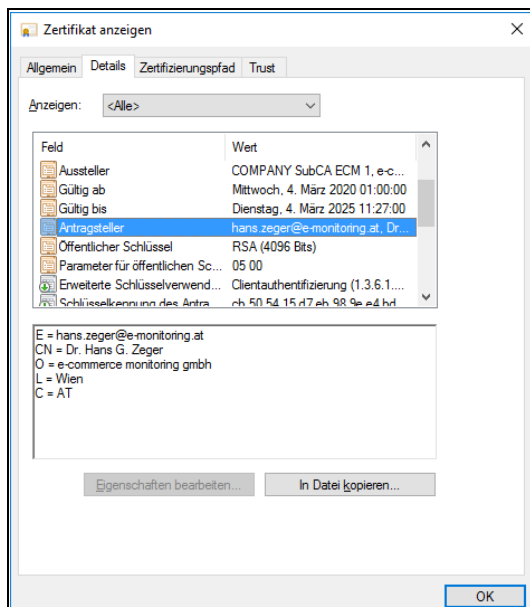
Details zum Zertifikat

unter Reiter "Allgemein" ⇒ Zertifikat anzeigen... ⇒ Reiter "Allgemein" ⇒



Screen 28: Signaturprüfung V

Reiter "Details" ⇒ Auswahl "Antragsteller" ⇒ zeigt die Person an, für die Zertifikat ausgestellt wurde
GLOBALTRUST übernimmt die Verantwortung, dass die Identität dieser Person sorgfältig geprüft ist¹



Screen 29: Signaturprüfung VI

Details zur Identitätsprüfung finden sich in folgenden Dokumenten:

- <http://service.globaltrust.eu/static/globaltrust-certificate-policy.pdf>
- <http://service.globaltrust.eu/static/globaltrust-certificate-practice-statement.pdf>

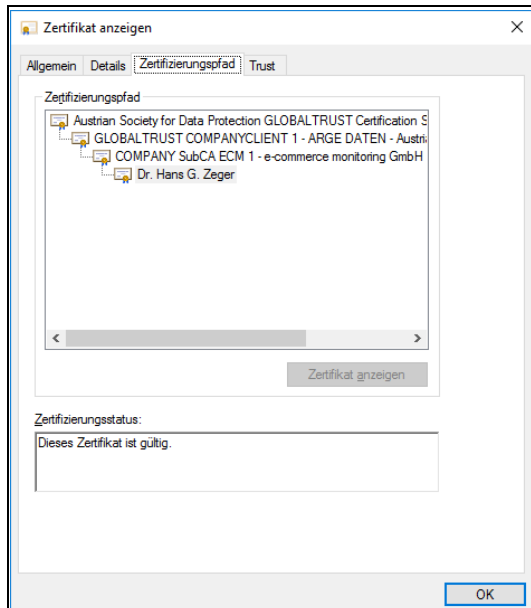
Eine Übersicht zur Policy von GLOBALTRUST und den verwendeten CAs findet sich unter:

- <http://www.globaltrust.eu/certificate-policy.html>
- <https://fruit.globaltrust.eu/certificate-policy/>

¹

Die Identitätsprüfung kann entweder durch GLOBALTRUST direkt erfolgt sein, durch ein Video-Ident-Verfahren, durch einen Zertifizierungspartner oder im Rahmen der COMPANY-Zertifikate durch eine bevollmächtigte Person innerhalb des angegebenen Unternehmens. Bestehen Zweifel an der Korrektheit der Angaben, dann kann sich jeder Signaturempfänger direkt an GLOBALTRUST bezüglich Auskunft zur signierenden Person wenden.

Reiter "Zertifizierungspfad" ⇨



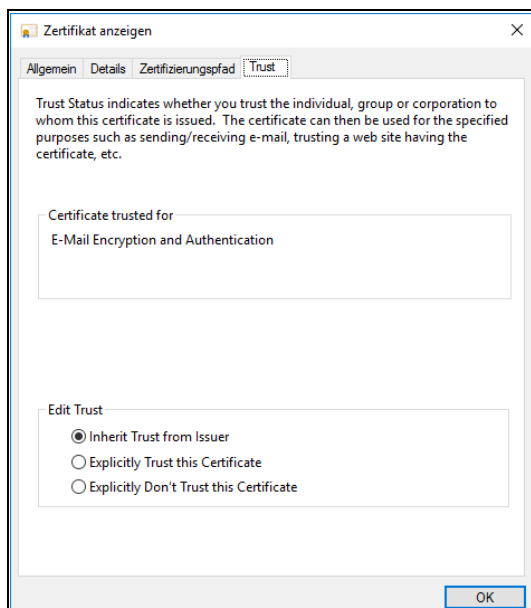
Screen 30: Signaturprüfung VII

GLOBALTRUST verwendet 3 Stammzertifikate (RootCAs):

- GLOBALTRUST 2006 (in der Regel nur als GLOBALTRUST) bezeichnet und noch unter dem Friendly Name "Austrian Society for Data Protection GLOBALTRUST" ausgestellt
- GLOBALTRUST 2015 mit Friendly Name "GLOBALTRUST 2015"
- GLOBALTRUST 2020 mit Friendly Name "GLOBALTRUST 2020" (aktiv ab Mai 2020)

Alle GLOBALTRUST-RootCAs entsprechen den Anforderungen der europäischen eIDAS-Verordnung.

Reiter "Trust" ⇨



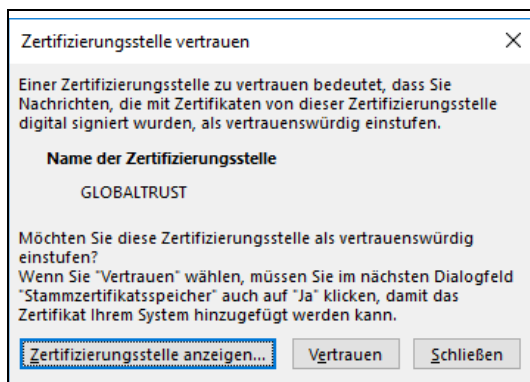
Screen 31: Signaturprüfung VIII

Hier hat der Empfänger die Möglichkeit den automatisch vorgeschlagenen Vertrauensstatus von Outlook 2016 zu "überschreiben". Dies kann sinnvoll sein, wenn ein Zertifikat als nicht vertrauenswürdig angezeigt wird, obwohl es nach individueller Prüfung des Empfängers vertrauenswürdig ist oder wenn ein Zertifikat als vertrauenswürdig angezeigt wird, obwohl der Empfänger dem Absender nicht vertraut (⇒ Abschnitt 7.1 Fehlermeldungen und Warnhinweise p49)

Bedeutung der Einstellungen:

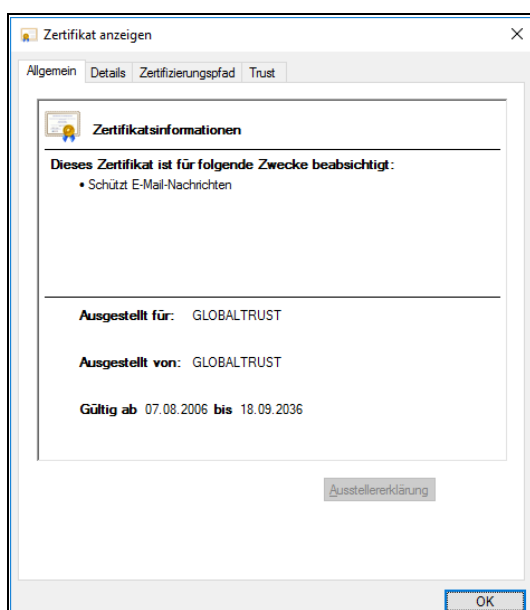
- Inherit Trust from Issuer (Standardfall): Outlook hat eine vollständige Vertrauenskette gefunden und vertraut deswegen dem Zertifikat
- Explicitly Trust this Certificate: der Benutzer vertraut dem Zertifikat, unabhängig vom Prüfergebnis von Outlook
- Explicitly Don't Trust this Certificate: der Benutzer vertraut NICHT dem Zertifikat, unabhängig vom Prüfergebnis von Outlook

Zertifizierungsstelle vertrauen... ⇒



Screen 32: Signaturprüfung IX

Zertifizierungsstelle anzeigen... ⇒



Screen 33: Signaturprüfung X

4.3 E-MAIL VERSCHLÜSSELT VERSCHICKEN

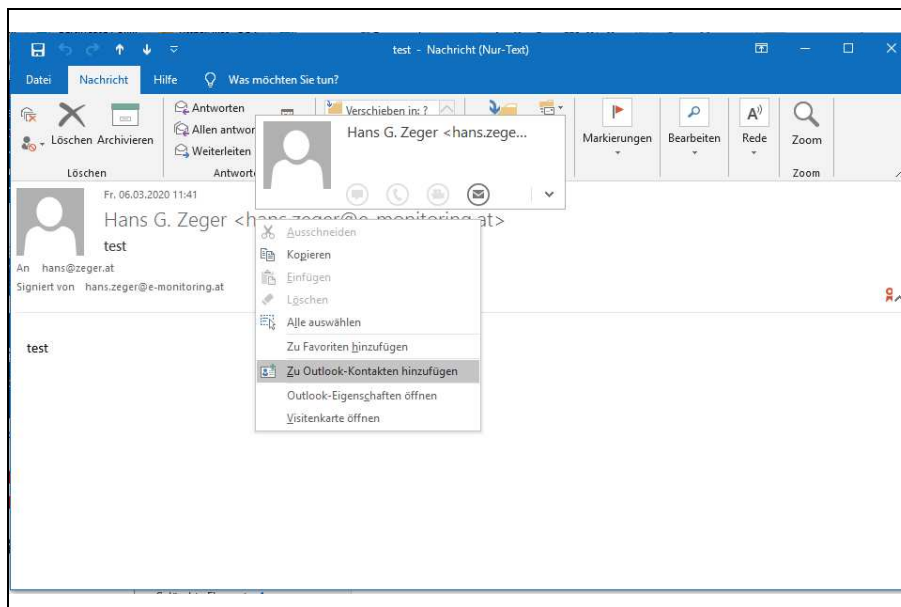
Möglichkeiten des Verschlüsseln von Nachrichten

- Fall 1: der vorgesehene Empfänger hat ein signiertes E-Mail geschickt
- Fall 2: mit dem Empfänger gibt es noch keine Kommunikation, er ist jedoch im LDAP-Verzeichnis eines Zertifizierungsanbieters eingetragen

4.3.1 FALL 1: VORGESEHENER EMPFÄNGER HAT EIN SIGNIERTES E-MAIL GESCHICKT

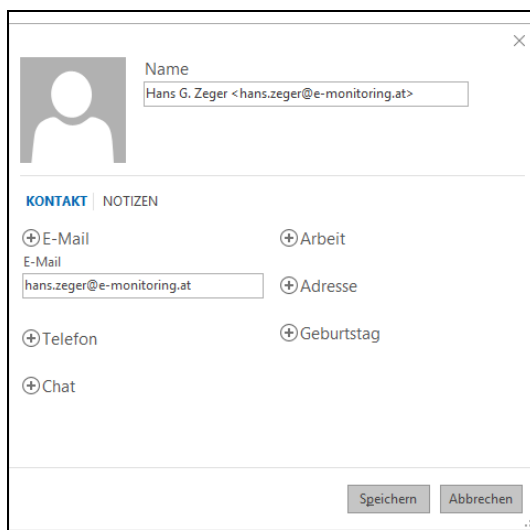
In diesem Fall ist der einfachste Weg den vorgesehenen Empfänger in das eigene Outlook-Adressbuch zu übernehmen. Dabei wird automatisch auch das Signaturzertifikat übernommen. Dieses dient zum Verschlüsseln der Nachricht.

signiertes E-Mail öffnen ⇒ Rechtsklick auf Absender ⇒



Screen 34: Signiertes E-Mail

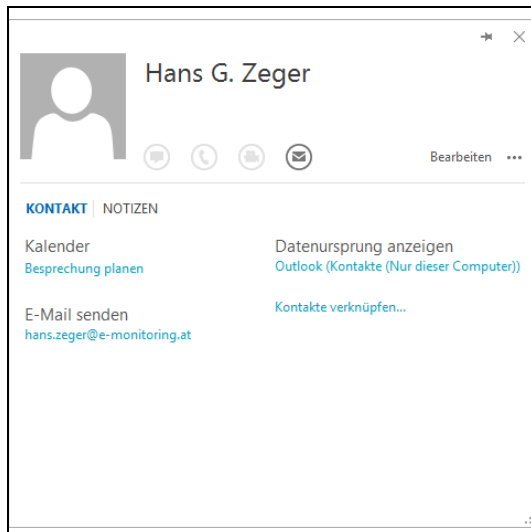
Zu Outlook-Kontakten hinzufügen ⇒



Screen 35: Übersicht Kontaktdaten eines E-Mail Empfängers

Speichern ⇒

(Optional können die vorgesehenen Outlook-Kontaktfelder ergänzt werden)



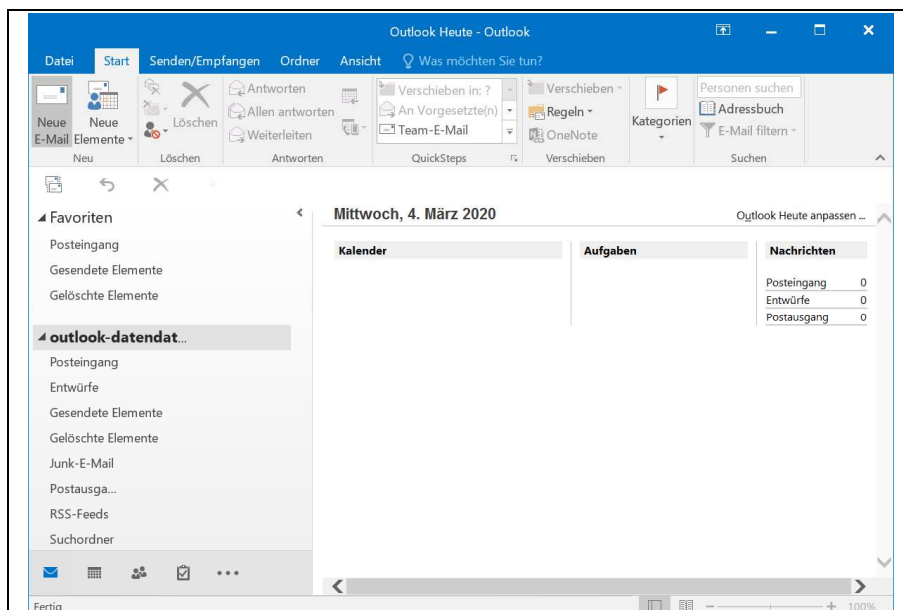
Screen 36: Übersicht Kontaktdaten eines E-Mail Empfängers II

Fenster schließen (X) ⇒

Anschließend weiter wie bei ⇒ Abschnitt 4.3.2 Fall 2: Empfänger in LDAP-Server suchen (p27), jedoch mit dem Unterschied, dass beim Adressbuch "Kontakte (nur dieser Computer)" auszuwählen ist.

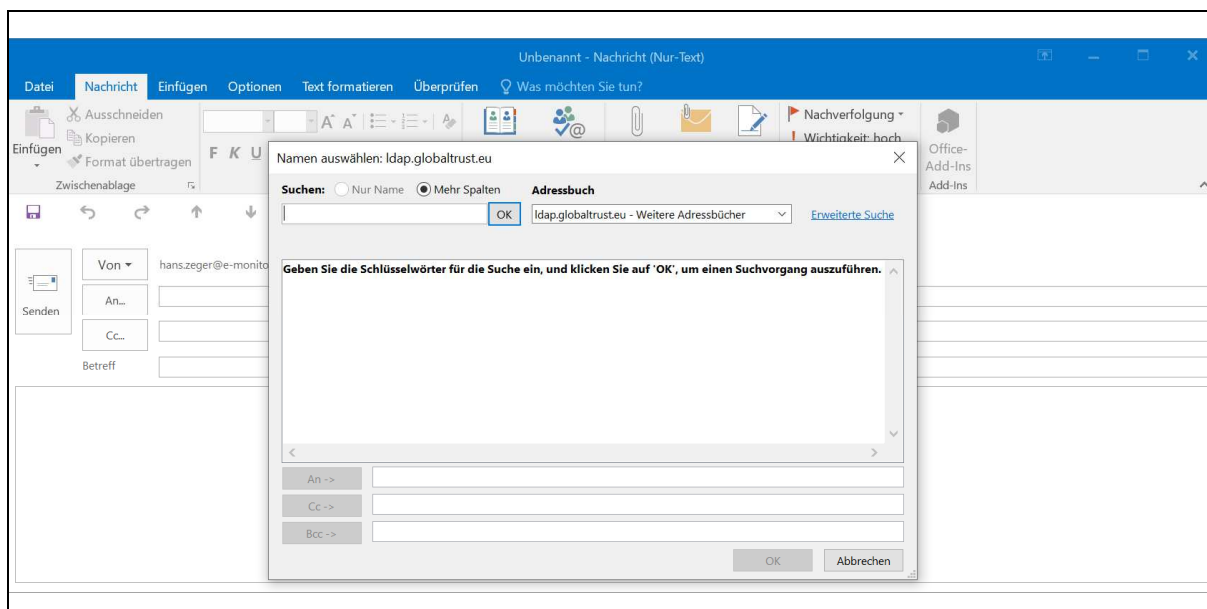
4.3.2 FALL 2: EMPFÄNGER IN LDAP-SERVER SUCHEN

Mails können an Empfänger ohne vorherige Kommunikation verschlüsselt verschickt werden, wenn der Empfänger ein öffentlich einsehbares Zertifikat hat (erfordert ⇒ Abschnitt 5 GLOBALTRUST LDAP-Server ldap.globaltrust.eu verwenden p31)



Screen 37: Outlook 2016 Einstiegsseite

Neue E-Mail ⇒ Adressbuch aufrufen ⇒



Screen 38: Outlook Adressbuch

im Feld "Adressbuch" MUSS der gewünschte LDAP-Server stehen!

Erfolgt häufig eine Suche in einem LDAP-Server, dann sollte dieser vorgereicht werden ⇒ Abschnitt 5.3 optionale Anpassung des Outlook-Adressbuches (p37)

Erweiterte Suche ⇨

Suchen

Suche

Anzeigenname: schönherr

Vorname: Nachname:

Position: Alias:

Firma: E-Mail:

Büro: Abteilung:

Telefon: Ort:

Suchkriterien

☐ Beginnt mit ☒ Enthält

OK Abbrechen

Screen 39: Mailempfänger suchen

gesuchten Empfänger eintragen ⇨ OK ⇨

Namen auswählen: ldap.globaltrust.eu

Suchen: ☐ Nur Name ☒ Mehr Spalten

Adressbuch

ldap.globaltrust.eu - Weitere Adressbücher

Erweiterte Suche

Name	E-Mail-Adresse	E-Mail-Typ	Telefon gesch...	Büro	Posit
Charlotte Schönherr	schoenherr@e-monitoring.at	SMTP			
Charlotte Schönherr	schoenherr@e-monitoring.at	SMTP			
Charlotte Schönherr	schoenherr@e-monitoring.at	SMTP			

An -> Charlotte Schönherr

Cc ->

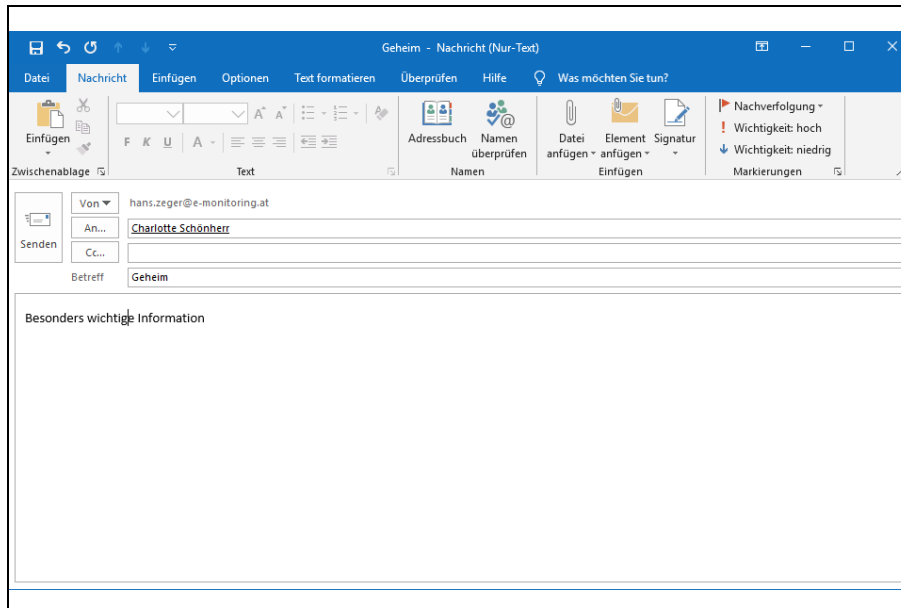
Bcc ->

OK Abbrechen

Screen 40: Liste der gefundenen Empfänger

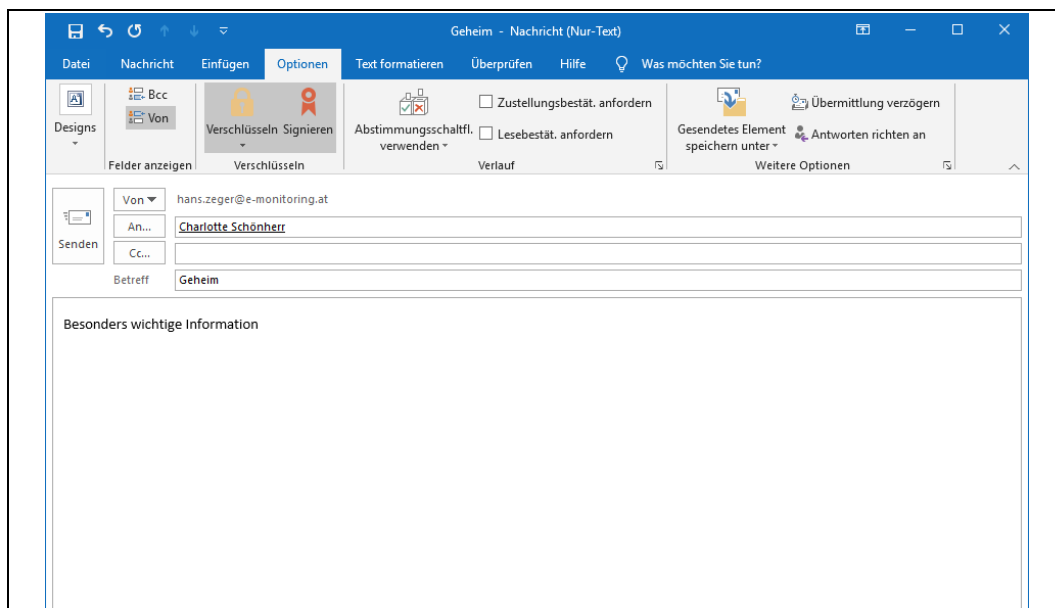
gewünschten Empfänger auswählen ⇨ Doppelklick ⇨ OK ⇨

E-Mail wie gewohnt verfassen



Screen 41: E-Mail schreiben

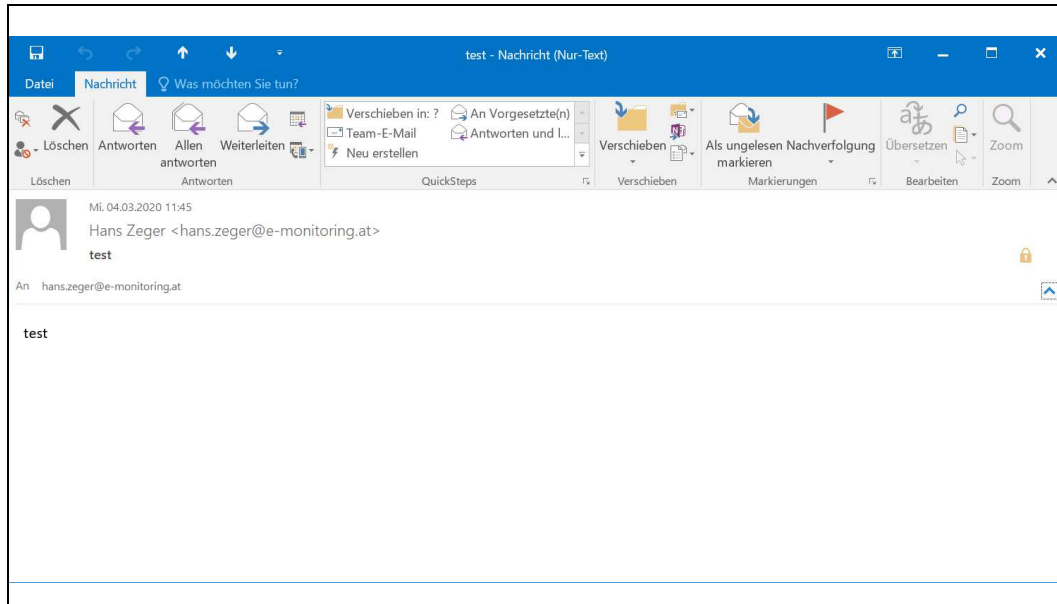
Optionen ⇒ Verschlüsseln auswählen (kann auch voreingestellt sein ⇒ optionale Konfigurationsmaßnahmen, p14)



Screen 42: Mail mit Optionen eigene Signatur + Verschlüsseln mit Schlüssel des Empfängers

Senden ⇨

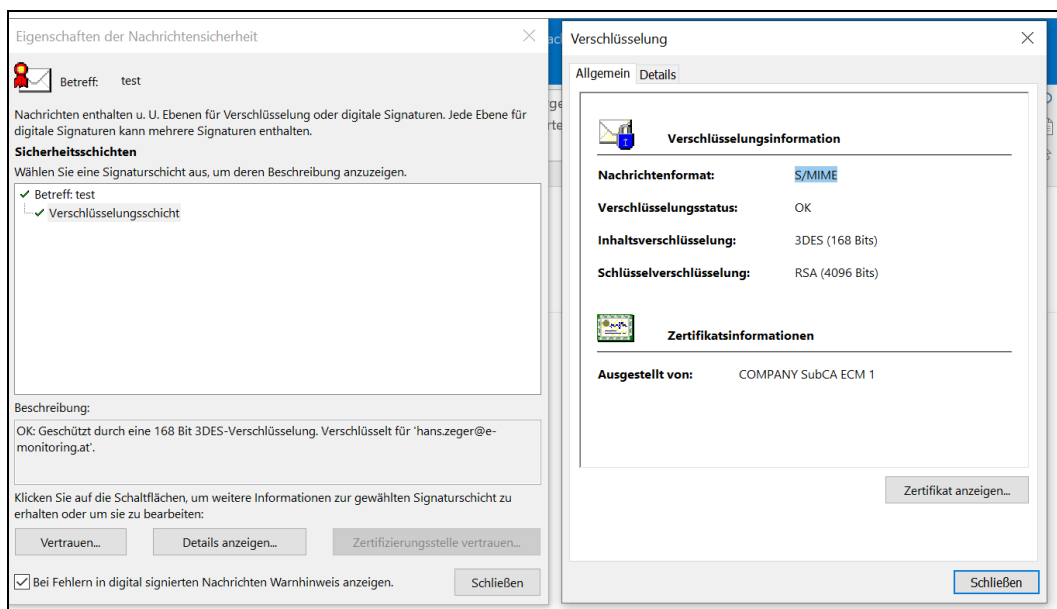
Beim berechtigten Empfänger wird die Nachricht - je nach Mailprogramm - automatisch oder nicht automatisch entschlüsselt. Outlook 2016 entschlüsselt automatisch.



Screen 43: Anzeige Nachricht beim Empfänger

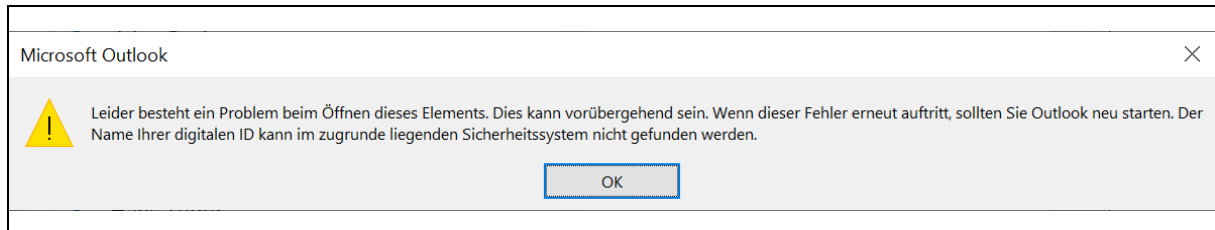
Details zur Verschlüsselung

Schloß-Symbol ⇨ Doppelklick ⇨ Details anzeigen ⇨



Screen 44: Detailinformationen zur Verschlüsselung

Fehlermeldung wenn verschlüsselte Information an falschen Empfänger kommt ⇨



Screen 45: Fehlermeldung von Outlook 2016 bei Versuch eine verschlüsselte Nachricht zu öffnen, die für jemanden anderen bestimmt ist

5 GLOBALTRUST LDAP-SERVER LDAP.GLOBALTRUST.EU VERWENDEN

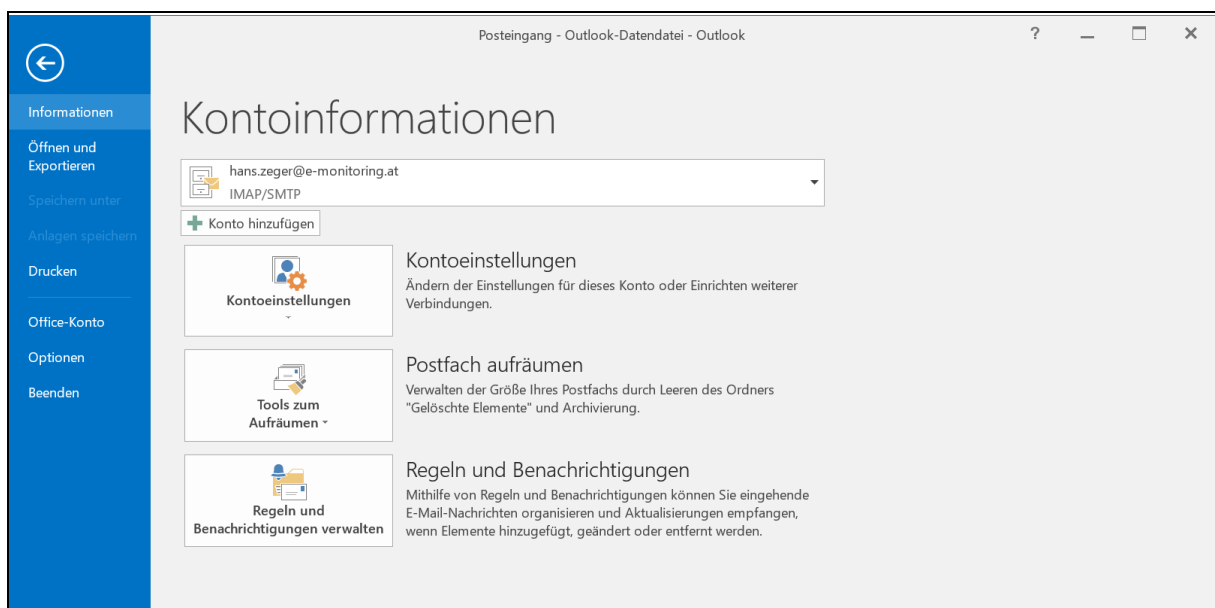
Mit Hilfe des GLOBALTRUST-LDAP-Servers können auch die Zertifikate anderer E-Mail-Nutzer downgeloadet werden.

5.1 LDAP-SERVER LDAP.GLOBALTRUST.EU EINRICHTEN

Hinweis!

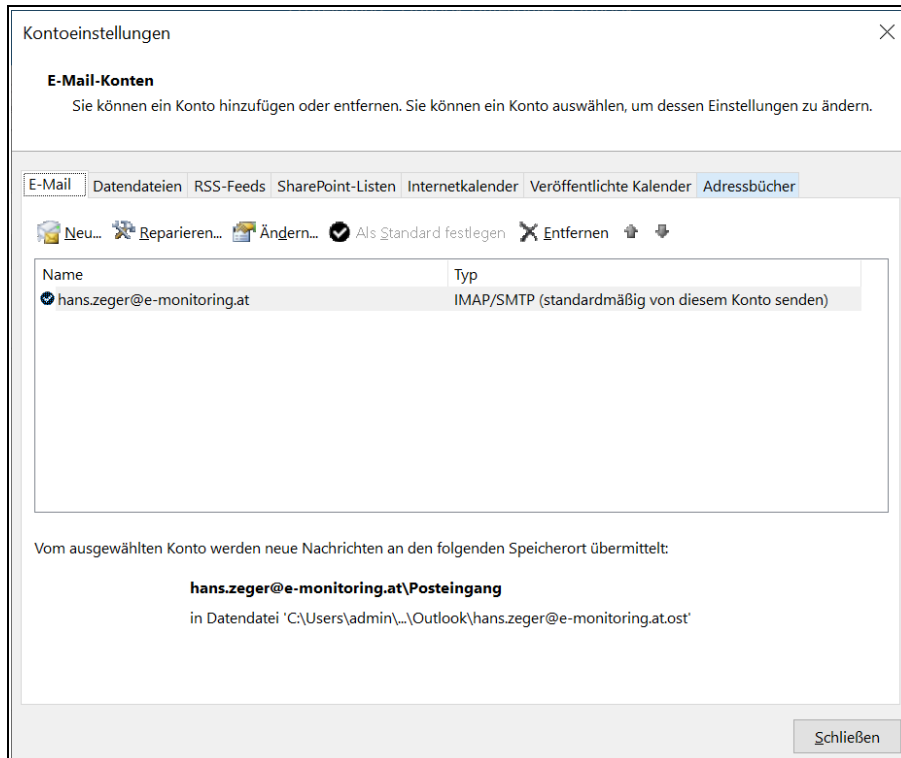
Die vorliegende LDAP-Konfiguration ist für den GLOBALTRUST-LDAP-Server optimiert. Es können hier nur von GLOBALTRUST ausgegebene Zertifikate und Mailadressen gesucht werden. Es kann erforderlich sein weitere LDAP-Server zusätzlich zu installieren.

Datei ⇨



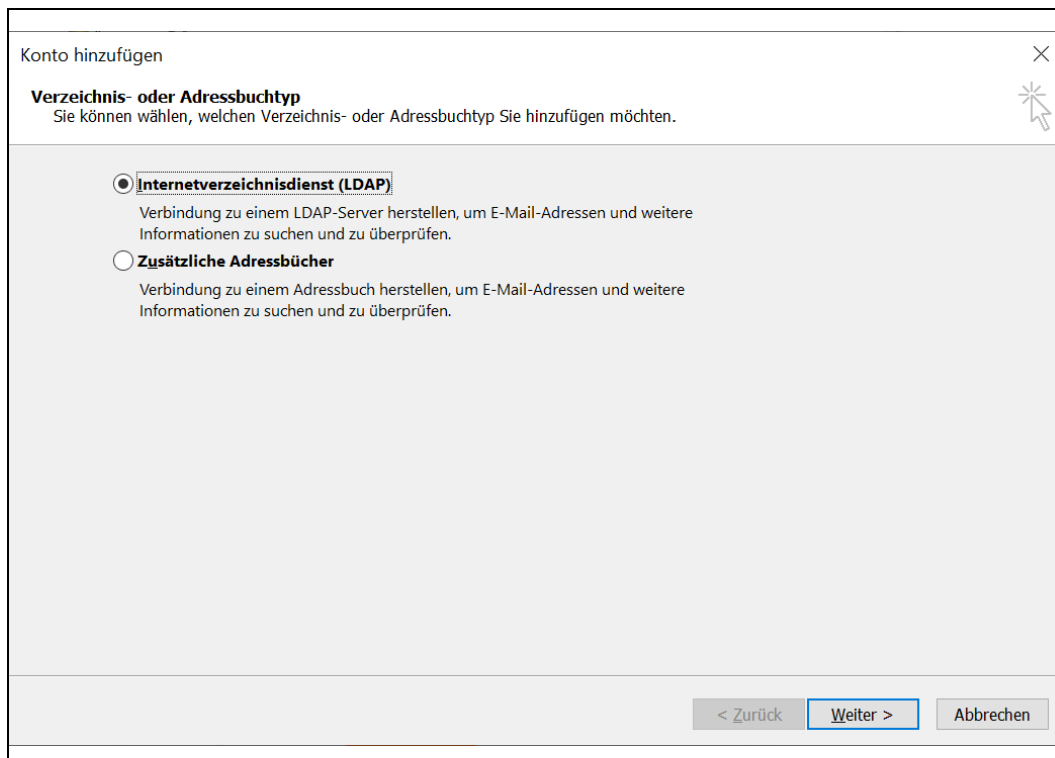
Screen 46: Kontoinformationen anzeigen

Konteneinstellungen ⇨



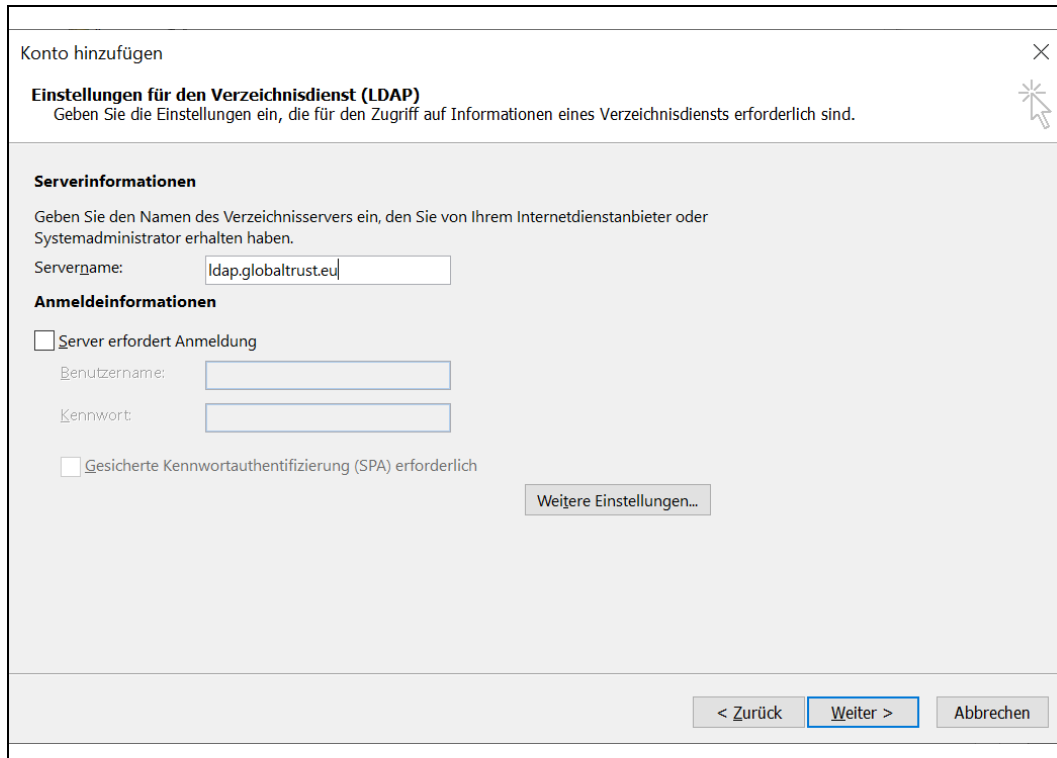
Screen 47: Konteneinstellungen anzeigen

Adressbücher ⇨ Neu ⇨



Screen 48: Auswahl Adressbuch

Internetverzeichnisdienst (LDAP) ⇒ Weiter ⇒



Konto hinzufügen

Einstellungen für den Verzeichnisdienst (LDAP)
Geben Sie die Einstellungen ein, die für den Zugriff auf Informationen eines Verzeichnisdiensts erforderlich sind.

Serverinformationen
Geben Sie den Namen des Verzeichnisservers ein, den Sie von Ihrem Internetdienstanbieter oder Systemadministrator erhalten haben.

Servername:

Anmeldeinformationen

☒ Server erfordert Anmeldung

Benutzername:

Kennwort:

☐ Gesicherte Kennwortauthentifizierung (SPA) erforderlich

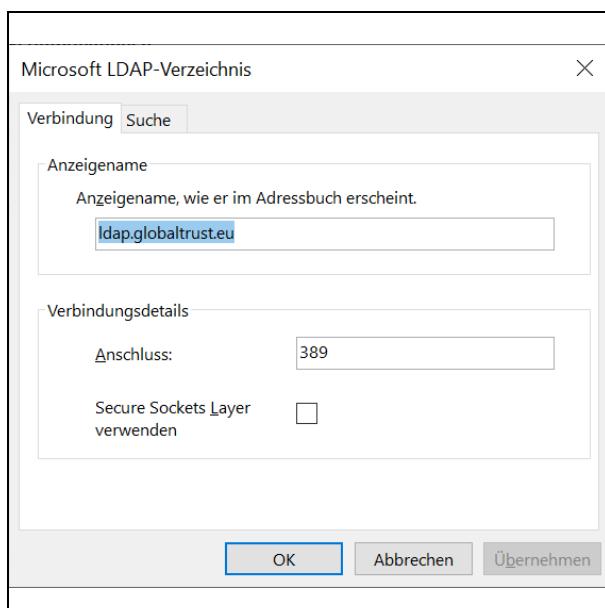
[Weitere Einstellungen...](#)

< Zurück Weiter > Abbrechen

Screen 49: Basiskonfiguration LDAP-Verzeichnisdienst

GLOBALTRUST LDAP-Server eintragen: ldap.globaltrust.eu

Weitere Einstellungen... ⇒ Reiter "Verbindung" ⇒



Microsoft LDAP-Verzeichnis

Verbindung Suche

Anzeigename
Anzeigename, wie er im Adressbuch erscheint.

Verbindungsdetails

Anschluss:

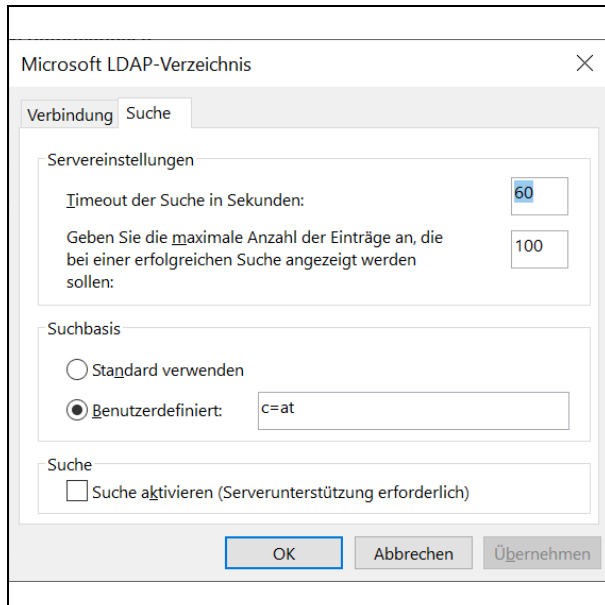
Secure Sockets Layer verwenden ☐

OK Abbrechen Übernehmen

Screen 50: Verbindungsoptionen LDAP Server

Anschluss eintragen: 389 (= ist die IP-Portnummer)

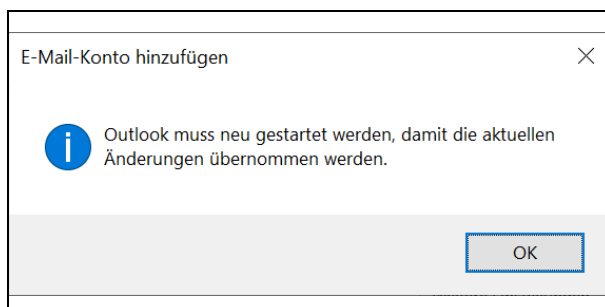
Wechsel zu Reiter "Suche" ⇨



Screen 51: Suchoptionen LDAP Server

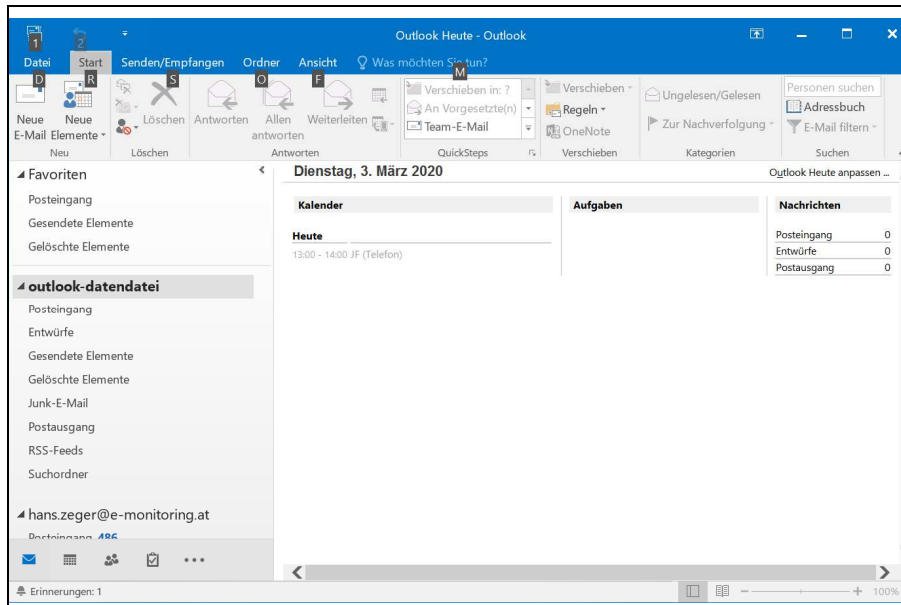
OK ⇨ Weiter ⇨

Damit die LDAP-Suche aktiviert wird, ist Neustart von Outlook erforderlich



Screen 52: Neustart Hinweis Outlook

5.2 PERSONENSUCHE MITTELS LDAP-SERVER LDAP.GLOBALTRUST.EU

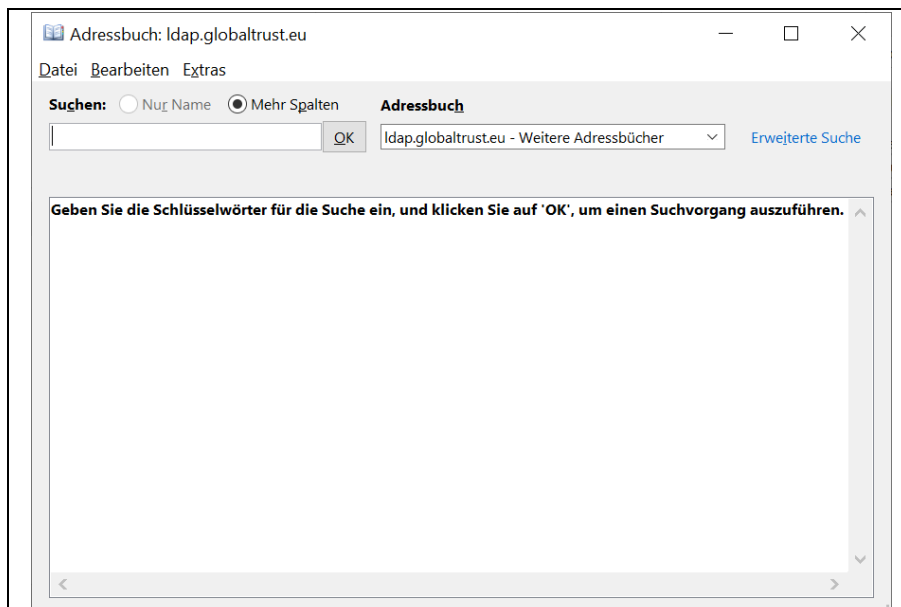


Screen 53: Übersichtsseite Outlook

Hinweis!

Die Suche im Outlook-Hauptmenu funktioniert für LDAP nicht!

Adressbuch öffnen ⇨



Screen 54: Adressbuch

Beste LDAP-Suchergebnisse mittels erweiterter Suche

Link "Erweiterte Suche" öffnen ⇨

Suchen

Suche

Anzeigename: zeger

Vorname: Nachname:

Position: Alias:

Firma: E-Mail:

Büro: Abteilung:

Telefon: Ort:

Suchkriterien

☐ Beginnt mit ☒ Enthält

OK Abbrechen

Screen 55: LDAP-Suchmaske

gesuchte Person in "Anzeigename" eintragen ⇒ "Enthält" auswählen ⇒ OK ⇒

Suchergebnis:

Adressbuch: ldap.globaltrust.eu

Datei Bearbeiten Extras

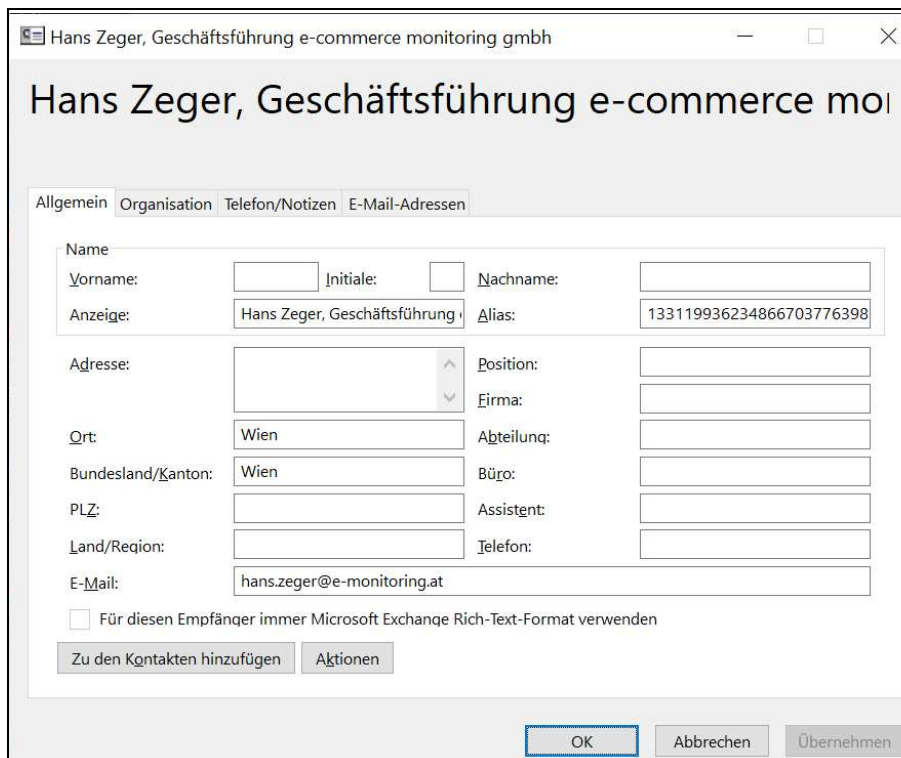
Suchen: ☐ Nur Name ☒ Mehr Spalten Adressbuch

OK ldap.globaltrust.eu - Weitere Adressbücher Erweiterte Suche

Name	E-Mail-Adresse	E-Mail-Typ	Telefon gesch...	Büro	Posit
Hans Zeger, Geschäft...	hans.zeger@e-monitoring.at	SMTP			
Hans Zeger, Testzertif...	hans.zeger@e-monitoring.at	SMTP			
Mag. Dr. Hans G. Zeger	hans.zeger@e-monitoring.at	SMTP			
Mag. Dr. Hans G. Zeger	hans.zeger@e-monitoring.at	SMTP			
Mag. Dr. Hans G. Zeg...	hans.zeger@e-monitoring.at	SMTP			
Mag. Dr. Hans G. Zeg...	hans.zeger@e-monitoring.at	SMTP			
Mag. Dr. Hans G. Zeg...	hans.zeger@e-monitoring.at	SMTP			
Mag. Dr. Hans G. Zeg...	hans.zeger@e-monitoring.at	SMTP			
Mag. Dr. Hans G. Zeg...	hans.zeger@e-monitoring.at	SMTP			
Mag. Dr. Hans Gerhar...	ocsp@globaltrust.info	SMTP			

Screen 56: Liste der gefundenen Adressen (inklusive Zertifikate) im LDAP-Server

E-Mail-Adresse in lokales Adressbuch übernehmen: Doppelclick auf gewünschte Adresse ⇨



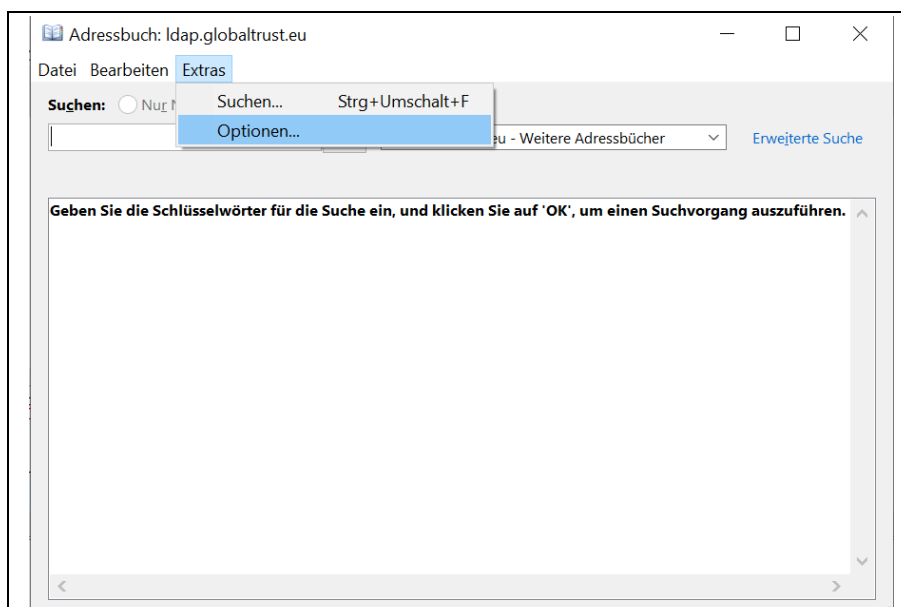
Screen 57: Übernahme LDAP-Eintrag in lokales Adressbuch

OK ⇨

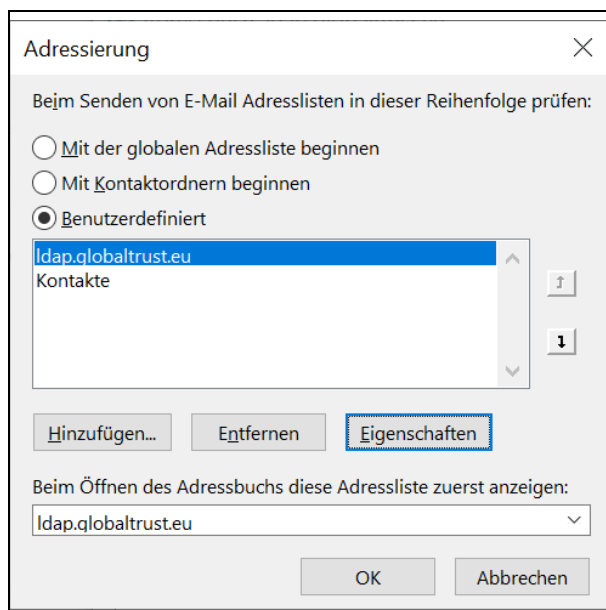
5.3 OPTIONALE ANPASSUNG DES OUTLOOK-ADRESSBUCHES

Erfolgt häufig eine LDAP-Suche, dann sollte der LDAP-Server vorgereicht werden (optional):

⇨ Extras ⇨ Optionen... ⇨



Screen 58: Adressbuch



Screen 59: Reihenfolge der Adress-Suche festlegen

6 EINRICHTEN OUTLOOK 2016 - E-MAIL-ACCOUNT

Dieser Abschnitt ist für das erstmalige Einrichten eines E-Mail-Accounts beim eigenen Mail-Server optimiert, bei dem die Anmeldedaten beim Server unterschiedlich von der E-Mail-Adresse ist.

Wenn Sie den Mail-Server von Microsoft, Google usw. verwenden, beachten Sie deren Installationsanleitungen.

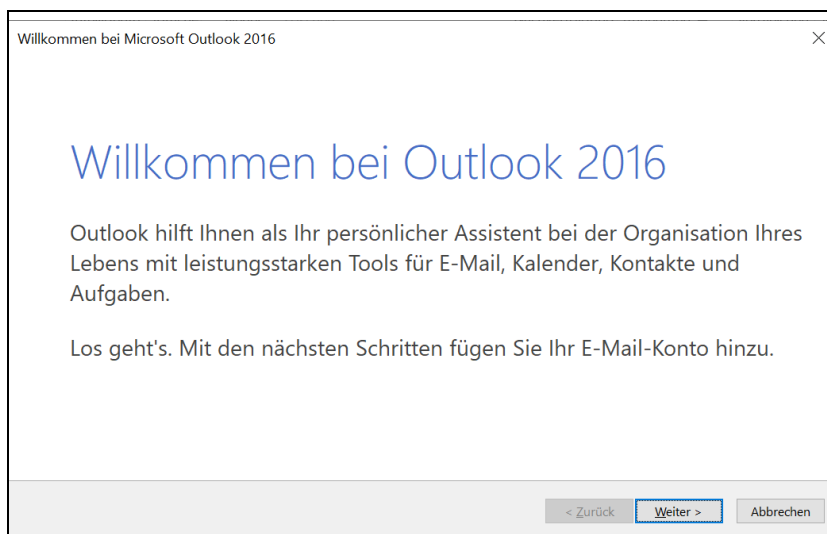
Outlook 2016 bietet zwei unterschiedliche Produkte an:

- ⇒ 6.1 Outlook 2016 "Standard" (p39)
- ⇒ 6.2 Outlook 2016 "Professional" (p47)

Abhängig vom verwendeten Outlook-Produkt ergeben sich unterschiedliche Installationsverfahren Ihres Accounts. Wenn Sie unsicher sind, welche Outlook-Version Sie verwenden, kontaktieren Sie Ihren IT-Betreuer.

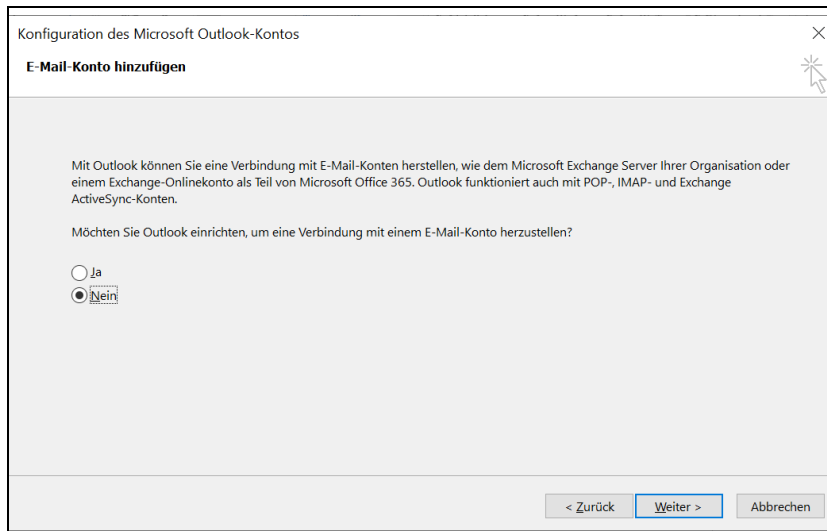
6.1 OUTLOOK 2016 "STANDARD"

Outlook 2016 starten ⇒



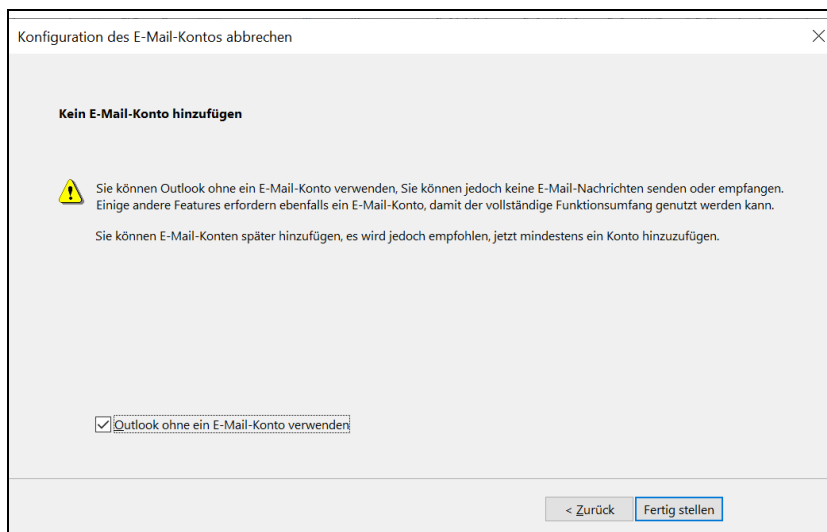
Screen 60: Einstieg Outlook 2016

Weiter ⇒ START mit Option "Outlook ohne Konto verwenden"² ⇒



Screen 61: Outlook ohne Konto einrichten I

Weiter ⇒ "Outlook ohne ein E-Mail-Konto einrichten" auswählen ⇒

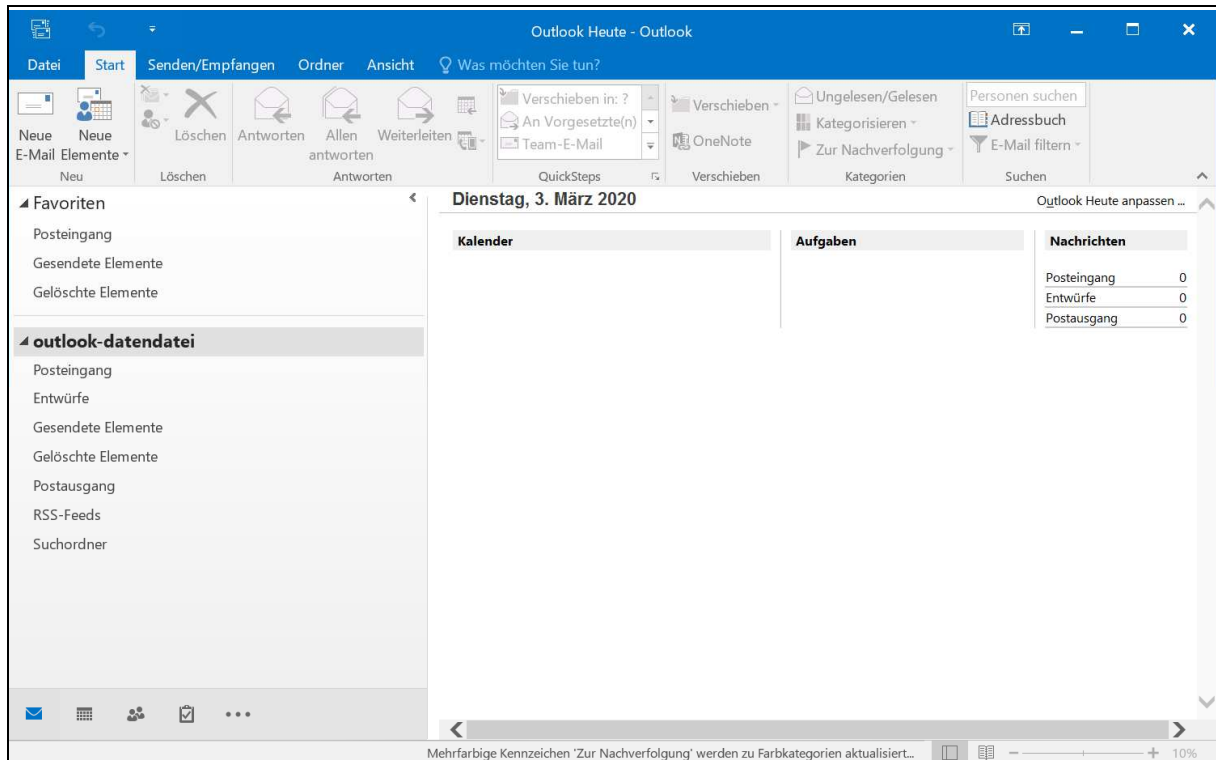


Screen 62: Outlook ohne Konto einrichten II

²

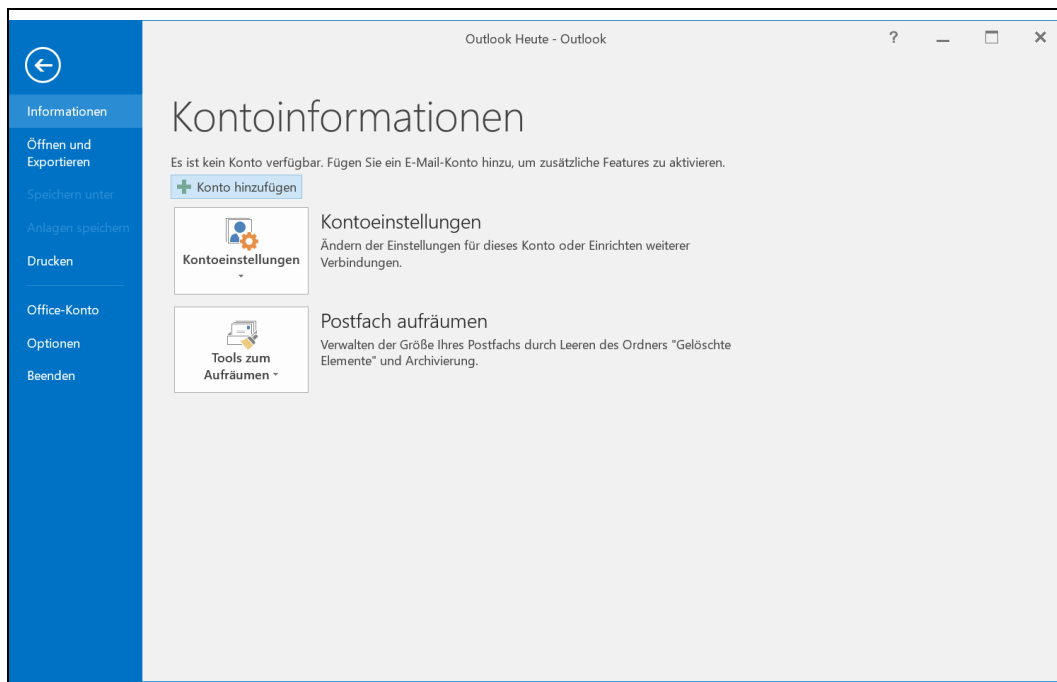
Als "Konto" bezeichnet Microsoft einen bei Microsoft angesiedelten Account (hotmail, live, outlook.com, ...), diese sind für professionelle Anwender im Regelfall wenig geeignet.

Fertig stellen ⇨



Screen 63: Basisansicht Outlook 2016

Datei ⇨



Screen 64: Übersicht Kontoinformationen

Konto hinzufügen ⇨

Screen 65: E-Mail Konto einrichten

"Manuelle Konfiguration oder zusätzliche Servertypen" auswählen ⇨ Weiter ⇨

Screen 66: E-Mail Serverart auswählen

"POP oder IMAP" auswählen ⇒

Screen 67: Basiseinstellungen E-Mail Account

Kontoeinstellungen gemäß Account beim eMail-Anbieter eintragen³

Weitere Einstellungen ⇒

Hinweis

Die Einstellungen dieses Abschnitts können Sie später unter folgendem Menu-Punkt ändern:
 Optionen ⇒ Erweitert ⇒ Senden/Empfangen ⇒ (Gruppe auswählen) ⇒ Bearbeiten... ⇒
 Kontoeigenschaften ⇒

³ Diese Informationen stellt Ihnen der eMailanbieter, meist ein Internet Service Provider, ein Telekomanbieter oder die IT-Abteilung zur Verfügung.

⇒ Reiter "Allgemein" (optional)

The screenshot shows the 'Internet-E-Mail-Einstellungen' dialog box with the 'Allgemein' tab selected. The 'E-Mail-Konto' section has a text input field for the account name and a checkbox for 'Mailadresse (wird übernommen)'. The 'Weitere Benutzerinformationen' section has a 'Firma:' label, a text input field for 'Firmenbezeichnung', and an 'Antwortadresse:' label with a text input field and a note 'alternative Antwortadresse (wird jedoch nicht empfohlen)'. At the bottom are 'OK' and 'Abbrechen' buttons.

Screen 68: Internet E-Mail Einstellungen allgemein

Reiter "Postausgangsserver" ⇒

The screenshot shows the 'Internet-E-Mail-Einstellungen' dialog box with the 'Postausgangsserver' tab selected. The 'Der Postausgangsserver (SMTP) erfordert Authentifizierung' checkbox is checked. Below it are two radio buttons: 'Gleiche Einstellungen wie für Posteingangsserver verwenden' (selected) and 'Anmelden mit'. The 'Anmelden mit' option has a 'Benutzername:' label, a text input field, a 'Kennwort:' label, a text input field, and a 'Kennwort speichern' checkbox which is checked. There is also an unchecked checkbox for 'Gesicherte Kennwortauthentifizierung (SPA) erforderlich'. At the bottom are 'OK' and 'Abbrechen' buttons.

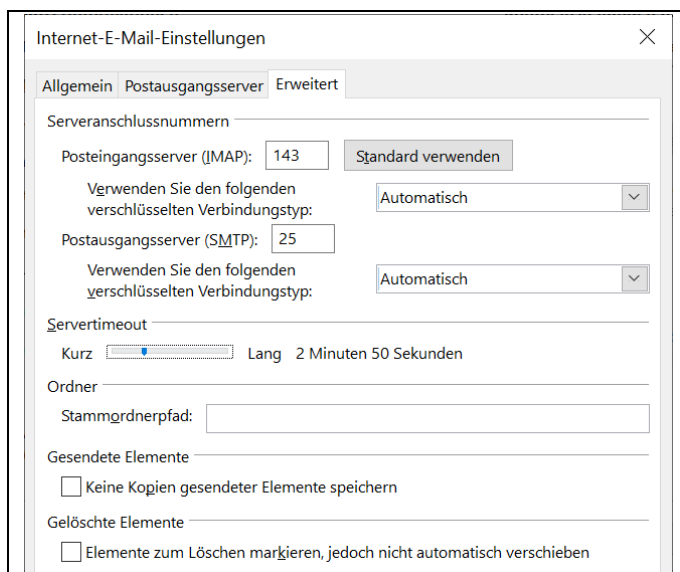
Screen 69: Konfiguration des SMTP-Servers

Hinweise:

- Um den Missbrauch als Relay- und Spam-Mail-Server zu verhindern erlauben die meisten SMTP-Server nur die Verwendung durch angemeldete Benutzer (wie etwa auch der Mailserver von e-monitoring.at).
- In der Regel sind die Anmeldedaten für ein- und ausgehende Server ident (wie etwa beim Mailserver von e-monitoring.at).

In der Regel muss zwingend "Der Postausgangsserver (SMTP) erfordert Authentifizierung" ausgewählt werden.

Reiter "Erweitert" (optional) ⇒

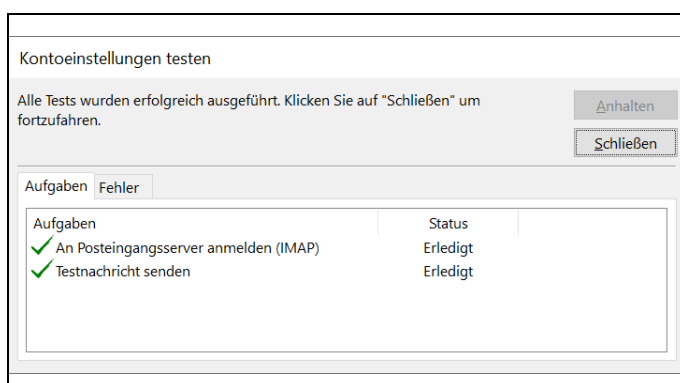


Screen 70: Internet E-Mail Einstellungen erweitert

- Port des Posteingangsservers ist bei IMAP im Regelfall: 143 (ansonsten ist der IT-Betreuer zu kontaktieren)
- Port des Postausgangsservers ist bei SMTP im Regelfall 25 (ansonsten ist der IT-Betreuer zu kontaktieren)
- bei schlechten Internet-Verbindungen sollte auf jeden Fall das Servertimeout erhöht werden

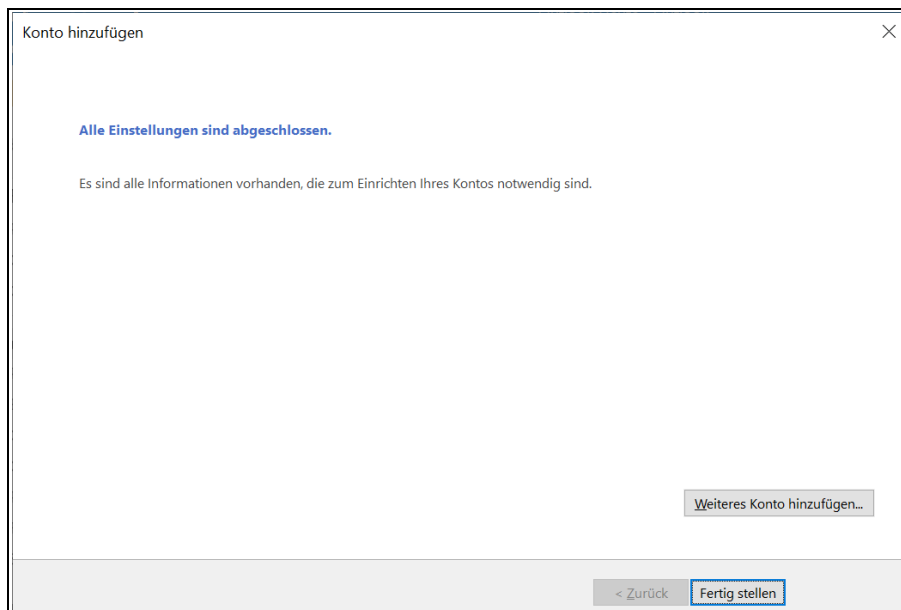
OK ⇒ Weiter ⇒

Anschließend führt Outlook eine Mail-Serverprüfung durch, wenn OK:



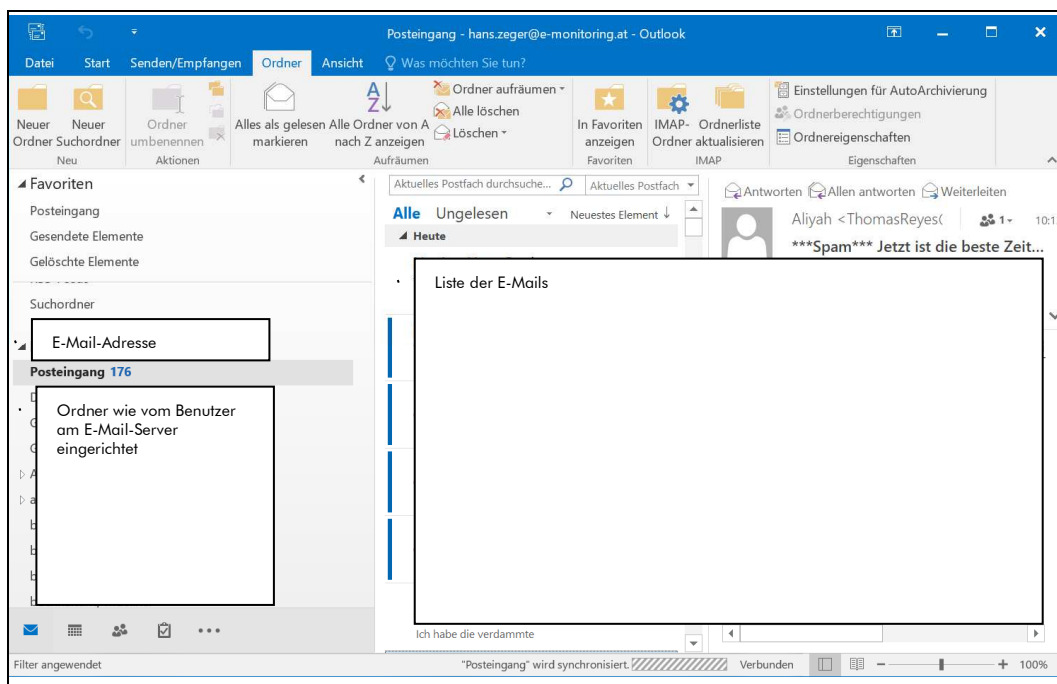
Screen 71: Erfolgreicher Verbindungstest zum Mail Server

Schließen ⇒



Screen 72: Abschluss Konto hinzufügen

⇒ Fertig stellen ⇒ anschließend wird das Konto angezeigt

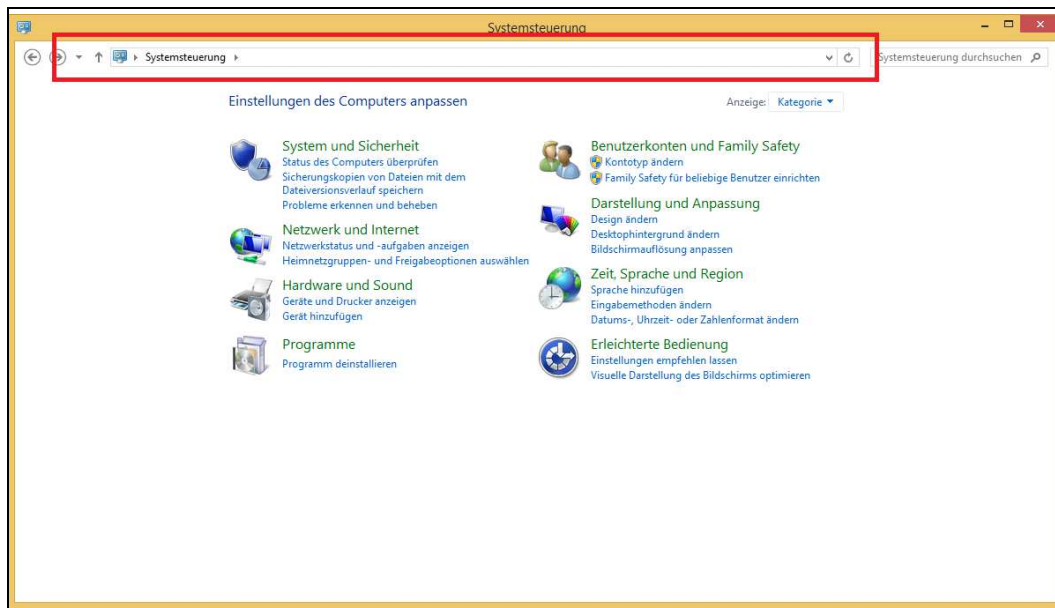


Screen 73: eingerichtetes Konto

6.2 OUTLOOK 2016 "PROFESSIONAL"

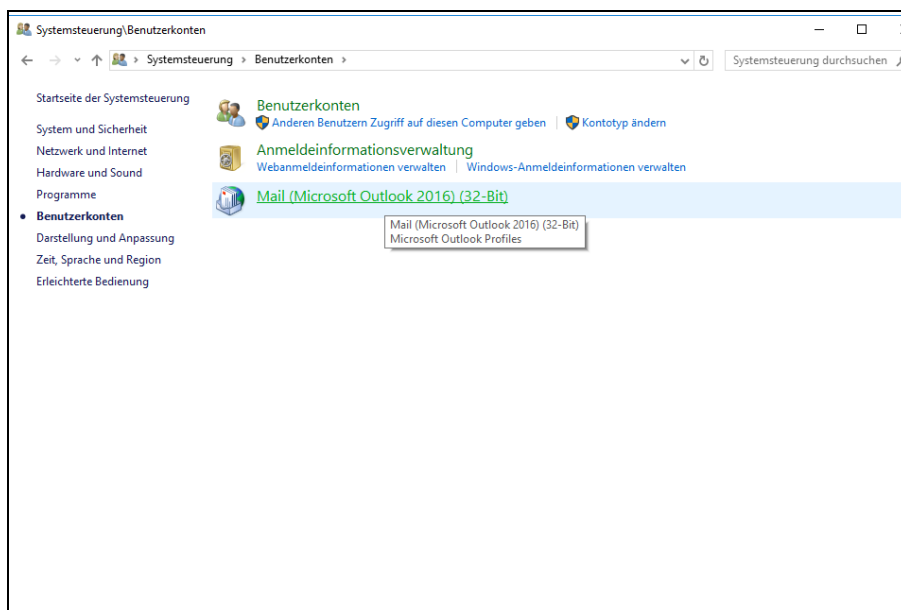
Die "Professional"-Version stellt keine direkte Option zum Einrichten eines Accounts mit abweichenden Namen zur Verfügung, man muss stattdessen den "Umweg" über die Systemsteuerung wählen

Systemsteuerung über Windowssuche aufrufen (zB Windows-Key auf Tastatur) ⇒



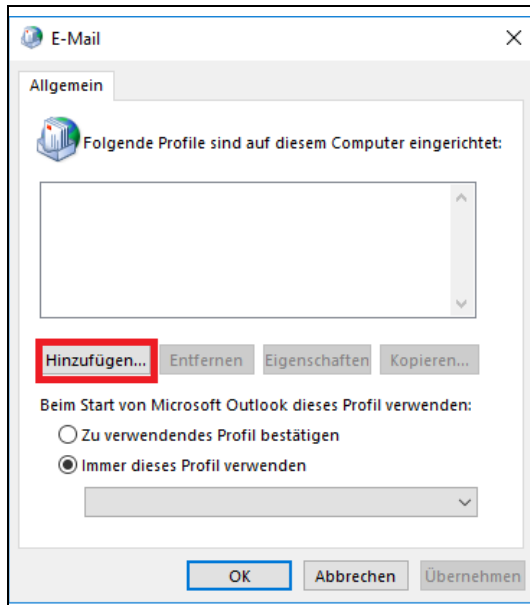
Screen 74: Windows 10 Systemübersicht

"Benutzerkonten" (bzw. "Benutzerkonten und Family Safety") ⇒



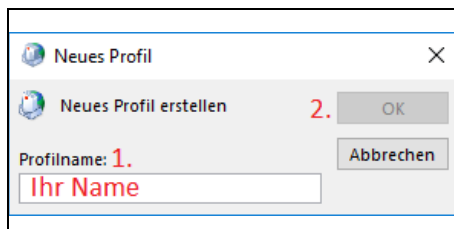
Screen 75: Auswahl Benutzerkonten

Mail (Microsoft Outlook 2016) (Version 32 bit bzw. 64 bit) ⇒



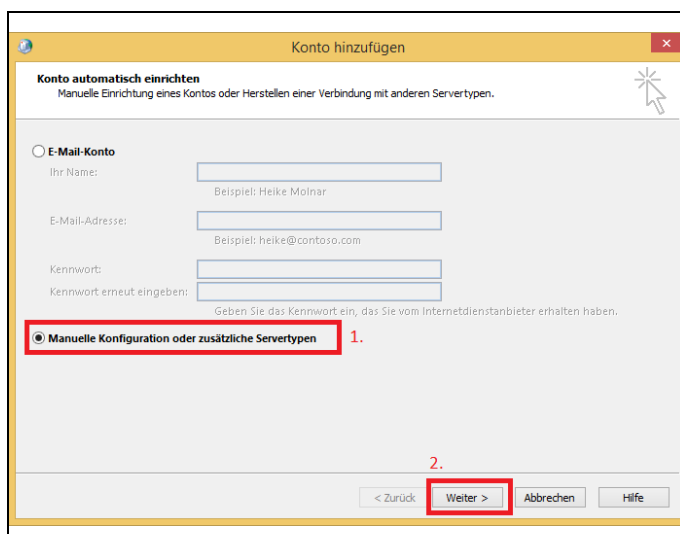
Screen 76: Übersicht E-Mail Konten

Hinzufügen... ⇒



Screen 77: neues Konto einrichten

OK ⇒



Screen 78: E-Mail Konto einrichten

Weiter ident zu Abschnitt 6.1 Outlook 2016 "Standard" ab "Manuelle Konfiguration oder zusätzliche Servertypen" auswählen ⇒ (p42).

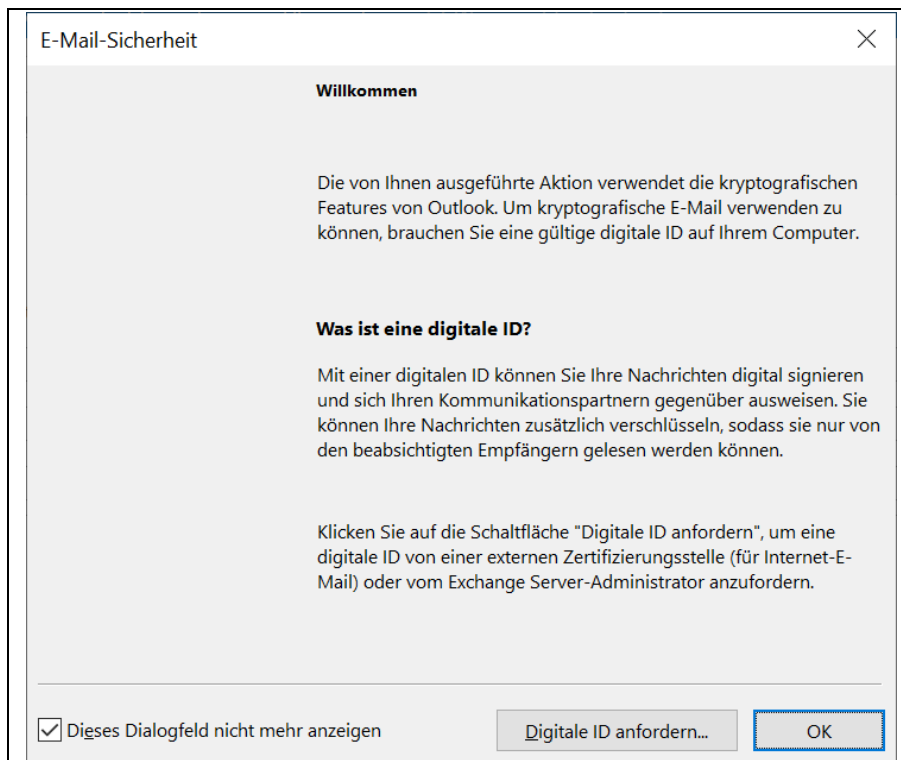
7 TROUBLESHOOTING OUTLOOK 2016

GLOBALTRUST-Zertifikate sind ausgereifte Produkte und EU-weit als rechtsgültig anerkannt. Trotzdem kann es vor'kommen, dass im Rahmen der Nutzung in Outlook unverständliche Meldungen erscheinen. Einige (wenige) dieser Meldungen finden Sie in diesem Abschnitt.

7.1 FEHLERMELDUNGEN UND WARNHINWEISE

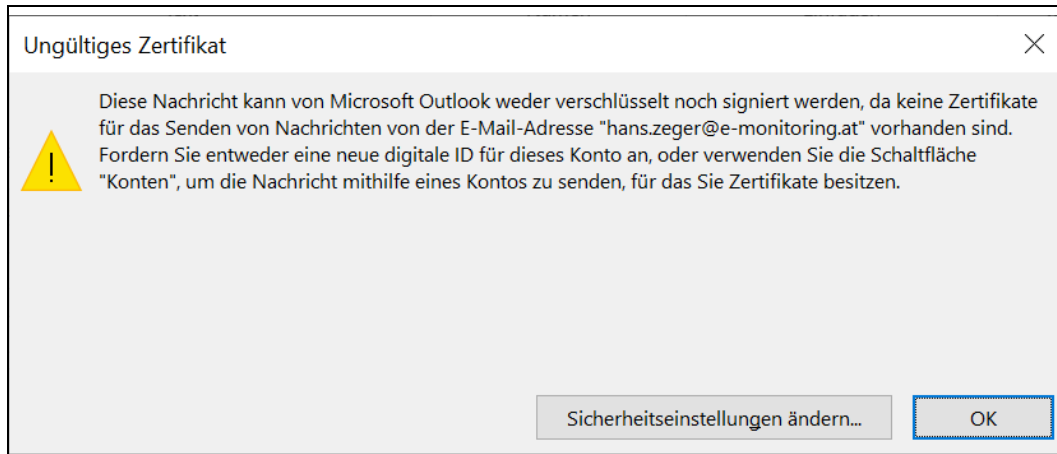
7.1.1 SCHEINBARES FEHLEN DES ZERTIFIKATES

Es erscheint folgende Fehlermeldung:



Screen 79: Outlook Meldung wegen fehlendem Zertifikat

OK ⇒



Screen 80: Warnhinweis ungültiges Zertifikat

- Stellen Sie sicher, dass Sie die Installationsschritte korrekt durchgeführt haben ⇒ Abschnitt 3 Einrichten des Zertifikates (E-Mail Sicherheit) in OUTLOOK 2016 (p6)

bleibt der Fehler, kann es an einem dieser Punkte liegen (nicht vollständig):

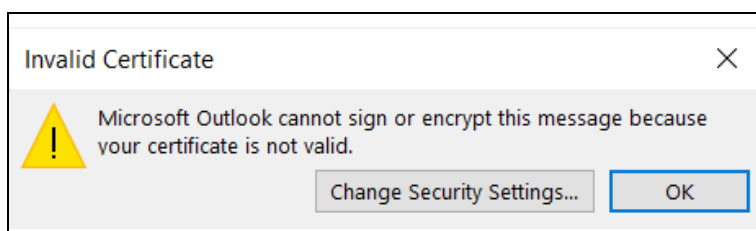
- Ihr Zertifikat ist schon abgelaufen ist (Prüfung Zertifikat ⇒ Abschnitt 7.2.1 Prüfen Laufzeit des Zertifikates, p60)
- Ihr Zertifikat wurde widerrufen (Prüfung Widerrufsliste ⇒ Abschnitt 7.2.2 Prüfen Widerrufsstatus, p63)
- es gibt einen Fehler in der Zertifikatskette (zB die CAs wurden irrtümlich gelöscht oder Firewall-Einstellungen im Unternehmen verhindern Windows am automatischen Aktualisieren Ihres Zertifikatsspeichers) ⇒ Kontaktieren Sie Ihren IT-Betreuer

7.1.2 ZERTIFIKAT WIRD VON MICROSOFT NICHT ZUR EMAIL-SIGNATUR AKZEPTIERT

Grundsätzlich enthalten alle GLOBALTRUST-Zertifikate eine Kennung zur Signatur (inklusive der eMail-Signatur). Microsoft verwendet jedoch in seinen Produkten eine eigene Security-Verwaltung welche Zertifikatstypen für welche Signaturformen erlaubt sind. Zur eMail-Signatur muss daher das Signatur-Flag "SMIME-Signatur" bzw "eMail-Signatur" freigeschalten sein.

Diese Freischaltung ist für alle GLOBALTRUST-Root-Zertifikate mit Microsoft vereinbart. Es kann jedoch vorkommen, das in lokalen Installationen diese Freischaltung (a) deaktiviert wurde oder (b) nicht wie erwartet funktioniert.

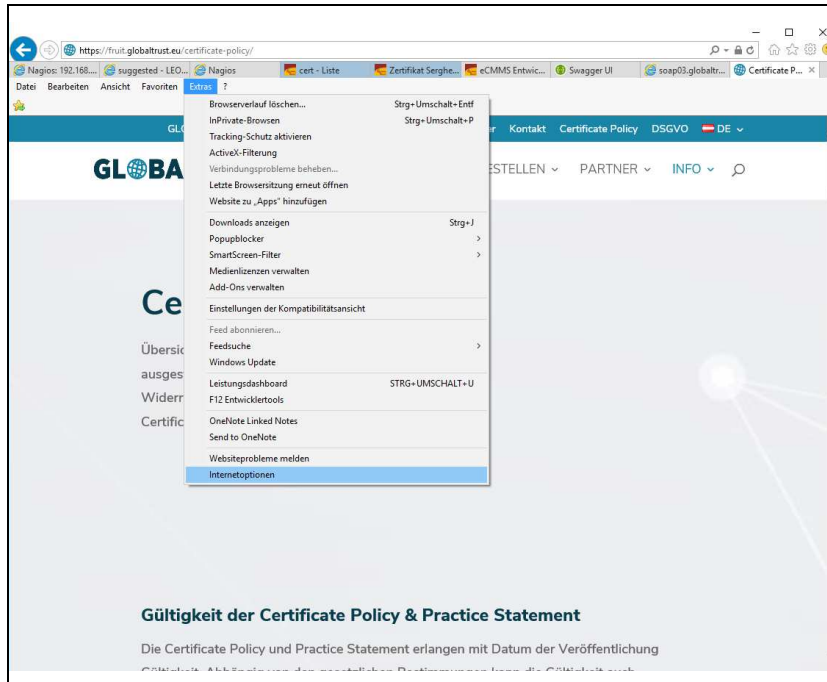
Es können Meldungen, ähnlich folgender auftreten:



Screen 81: Warnhinweis zu fehlender S/MIME Eigenschaft

In diesem Fall ist die Microsoft-Zertifikatsverwaltung zu prüfen und gegebenenfalls zu korrigieren.

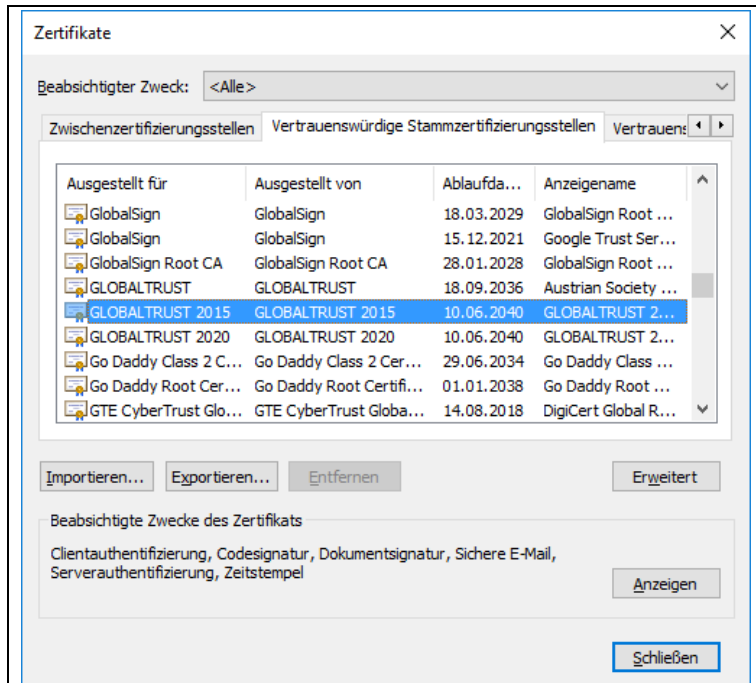
Aufruf der Microsoft-Zertifikatsverwaltung mittels IE ⇒ Extras ⇒ Internetoptionen ⇒
(alternativer Aufruf: über Systemsteuerung ⇒ Internetoptionen ⇒)



Screen 82: Microsoft Zertifikatsverwaltung

STEP 1: PRÜFEN STAMMZERTIFIKATE IN ZERTIFIKATE

Reiter Inhalte ⇒ Zertifikate ⇒ Vertrauenswürdige Stammzertifizierungsstellen ⇒



Screen 83: Microsoft Zertifikatsverwaltung II

Hier müssen die RootZertifikate von GLOBALTRUST eingetragen sein und als "Beabsichtigte Zwecke des Zertifikates" muss zumindest "Sichere E-Mail" angezeigt werden

STEP 1A: IMPORT STAMMZERTIFIKAT (NUR BEI FEHLNDEN ZERTIFIKATEN ERFORDERLICH)

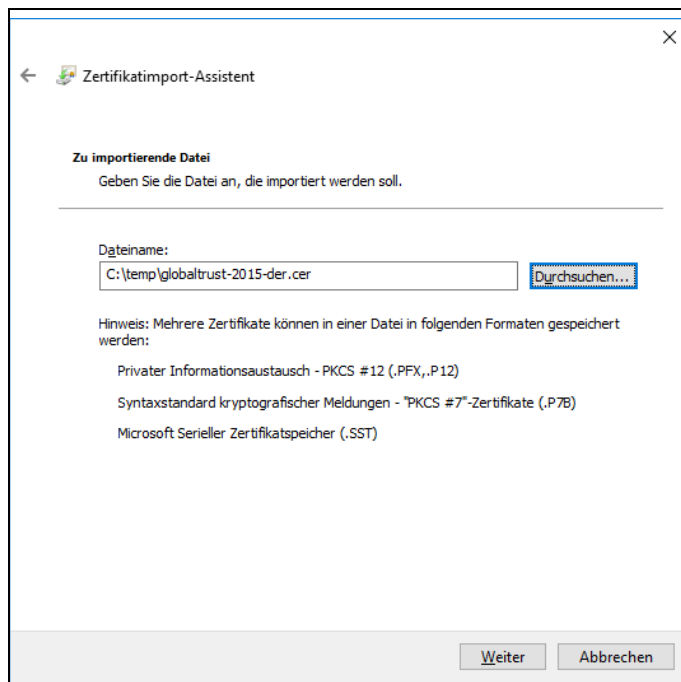
Fehlt⁴ das Rootzertifikat kann es nachinstalliert werden. Download-Stellen für die Root-Zertifikate:

- GLOBALTRUST: <https://www.globaltrust.eu/static/globaltrust2006-der.cer>
- GLOBALTRUST 2015: <http://service.globaltrust.eu/static/globaltrust-2015-der.cer>
- GLOBALTRUST 2020: <http://service.globaltrust.eu/static/globaltrust-2020-der.cer>

4

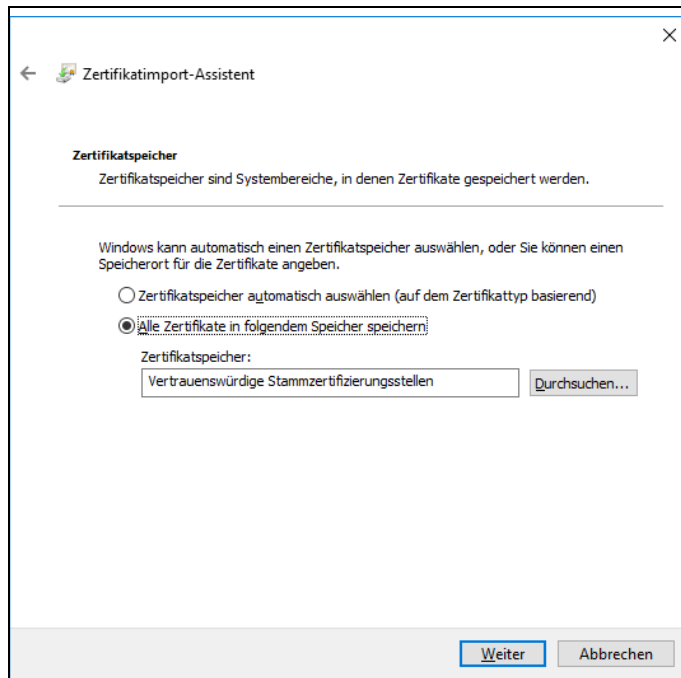
Auf Grund der Vereinbarung von GLOBALTRUST mit Microsoft sollte das Root-Zertifikat automatisch installiert werden. In manchen Unternehmen ist jedoch das automatische Update von Windows-Diensten deaktiviert. In diesen Fällen ist eine manuelle Nachinstallation erforderlich.

Importieren... ⇒ Weiter ⇒ Durchsuchen... ⇒



Screen 84: Import eines Root Zertifikates I

"Vertrauenswürdige Stammzertifizierungsstellen" auswählen ⇒ Weiter ⇒



Screen 85: Import eines Root Zertifikates II

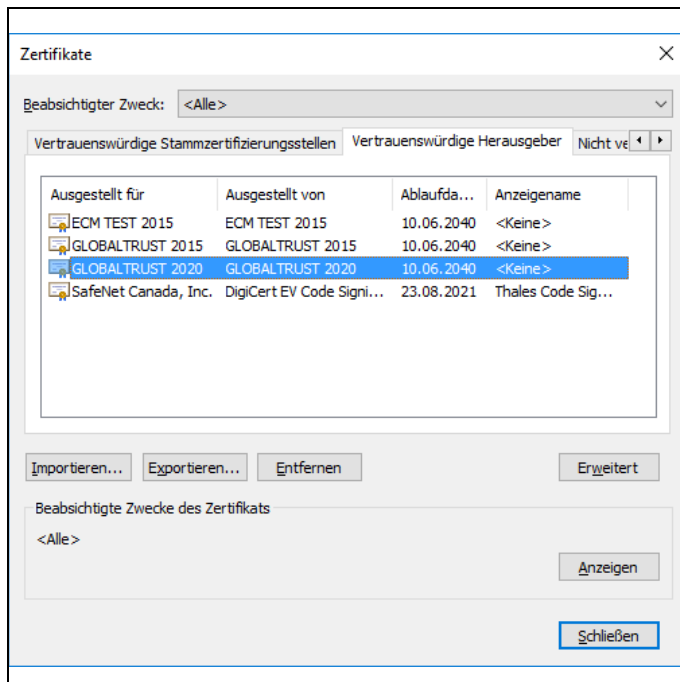
Weiter ⇒

(der Import ist abgeschlossen)

STEP 2: PRÜFEN STAMMZERTIFIKATE IN VERTRAUENSWÜRDIGE HERAUSGEBER

Zusätzlich zur generellen Zertifikatsverwaltung bietet Microsoft eine weitere Zertifikatsverwaltung für die Office-Produkte an. Hier sollten alle Root-Zertifikate eingetragen werden, die für Anwendungen vorgesehen sind, die von Microsoft nicht automatisch freigeschalten wurden.

Reiter Inhalte ⇒ Inhalte ⇒ Vertrauenswürdige Herausgeber ⇒



Screen 86: Microsoft Zertifikatsverwaltung III

Im vorliegenden Fall wurde das Zertifikat GLOBALTRUS 2020 für alle denkbare Signaturanwendungen freigegeben.

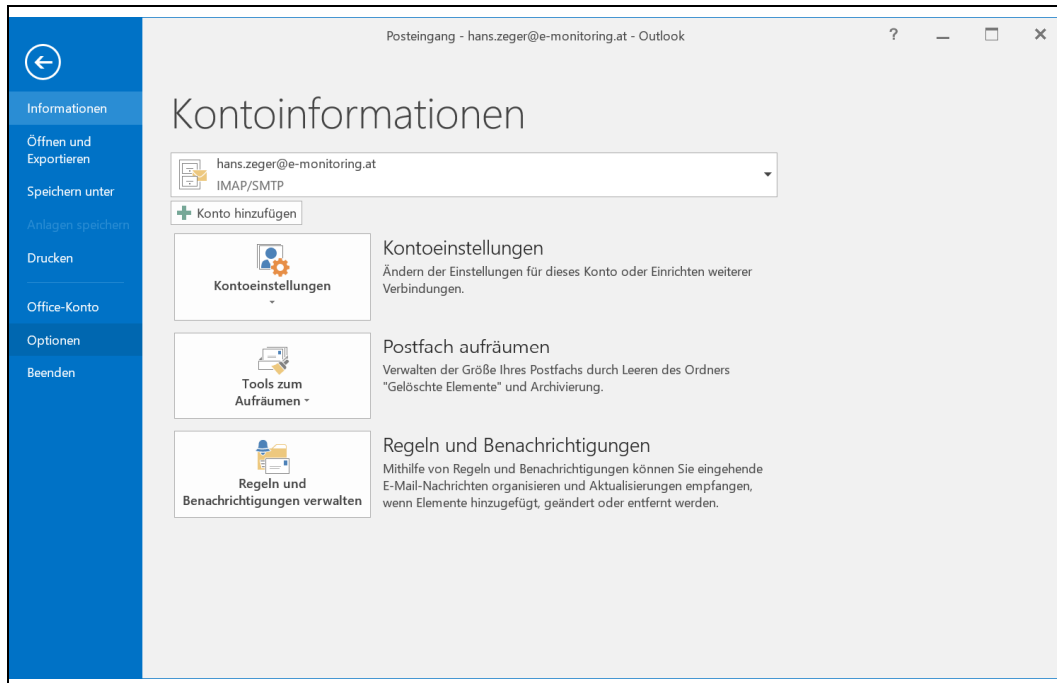
Hinweis!

Es handelt sich hier nur um eine windowsspezifische Freigabe. Die Freigabe erlaubt nur die Verwendung eines Zertifikates, soweit eine bestimmte Eigenschaft tatsächlich im Zertifikat eingetragen ist.

Der Import fehlender Zertifikate funktioniert ident wie im Fall ⇒ STEP 1a: Import Stammzertifikat (nur bei fehlenden Zertifikaten erforderlich), p52

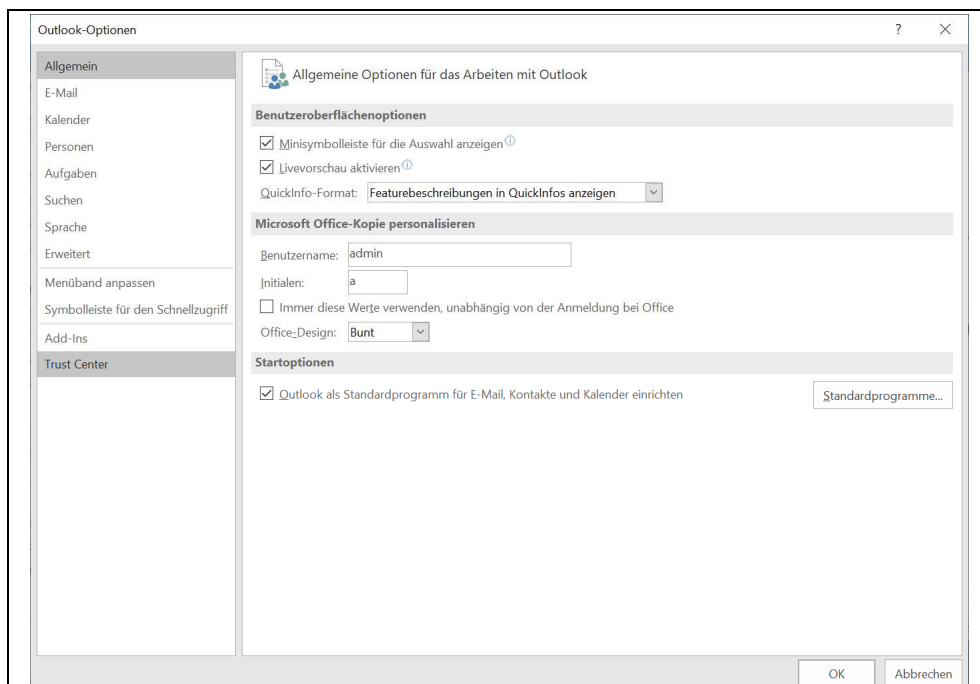
STEP 3: PRÜFEN EINSTELLUNGEN IN OUTLOOK TRUST CENTER

Öffnen Outlook 2016 ⇒ Datei ⇒



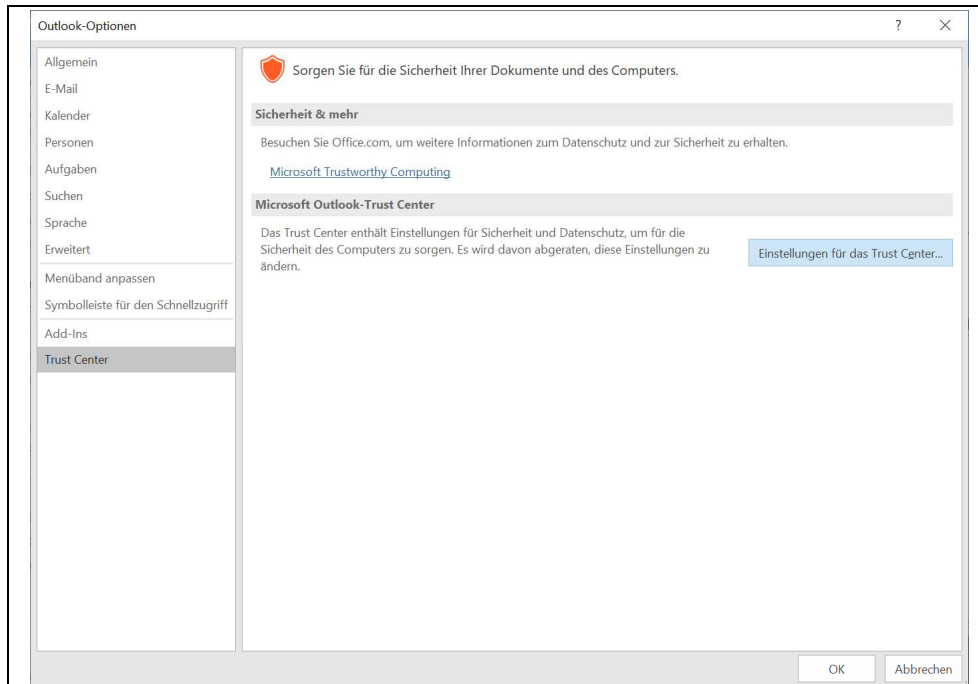
Screen 87: Outlook 2016 Datei Übersicht

Optionen ⇒



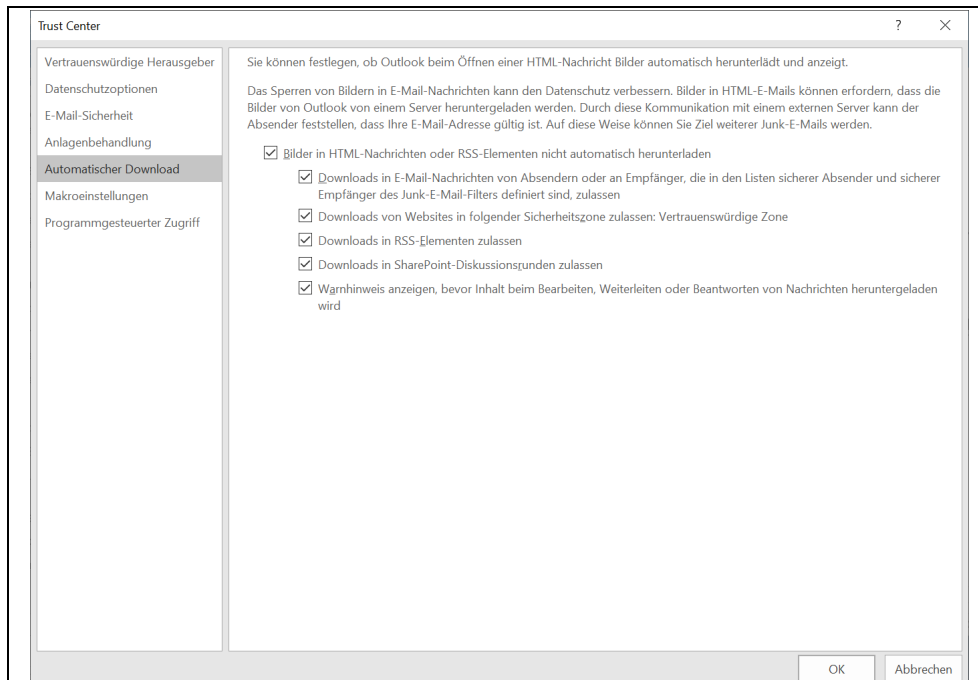
Screen 88: Übersicht Optionen

Trust Center ⇨



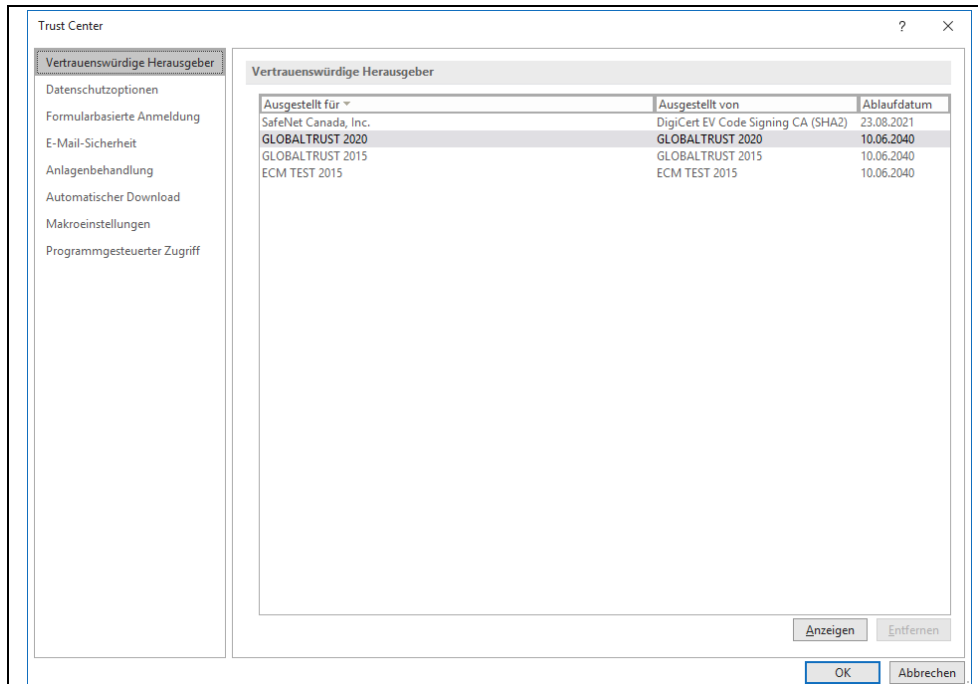
Screen 89: Übersicht Trust Center

Einstellungen für das Trust Center... ⇨



Screen 90: Übersicht Trust Center II

Vertrauenswürdige Herausgeber ⇨



Screen 91: Übersicht Vertrauenswürdige Herausgeber

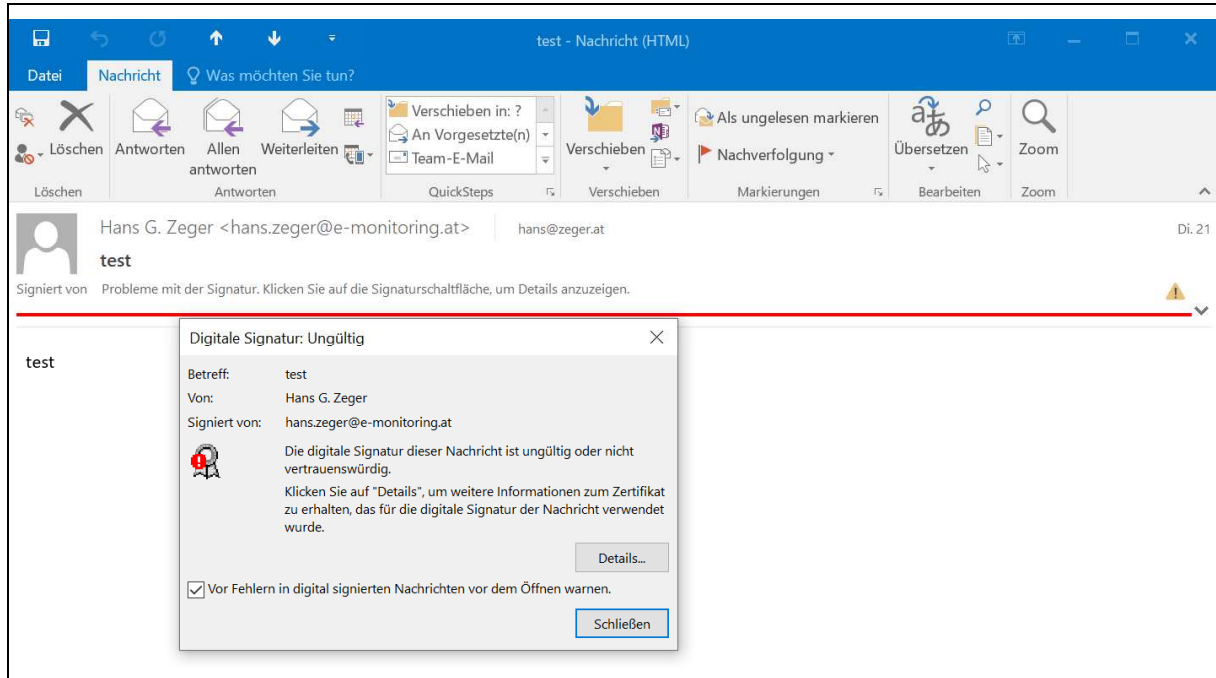
Hier scheinen alle Root-Zertifikate auf, die im vorigen Schritt eingetragen wurden ⇨

Empfehlung

GLOBALTRUST empfiehlt ausdrücklich den Eintrag der GLOBALTRUST Root-Zertifikate in die Liste der vertrauenswürdigen Herausgeber. Auf diese Weise werden künftige Fehler oder unerwünschte Änderungen der Microsoft-Policy vermieden.

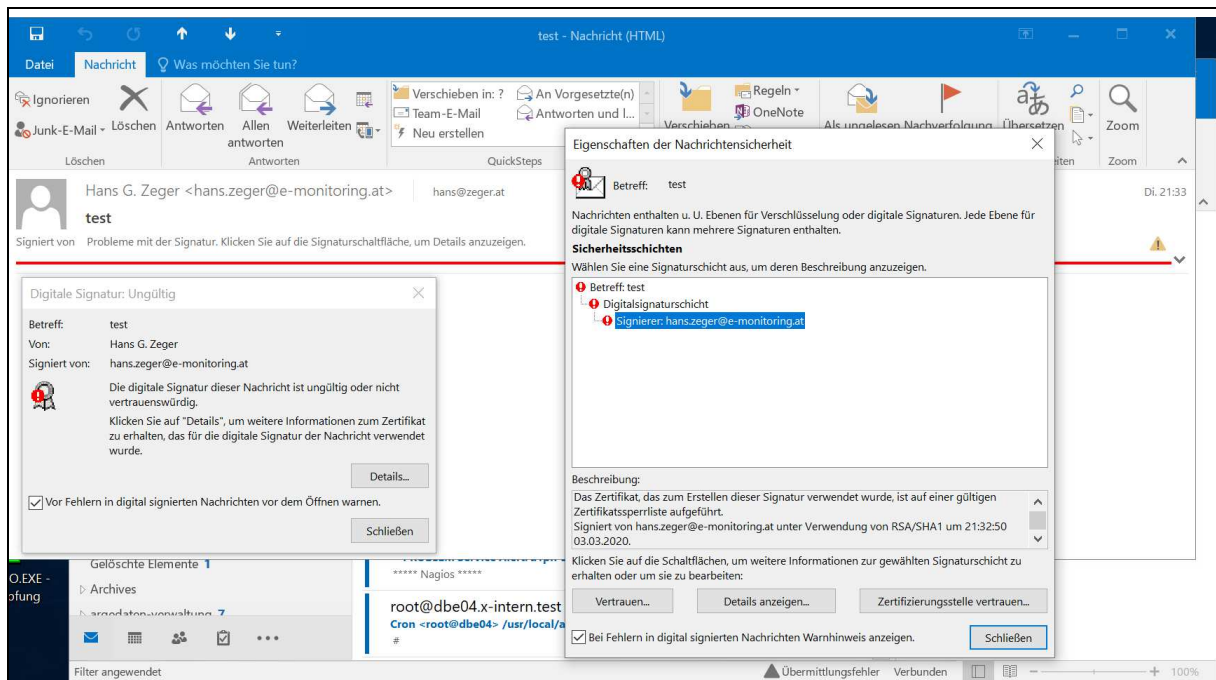
7.1.3 FEHLERHAFT ZERTIFIKATS-KETTE BEI EINEM EINGEHENDEN E-MAIL

Statt dem Siegelsymbol erscheint folgende Warnung:



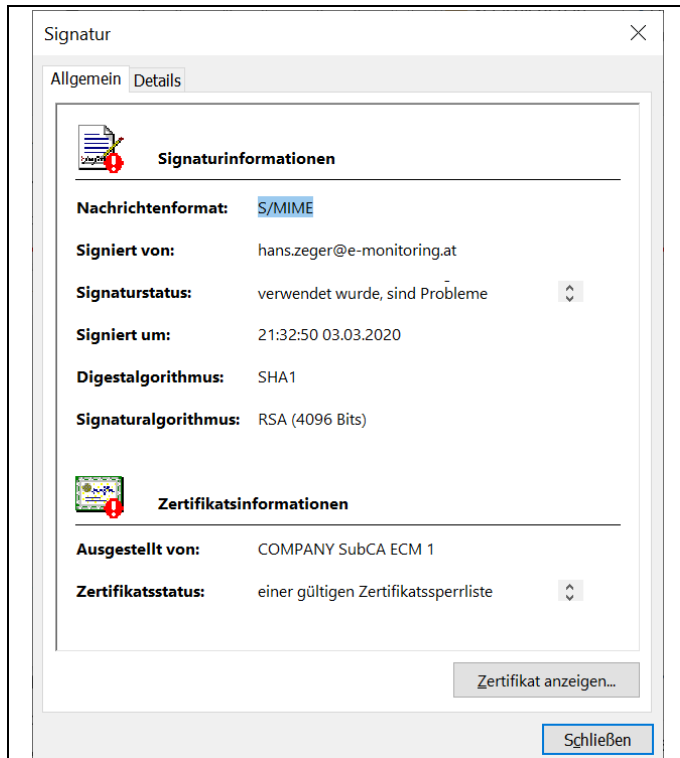
Screen 92: Warnhinweis zu einem signierten E-Mail

Details... ⇨



Screen 93: Warnhinweis zu einem signierten E-Mail II

Details anzeigen... ⇨



Screen 94: Warnhinweis zu einem signierten E-Mail III

In der Beschreibung zum Signierer findet sich der Eintrag "Das Zertifikat, das zum Erstellen dieser Signatur verwendet wurde, ist auf einer gültigen Zertifikatssperrliste aufgeführt." (Prüfung Widerrufsliste ⇨ Abschnitt 7.2.2 Prüfen Widerrufsstatus, p63)

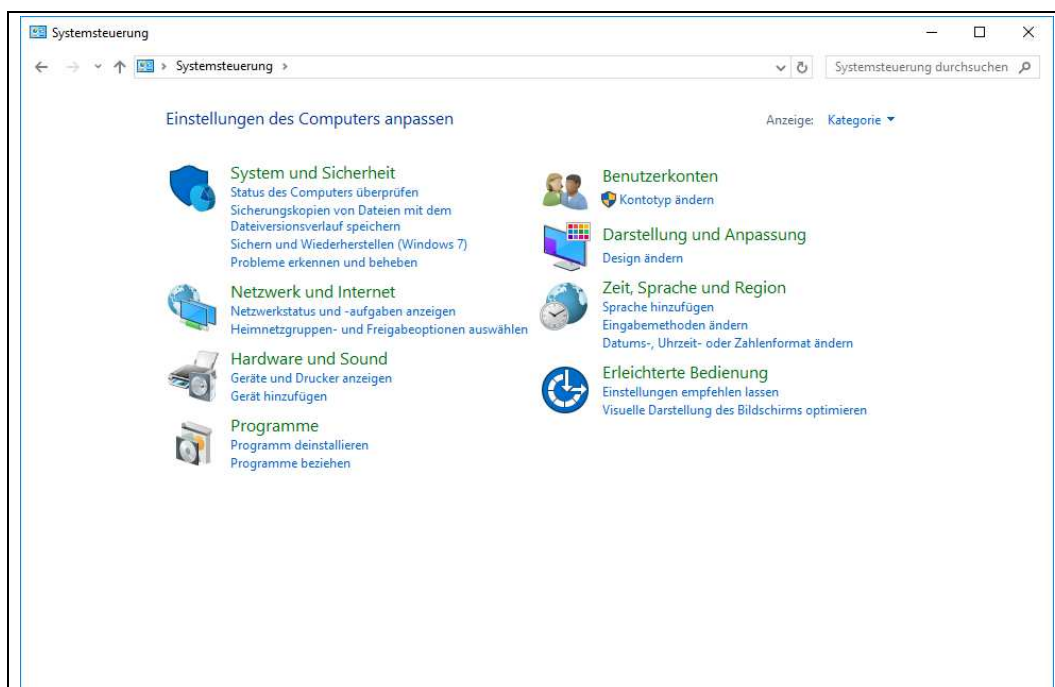
7.2 HILFSMASSNAHMEN

Üblicherweise werden die GLOBALTRUST-Zertifikate von Windows und allen Windowsfähigen Programme automatisch korrekt erkannt und auch Laufzeit, Wiederrufsstatus und Zertifikatskette korrekt abgerufen.

Die nachfolgenden Schritte erlauben Ihnen jedoch manuell nachzuvollziehen, ob Windows auf Ihrem Computer richtig konfiguriert ist und korrekte Ergebnisse zeigt.

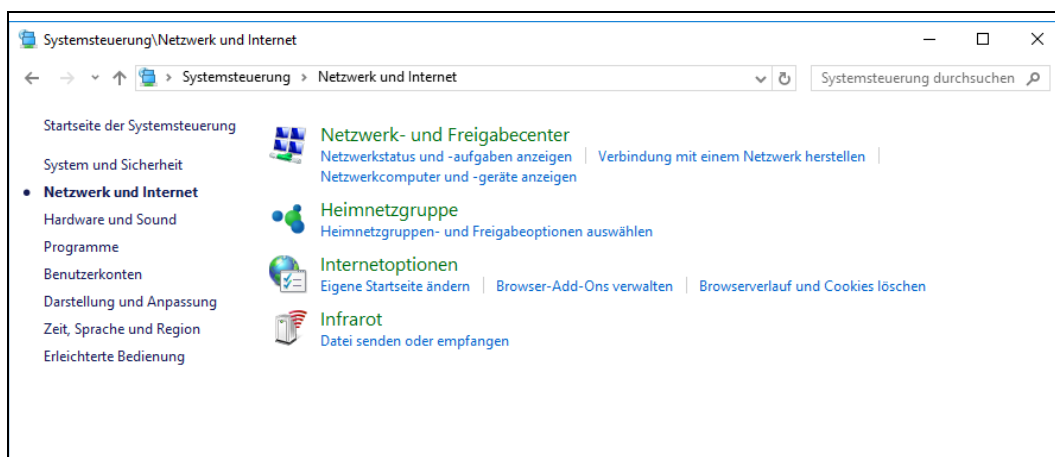
7.2.1 PRÜFEN LAUFZEIT DES ZERTIFIKATES

Systemsteuerung ⇒



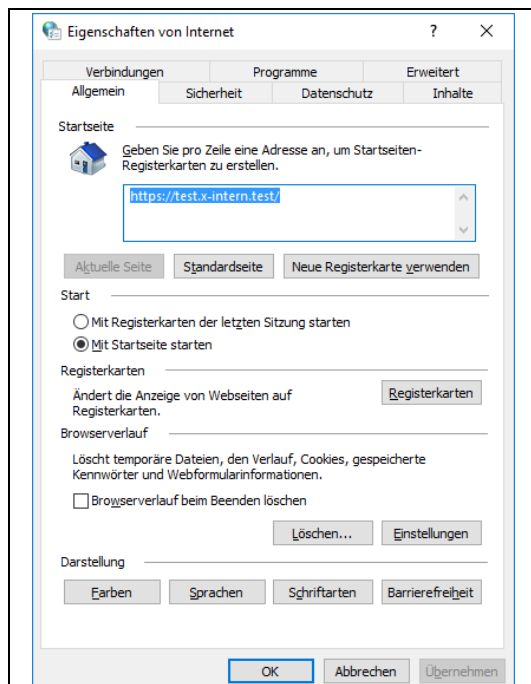
Screen 95: Übersicht Systemsteuerung

Netzwerk und Internet ⇒



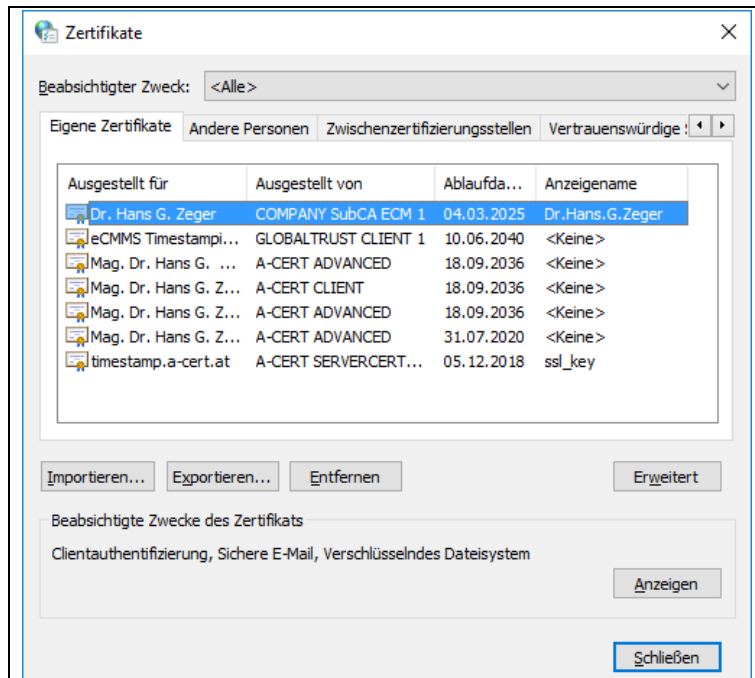
Screen 96: Übersicht Netzwerk und Internet

⇒ Internetoptionen



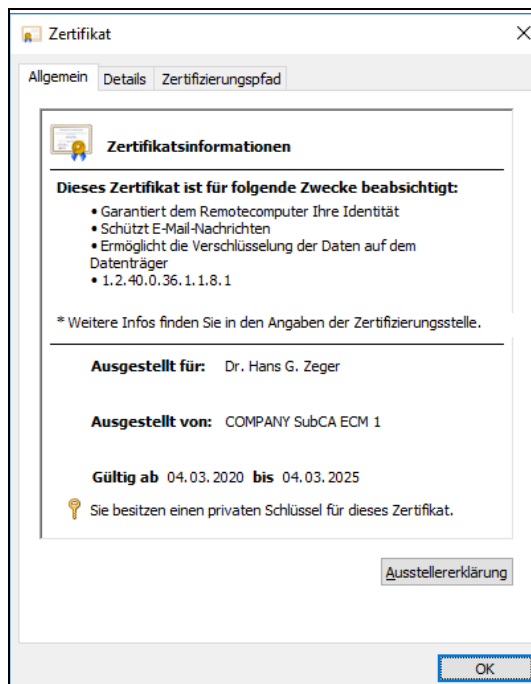
Screen 97: Übersicht Internetoptionen

Inhalte ⇒ Zertifikate ⇒ Eigene Zertifikate ⇒



Screen 98: Übersicht eigene Zertifikate

gewünschtes Zertifikat ⇒ (Doppelklick) ⇒



Screen 99: Basisinformationen zum Zertifikat

Unter "Gültig ab" ist der Zeitraum der Gültigkeit ausgewiesen

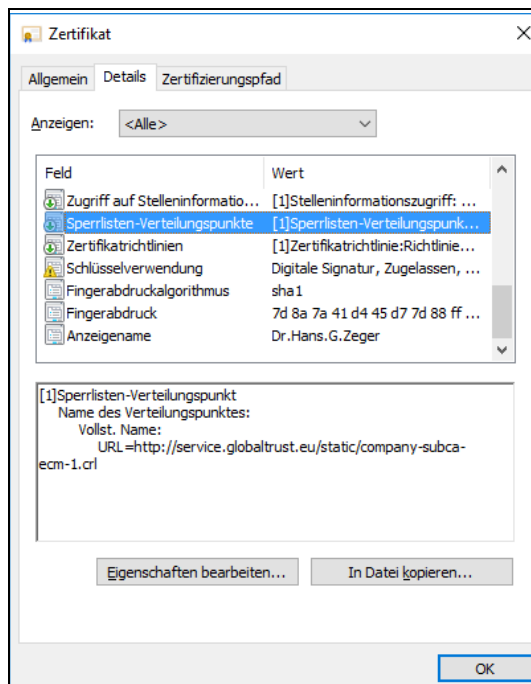
Hinweis!

An dieser Stelle kann nicht erkannt werden, ob das Zertifikat widerrufen ist. Ein Widerruf ändert nicht den Gültigkeitszeitraum im Zertifikat!

7.2.2 PRÜFEN WIDERRUFSSTATUS

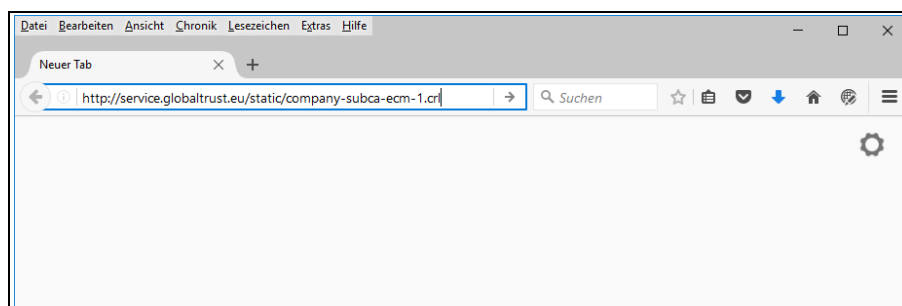
Zertifikatsaufruf ident wie ⇒ Abschnitt 7.2.1 Prüfen Laufzeit des Zertifikates (p60)

"Details" ⇒ Eintrag "Sperrlisten-Verteilungspunkte" auswählen ⇒

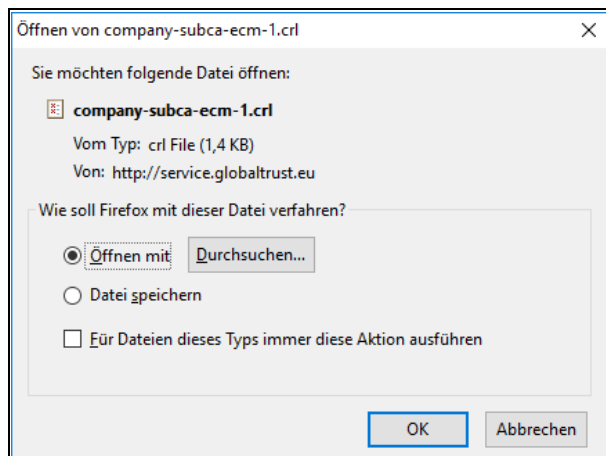


Screen 100: Details Zertifikat Sperrlisten-Verteilungspunkt

Die eingetragene URL markieren und mittels [Strg]-C Tastenkombination (auch [Ctrl]-C) kopieren ⇒ in einem beliebigen Browser eintragen ⇒

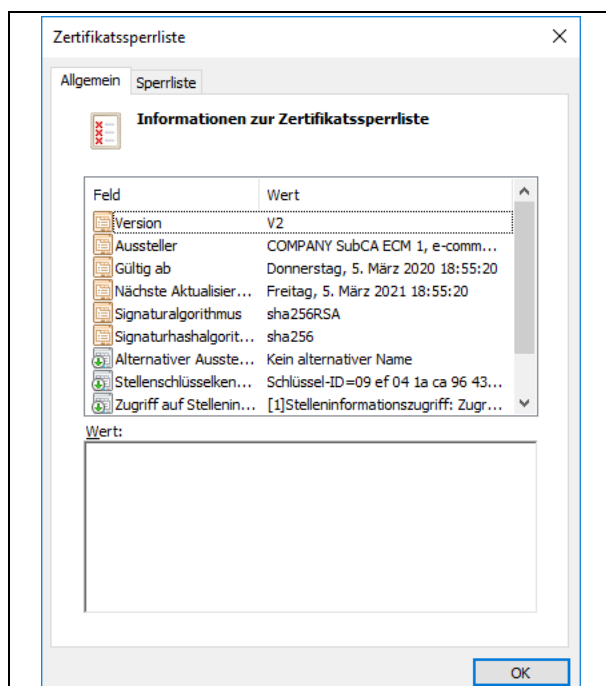


Screen 101: Aufruf der Sperrliste



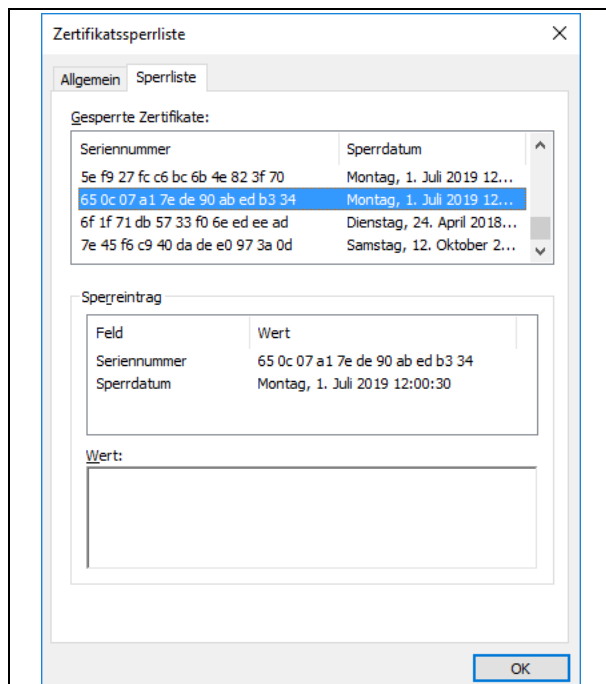
Screen 102: Download der Sperrliste

"Öffnen mit" auswählen ⇒ OK ⇒



Screen 103: Zertifikatssperrliste Allgemein

"Sperrliste" zeigt alle gesperrten Zertifikate dieser CA ⇒

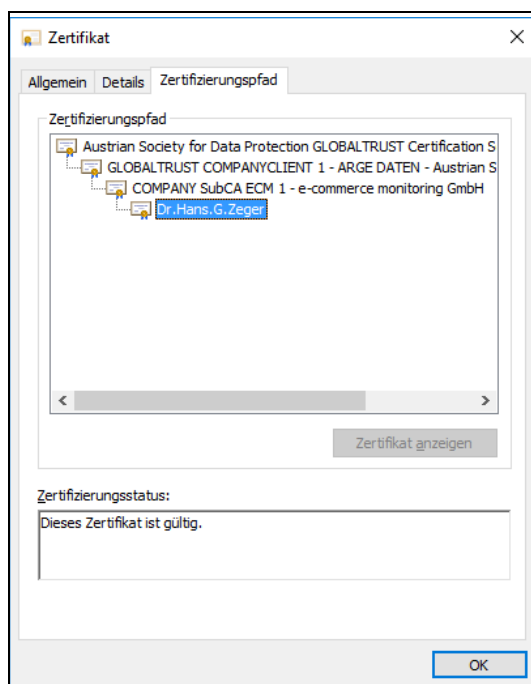


Screen 104: Zertifikatssperreliste

7.2.3 PRÜFEN ZERTIFIKATSKETTE

Zertifikatsaufruf ident wie ⇒ Abschnitt 7.2.1 Prüfen Laufzeit des Zertifikates (p60)

Statt Reiter "Allgemein" ist der Reiter "Zertifizierungspfad" auswählen ⇒



Screen 105: Zertifizierungspfad

Der Zertifizierungspfad ist in Ordnung, wenn er bis zum RootCA eine geschlossene Kette ohne Warnungen aufweist.

8 FRÜHERE OUTLOOK VERSIONEN

Dieser Abschnitt enthält Dokumentationshinweise zu früheren Outlookversionen. Er wird nicht mehr gewartet und kann daher in Details von bestehenden Installationen abweichen.

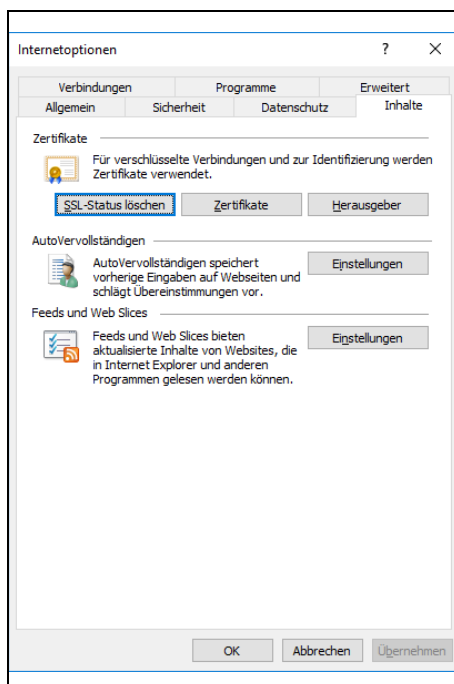
8.1 OUTLOOK 2013 – ZERTIFIKAT INSTALLIEREN UND VERWENDEN

8.1.1 ZERTIFIKAT INSTALLIEREN

8.1.1.1 ZERTIFIKAT IN WINDOWS INSTALLIEREN

Um die E-Mail Signatur in Outlook 2013 nutzen zu können, muss vorher in Windows das persönliche Zertifikat (PKCS12-Datei) im Zertifikatsspeicher installiert werden.

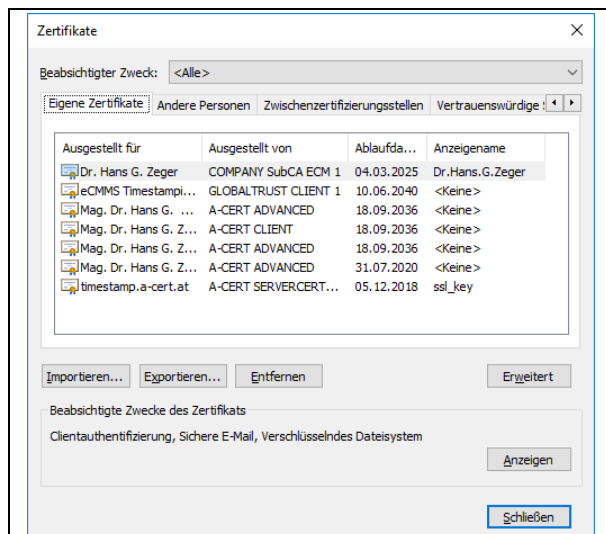
Die Installation des persönlichen Zertifikates variiert abhängig von der Windowsversion, verwendet aber immer das Eingabefenster "Internetoptionen"⁵:



Screen 106: Internetoptionen

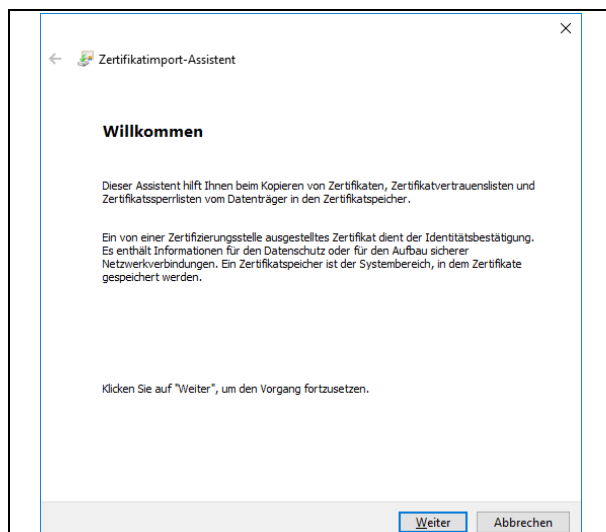
⁵ Wie Sie "Internetoptionen" bei Ihrer Windowsversion aufrufen erfahren Sie von Ihrem IT-Betreuer.

Inhalte ⇒ Zertifikate ⇒



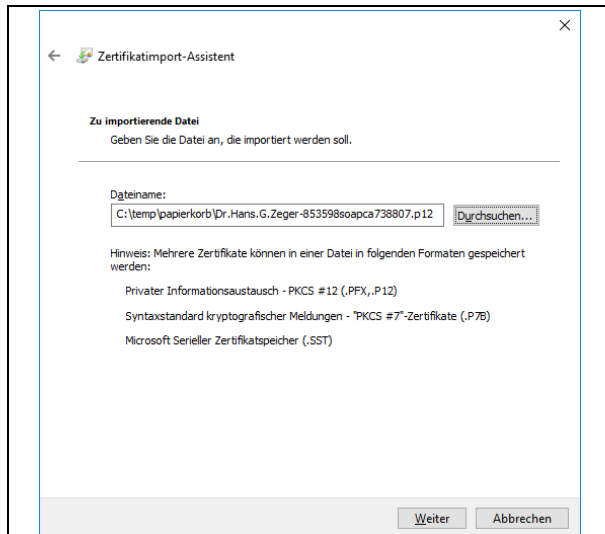
Screen 107: Zertifikatsverwaltung

Eigene Zertifikate ⇒ Importieren ⇒



Screen 108: Importassistent

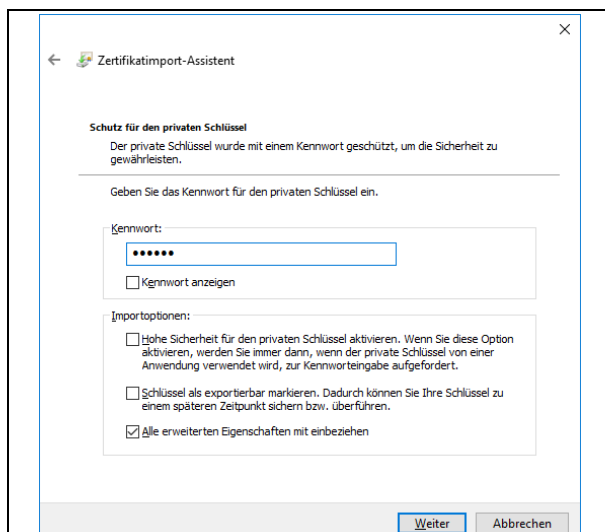
Weiter ⇨



Screen 109: Importassistent II

Auswahl geeignete PKCS12-Datei mit dem persönlichen Zertifikat

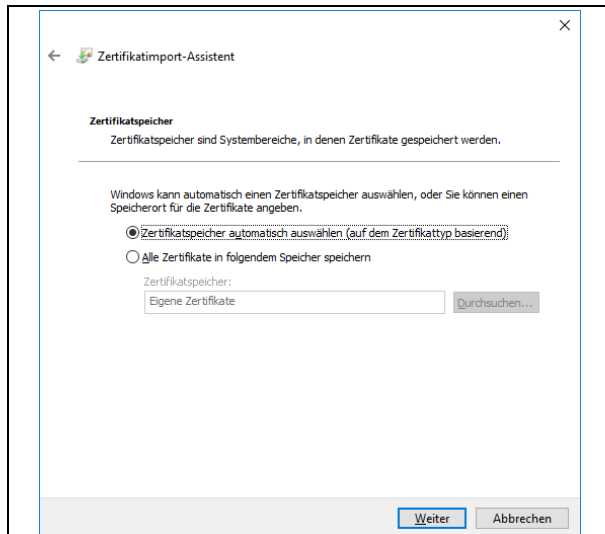
Weiter ⇨



Screen 110: Importassistent III

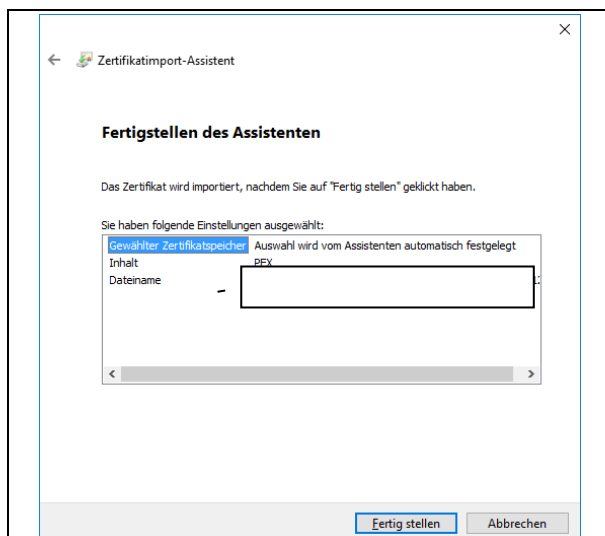
Es muss das Kennwort angegeben werden mit dem die PKCS12-Datei gesichert ist.

Weiter ⇨



Screen 111: Importassistent IV

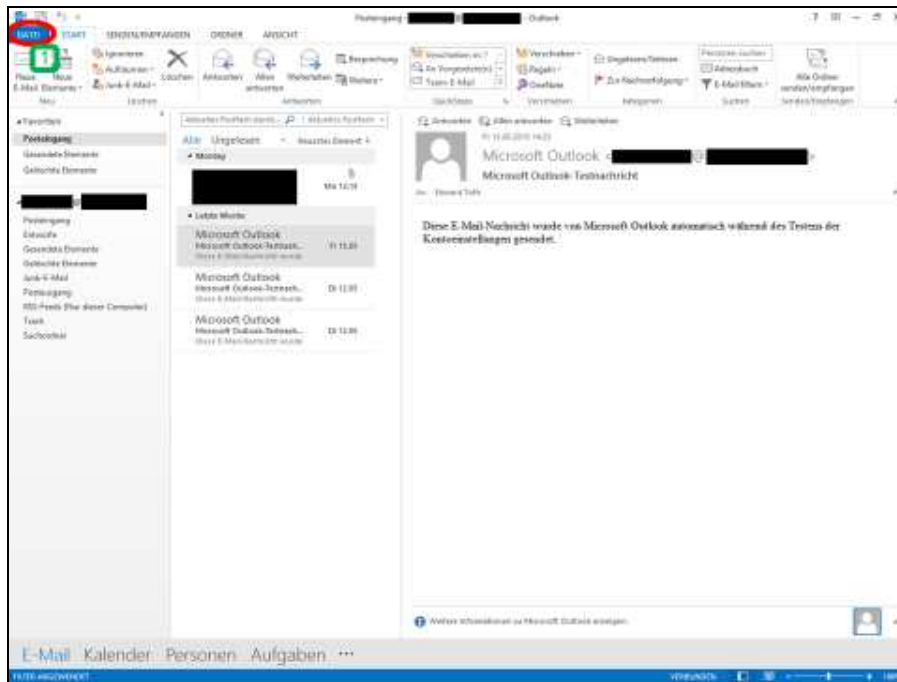
Empfohlen wird: "Zertifikatsspeicher automatisch auswählen" - es werden das persönliche Zertifikat und alle CA-Zertifikate im richtigen Windows-Zertifikatsspeicher abgelegt.



Screen 112: Importassistent V

Fertig stellen ⇨

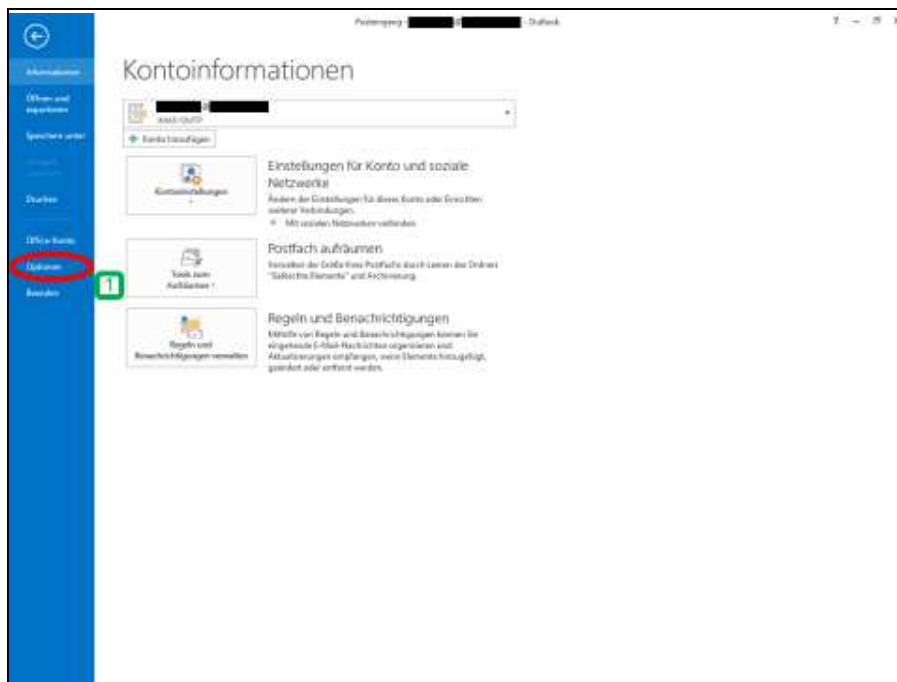
8.1.1.2 OUTLOOK 2013 MENÜ



Screen 113: Menü Outlook 2013

1 Im Hauptfenster „DATEI“ auswählen

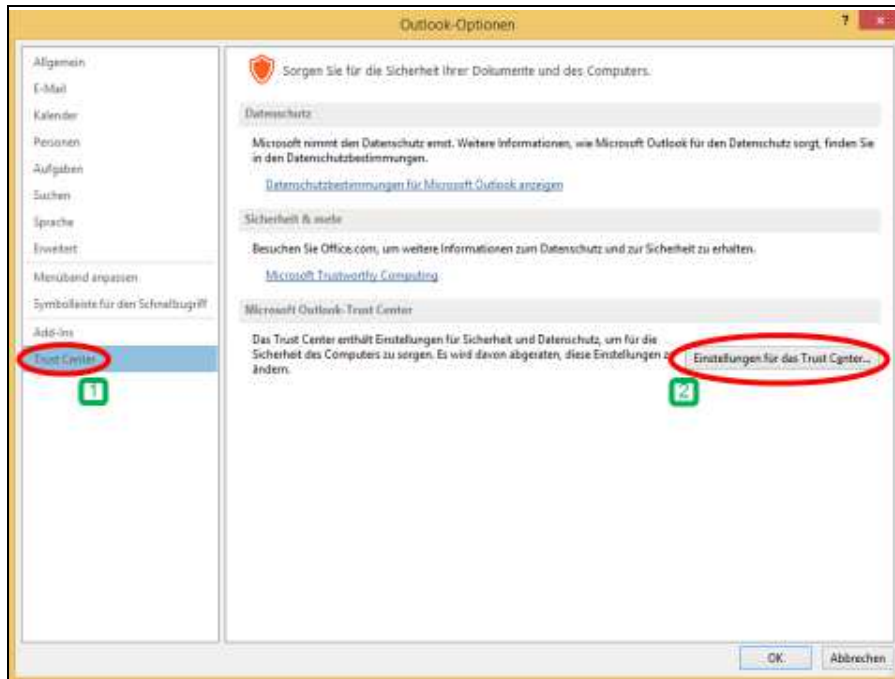
Optionen ⇒



Screen 114: Optionen wählen

1 In der linken Leiste „Optionen“ auswählen

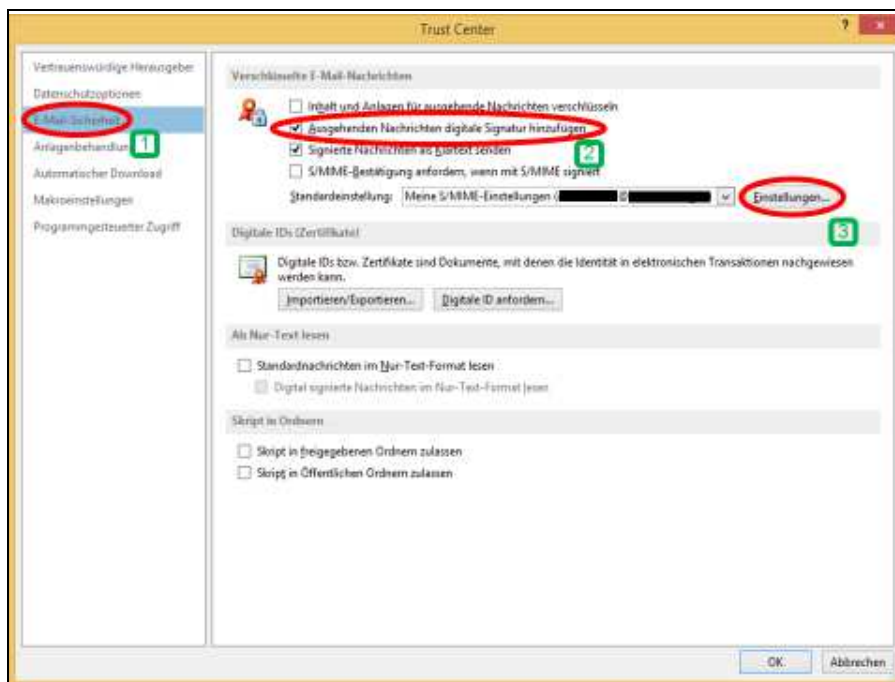
Trust Center Einstellungen ⇨



Screen 115: Trust Center Einstellungen

- 1 „Trust Center“ wählen
- 2 Im rechten Teil, den neu erschienenen Button „Einstellungen für das Trust Center...“ wählen

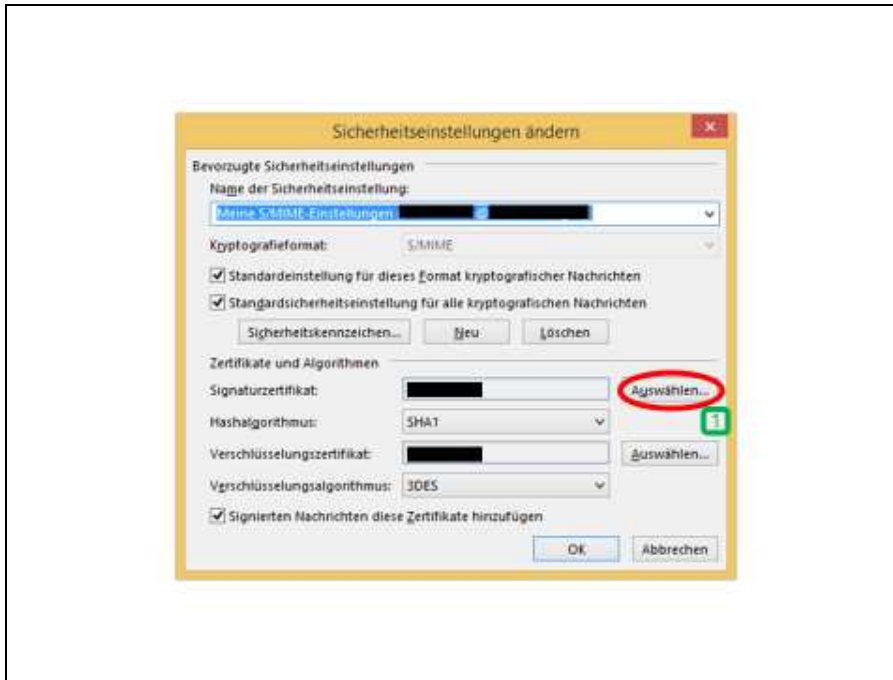
E-Mail Verschlüsselungs Einstellungen ⇨



Screen 116: E-Mail Verschlüsselungseinstellungen

- 1 Zuerst „E-Mail-Sicherheit“ wählen
- 2 Im rechten Bereich automatisches signieren von E-Mails wählen
- 3 „Einstellungen...“ auswählen

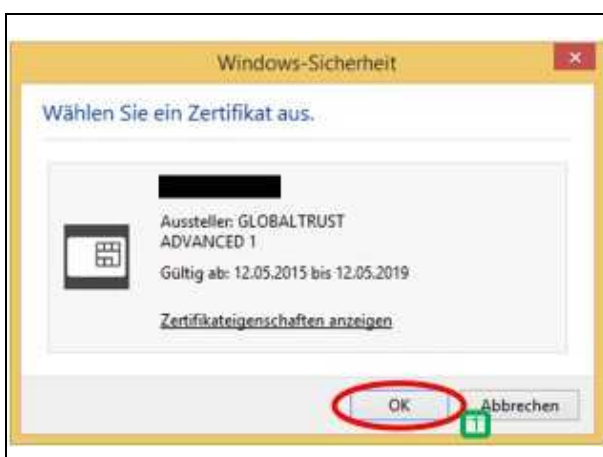
Sicherheitseinstellungen ⇨



Screen 117: Sicherheitseinstellungen

- 1 „Auswählen...“ Button betätigen um ein Signaturzertifikat hinzu zu fügen

Zertifikat wählen ⇨

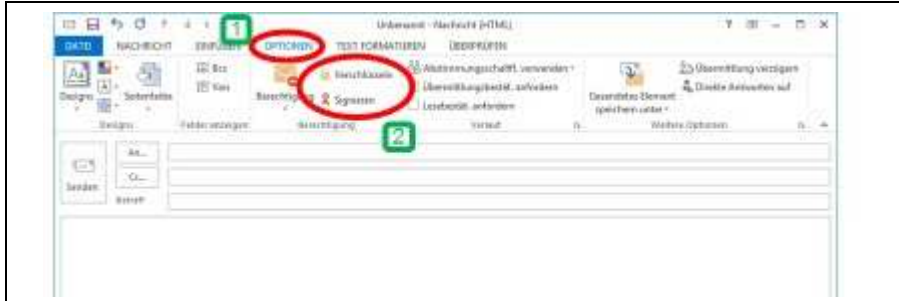


Screen 118: Zertifikat wählen

- 1 Aus der Liste der Zertifikate (im Beispiel ist nur eines zur Verfügung) das gewünschte auswählen und auf „OK“ drücken und auf die Hauptseite von Outlook zurückkehren. ⇨ Fertig

8.1.2 SIGNIERTE E-MAIL VERFASSEN UND VERSENDEN

Neue E-Mail verfassen ⇒



Screen 119: Neue E-Mail verfassen

- 1 Nachdem, wie gewohnt, ein neues Fenster geöffnet wurde um eine E-Mail zu verfassen, den „OPTIONEN“ Ribbon auswählen
- 2 In etwa der Mitte des Ribbons befinden sich der „Verschlüsseln“ und „Signieren“ Button.

E-Mail signieren ⇒



Screen 120: E-Mail signieren

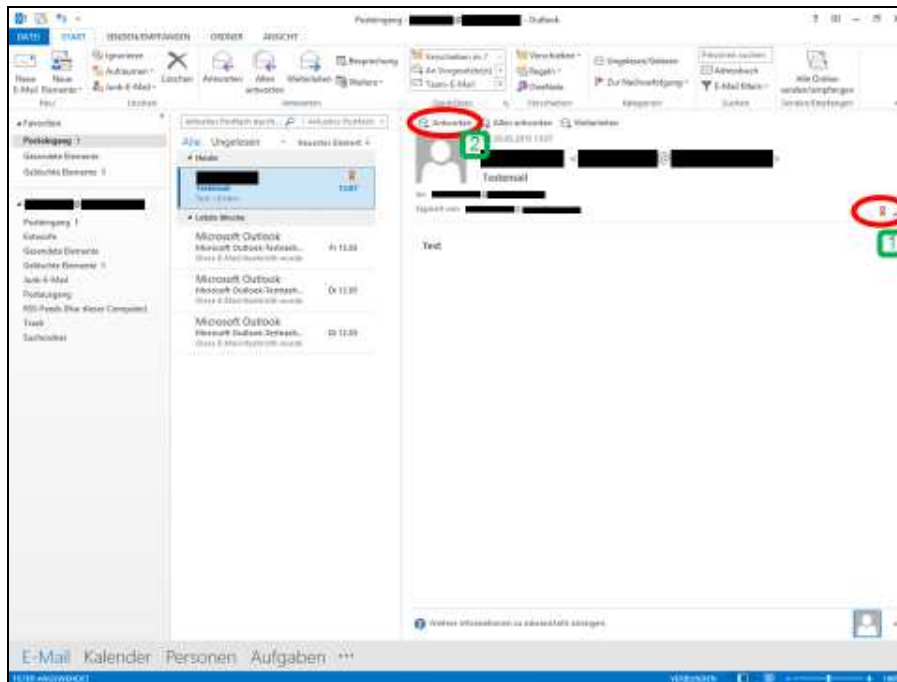
- 1 Wenn der „Signieren“ Button blau hinterlegt ist, ist nichts weiter zu tun. Die E-Mail kann wie gewohnt verfasst und versendet werden. Sollte der Button nicht blau hinterlegt sein, reicht es ihn einmal an zu klicken und die E-Mail somit zu signieren. ⇒ Fertig

8.1.3 E-MAILS VERSCHLÜSSELN

Um eine E-Mail verschlüsseln zu können, wird in jedem Fall das Zertifikat des Empfängers benötigt. Es gibt zwei Möglichkeiten dieses zu verwenden, die beide im folgenden beschrieben werden.

- Methode 1: Antwort auf eine signierte E-Mail
(siehe ⇒ Abschnitt 8.1.3.1 Methode I - Signatur erkennen und antworten, p74)
- Methode 2: Manuelles Hinzufügen eines Zertifikates zu einem Kontakt. Dazu muss im voraus das Zertifikat in Form einer Datei (Dateiendung .cer) mit dem entsprechenden Kontakt ausgetauscht werden und auf dem Computer vorliegen.
(siehe ⇒ Abschnitt 8.1.3.2 Methode II - Kontakt öffnen, p75)

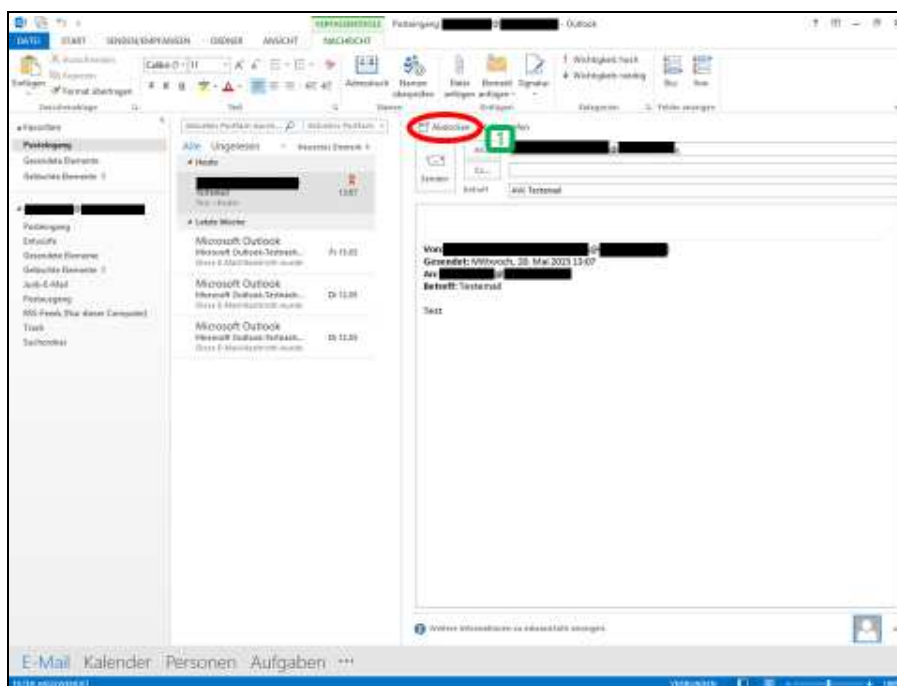
8.1.3.1 METHODE I - SIGNATUR ERKENNEN UND ANTWORTEN



Screen 121: Signatur erkennen und antworten

- 1 Wenn dieses Symbol in einer empfangenen E-Mail sichtbar ist, wurde sie von dem Absender signiert. Um die Antwort E-Mail zu verschlüsseln reicht es, wie gewohnt, zu antworten.
- 2 Auswählen des „Antworten“ Buttons

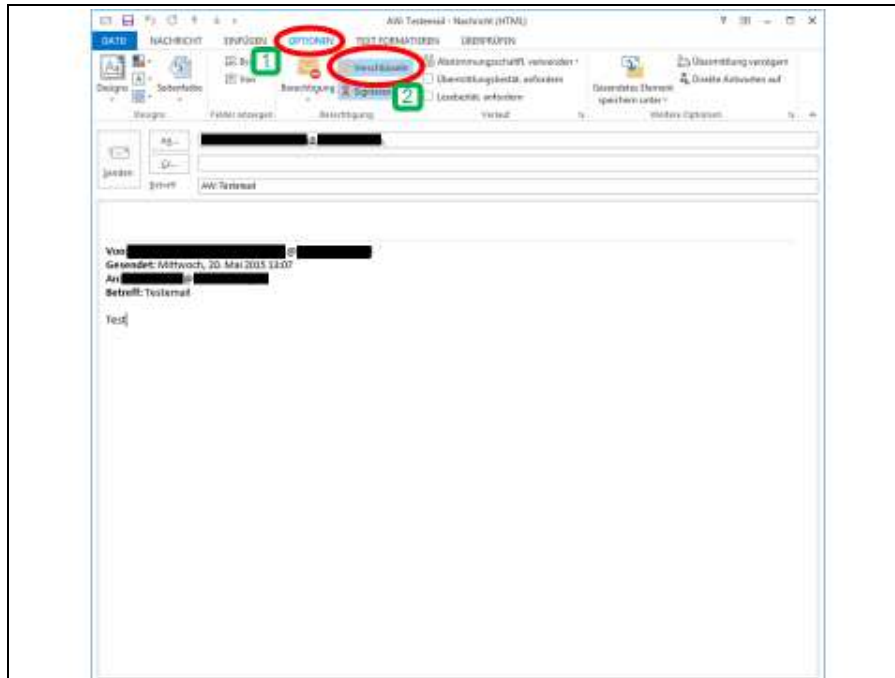
Antwort in separatem Fenster ⇒



Screen 122: Antwort in separatem Fenster

- 1 Um die Nachricht verschlüsseln zu können, wird das separate Fenster zum Verfassen von E-Mails benötigt. Um es zu öffnen „Abdocken“ auswählen

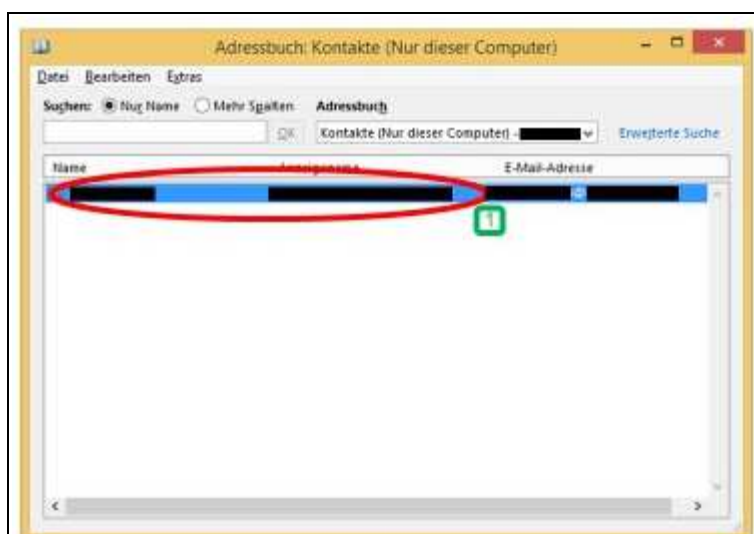
E-Mail Verschlüsseln ⇒



Screen 123: E-Mail verschlüsseln

- 1 Den „OPTIONEN“ Ribbon auswählen
 2 In etwa der Mitte des Ribbons befinden sich der „Verschlüsseln“ und „Signieren“ Button. Den „Verschlüsseln“ Button auswählen, sodass er blau hinterlegt ist. Nun, wie gewohnt, die E-Mail verfassen und versenden. Sie wird jetzt verschlüsselt übermittelt. ⇒ Fertig

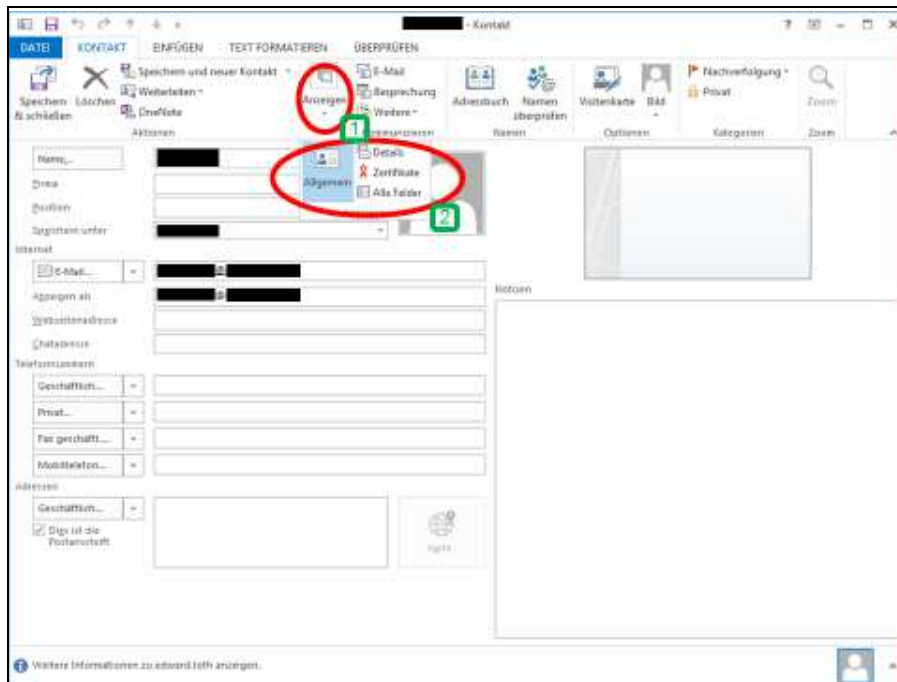
8.1.3.2 METHODE II - KONTAKT ÖFFNEN



Screen 124: Kontakte öffnen

1 Addressbuch öffnen und einen Doppelklick auf den gewünschten Kontakt machen

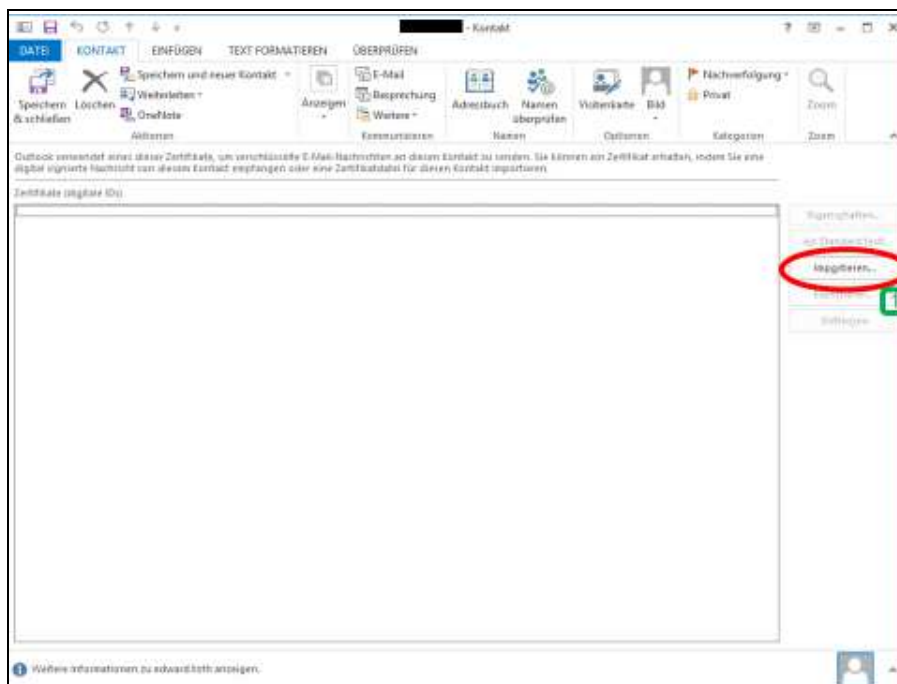
Kontakte Fenster ⇨



Screen 125: Kontakte Fenster

- 1 In „KONTAKT“ Ribbon „Anzeigen“ auswählen
- 2 Im kleinen neu erschienenen Fenster „Zertifikate“ auswählen

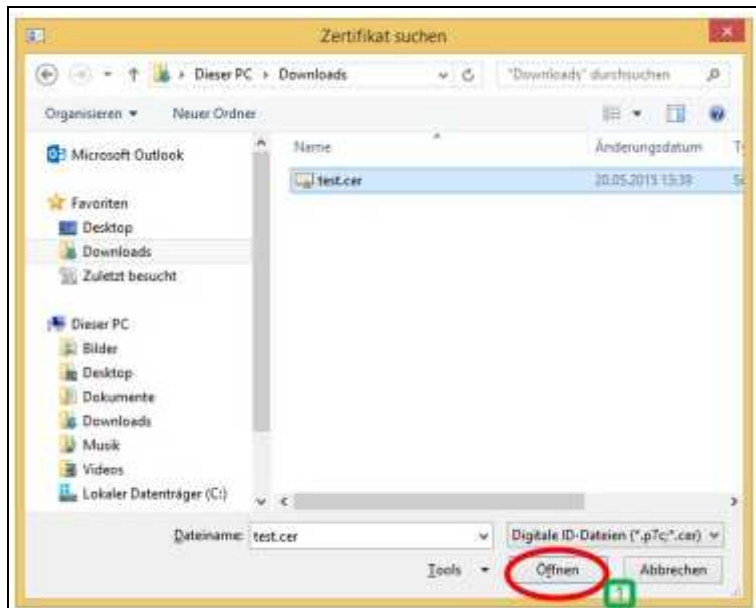
Zertifikate Fenster ⇨



Screen 126: Zertifikate Fenster

1 „Importieren...” auswählen

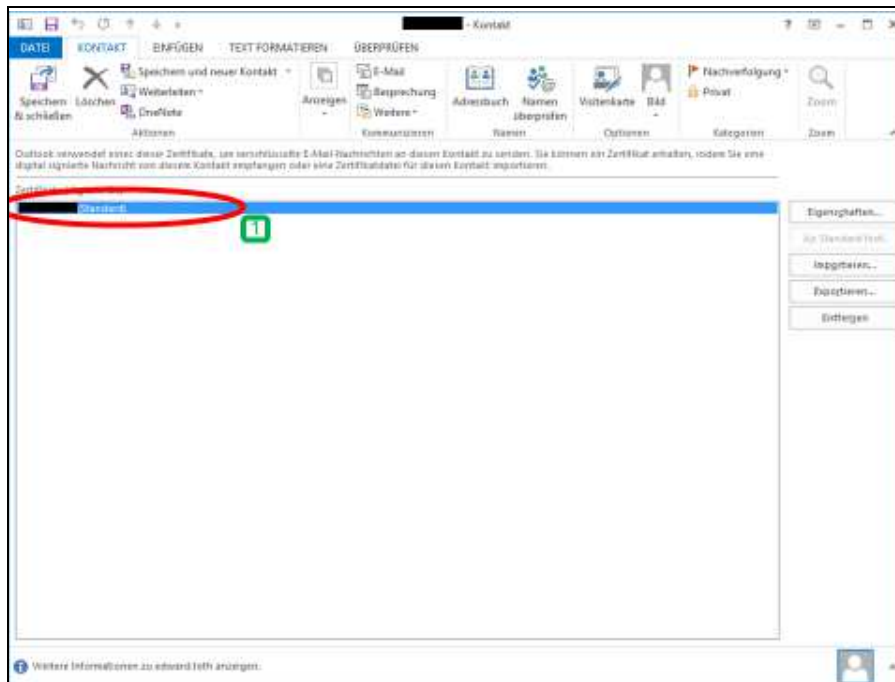
Zertifikat wählen ⇒



Screen 127: Zertifikat wählen

1 In den Ordner navigieren in dem sich das Zertifikat befindet (Dateiendung .cer), dieses auswählen und auf „Öffnen“ klicken

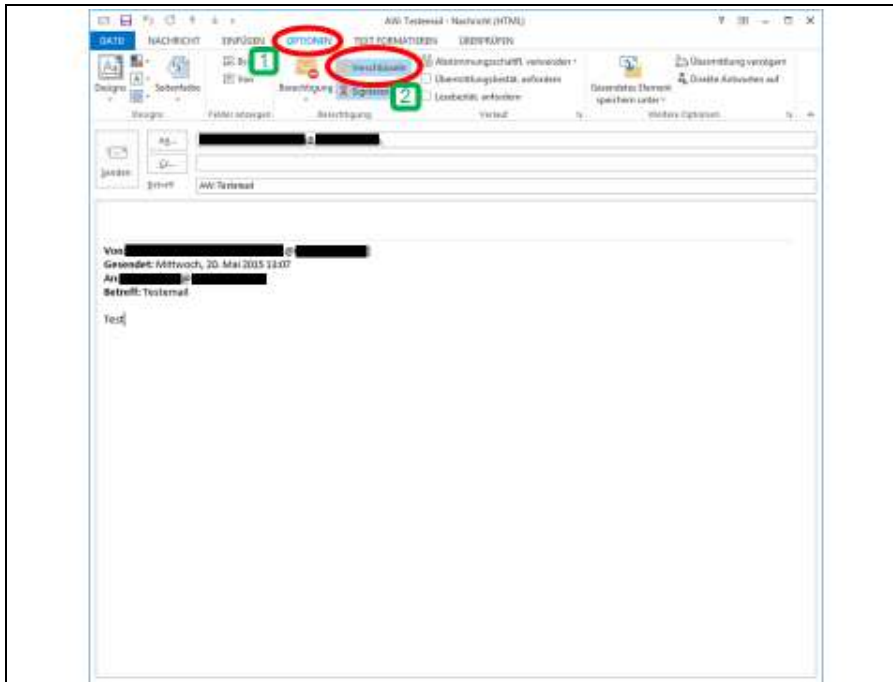
Zertifikat prüfen ⇒



Screen 128: Zertifikat prüfen

- 1 Mit einem Doppelklick auf auf den Eintrag können die Details zu dem Zertifikat aufgerufen werden, und es kann nochmal überprüft werden, ob das richtige Zertifikat ausgewählt wurde. Danach den Kontakt und das Adressbuch schließen und eine neue E-Mail verfassen.

E-Mail verschlüsseln ⇒



Screen 129: E-Mail verschlüsseln

- 1 „OPTIONEN“ Ribbon auswählen
- 2 In etwa der Mitte des Ribbons befinden sich der „Verschlüsseln“ und „Signieren“ Button. Den „Verschlüsseln“ Button auswählen, sodass er blau hinterlegt ist. Nun, wie gewohnt, die E-Mail verfassen und versenden. Sie wird jetzt verschlüsselt übermittelt. ⇒ Fertig

8.1.4 LDAP-SERVER EINRICHTEN

GLOBALTRUST stellt seinen Kunden ein LDAP Verzeichnis zur Verfügung. In diesem Verzeichnis sind alle von GLOBALTRUST ausgestellten Zertifikate zu finde. Somit ist es möglich an alle Personen mit einem GLOBALTRUST Zertifikat verschlüsselte E-Mails zu schicken. Es ist außerdem möglich dieses Verzeichnis in das Adressbuch von Microsoft Outlook zu integrieren.

8.1.4.1 KURZFASSUNG

Installation des LDAP Verzeichnisses:

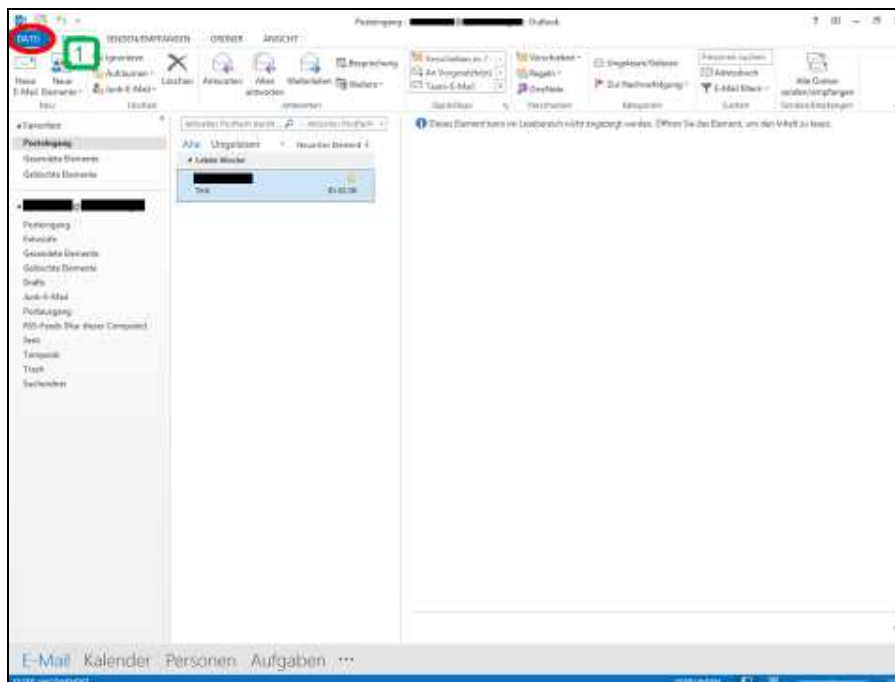
- In den Kontoeinstellungen bei Adressbüchern auf „Neu...“ klicken um ein neues Adressbuch hinzufügen zu können.
- Im Installations-wizard „Internetverzeichnisdienst (LDAP)“ auswählen.
- Als Servernamen „ldap.globaltrust.eu“ eingeben und in „Weitere Einstellungen...“ als benutzerdefinierte Suchbasis „c=at“ eingeben.
- Wizard abschließen und Outlook neu starten ⇒ Fertig

LDAP Verzeichnis verwenden:


- Adressbuch öffnen und im Dropdown Menü unter „Weitere Adressbücher“ „ldap.globaltrust.eu“ auswählen.
- In der erweiterten Suche das Suchwort in „Anzeigenname“ eingeben und bei den „Suchkriterien“ den „Enthält“ Radio-Button auswählen.
- In der Liste der gefundenen Zertifikate das gesuchte auswählen und zu den Kontakten hinzufügen. Wie gewohnt verschlüsselte Nachrichten verschicken ⇒ Fertig

8.1.4.2 INSTALLATION DES LDAP VERZEICHNISSES

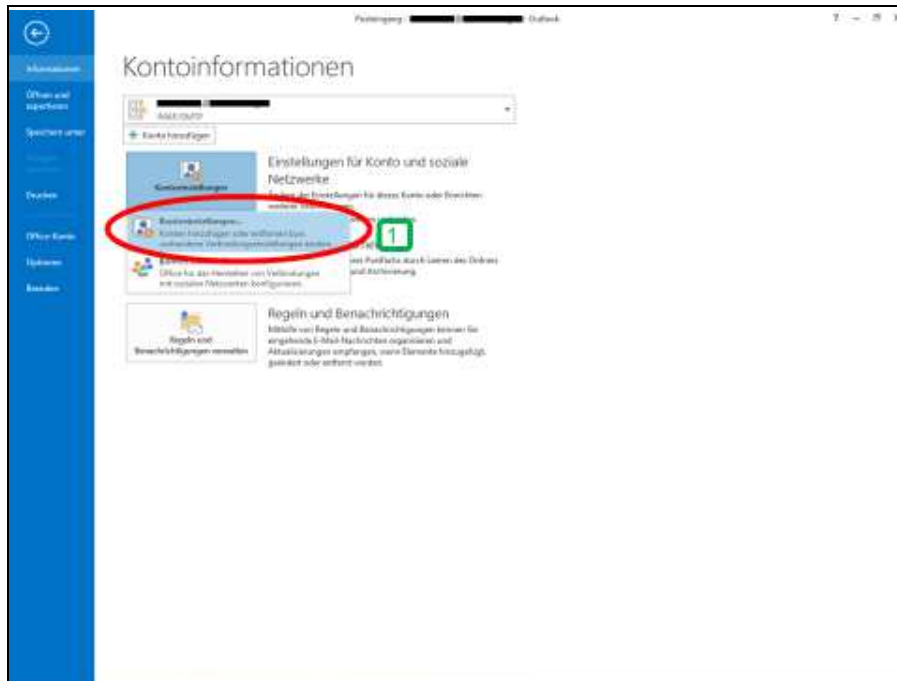
Outlook starten ⇒ DATEI ⇒



Screen 130: Outlook Datei

 Im Hauptfenster von Microsoft Outlook 2013 auf „DATEI“ klicken.

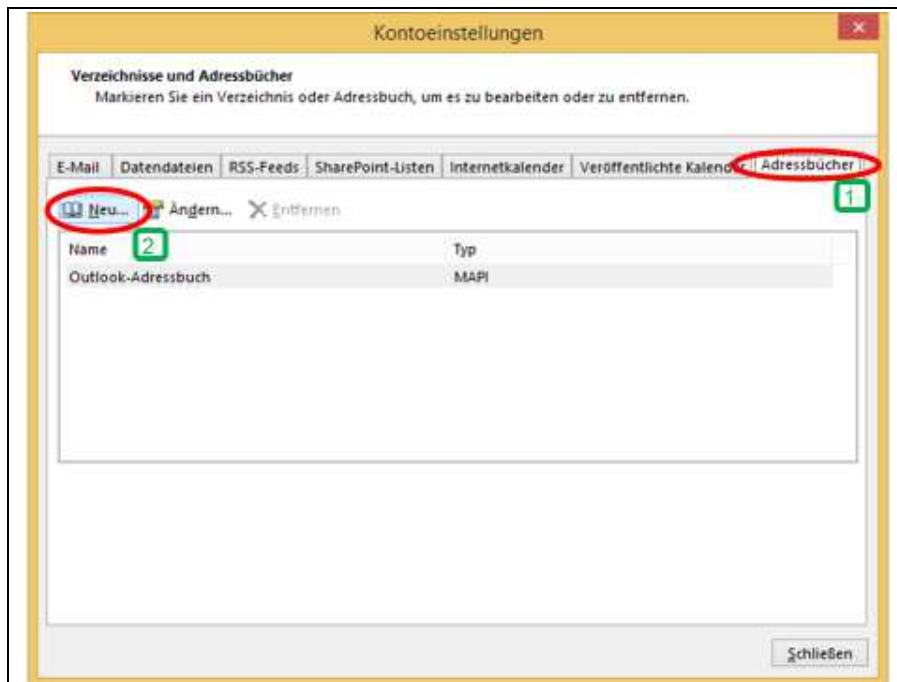
⇒ Kontoeinstellungen öffnen



Screen 131: Kontoeinstellungen öffnen

- 1 Auf „Kontoeinstellungen“ und nach dem erscheinen des Untermenüs auf „Kontoeinstellungen...“ klicken.

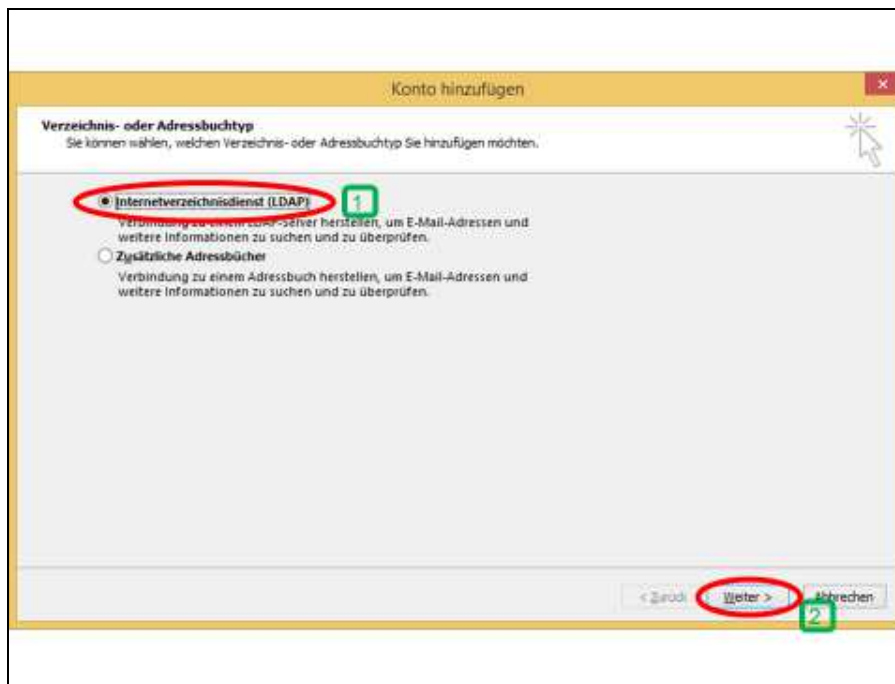
Neues Adressbuch anlegen ⇒



Screen 132: Konto Einstellungen öffnen

- 1 Im neu erschienen Fenster zum „Adressbücher“ Tab wechseln.
- 2 Auf „Neu...“ klicken um ein neues Adressbuch hinzufügen zu können.

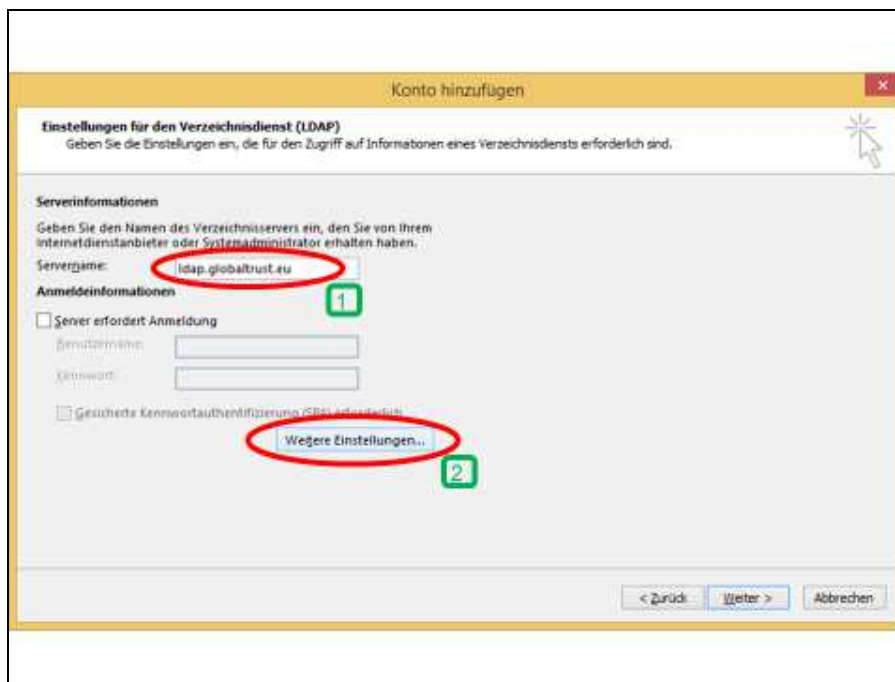
LDAP Verzeichnis wählen ⇨



Screen 133: LDAP-Verzeichnisdienst auswählen

- 1 „Internetverzeichnisdienst (LDAP)“ auswählen.
- 2 Auf „Weiter“ klicken.

Serverdaten eingeben ⇨

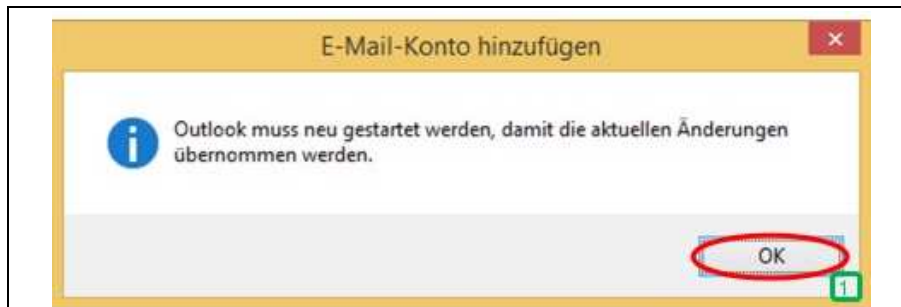


Screen 134: Serverdaten eingeben

- 1 Als Servernamen „ldap.globaltrust.eu“ eingeben.

2 Auf „Weitere Einstellungen...“ klicken.

Meldung bestätigen ⇒



Screen 135: Meldung bestätigen

1 Den „OK“ Button klicken um fortzufahren

Weitere Serverdaten eingeben ⇒



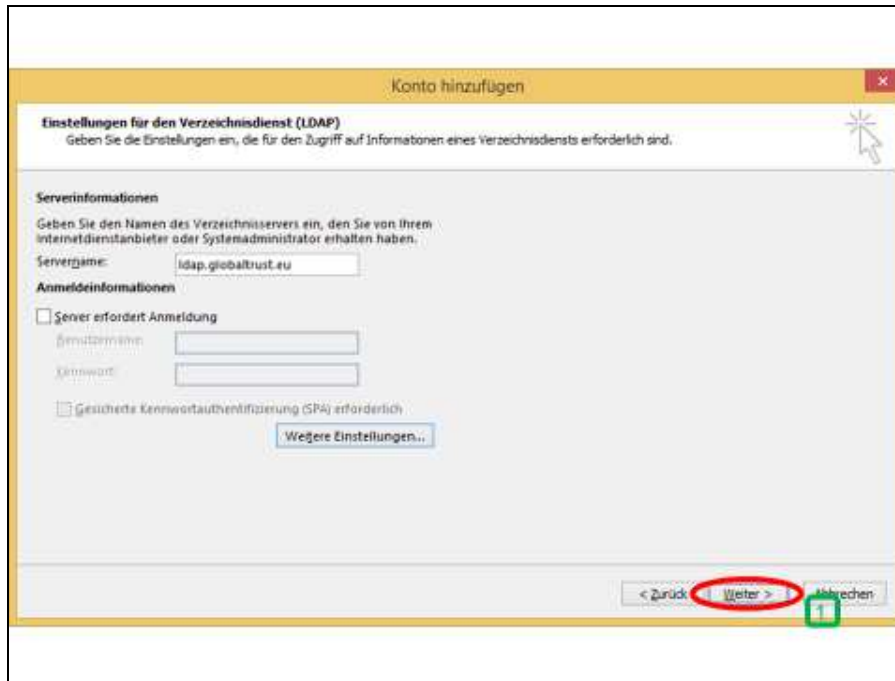
Screen 136: Weitere Serverdaten eingeben

1 In den Tab „Suche“ wechseln

2 In der Kategorie „Suchbasis“ bei „Benutzerdefiniert“ muss noch „c=at“ eingegeben werden.

3 Auf „OK“ klicken um fortzufahren.

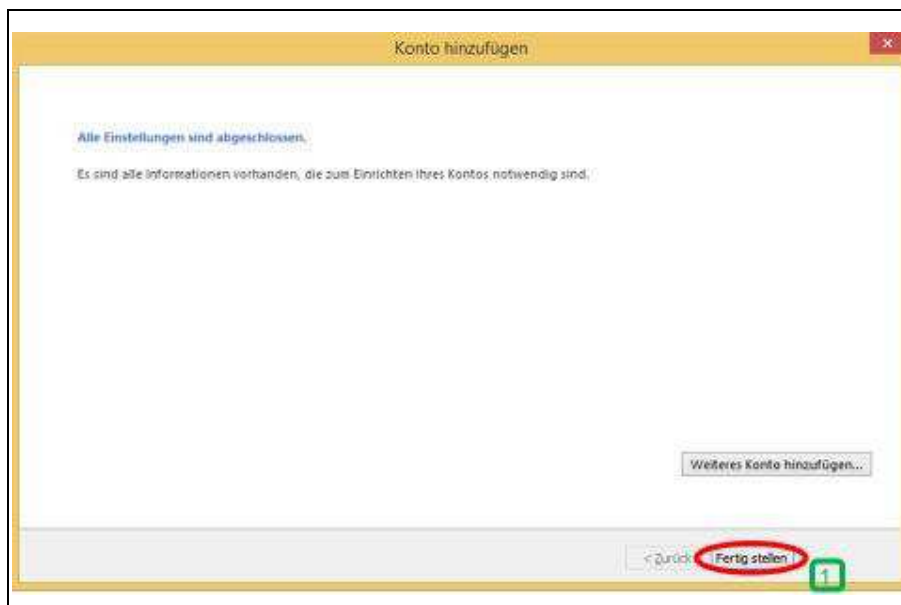
Installation fortfahren ⇨




Screen 137: Installation fortfahren

 Auf „Weiter“ klicken.

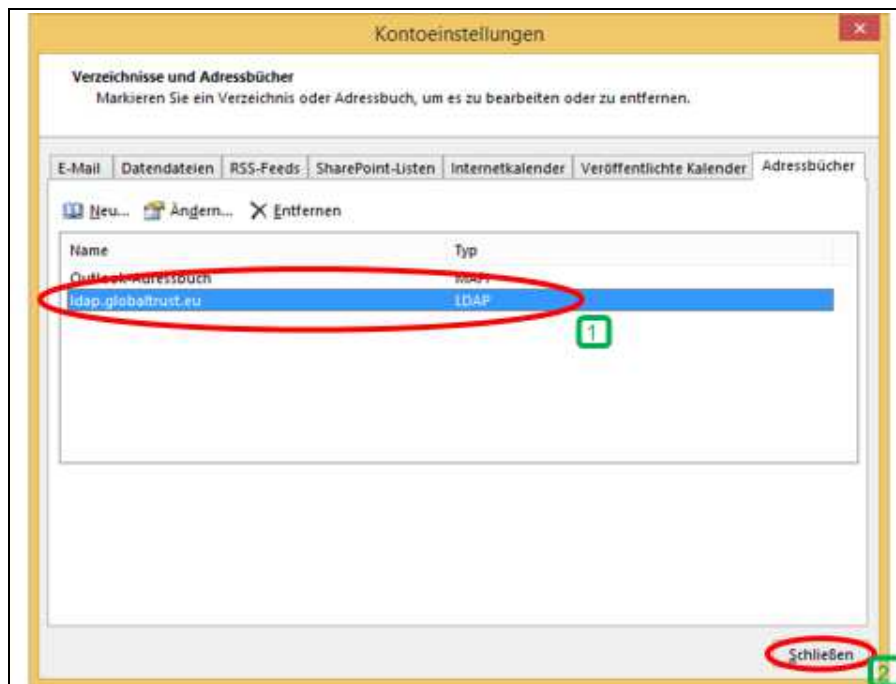
Installation fertig stellen ⇨



Screen 138: Installation fertig stellen

 Auf „Fertig stellen“ klicken um die Installation zu beenden.

Kontoeinstellungen ⇨

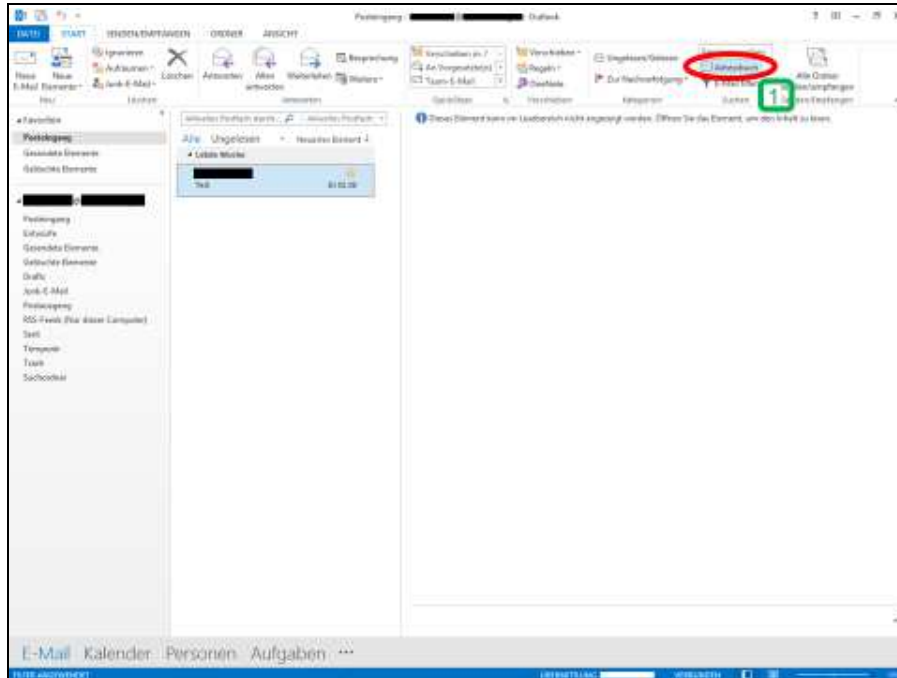


Screen 139: Kontoeinstellungen

- 1 In der Liste der Adressbücher gibt es nun einen neuen Eintrag für das LDAP Verzeichnis.
- 2 Auf „Schließen“ klicken und **Microsoft Outlook 2013 neu Starten** um die Installation abzuschließen. ⇨ Fertig

8.1.5 LDAP VERZEICHNIS VERWENDEN

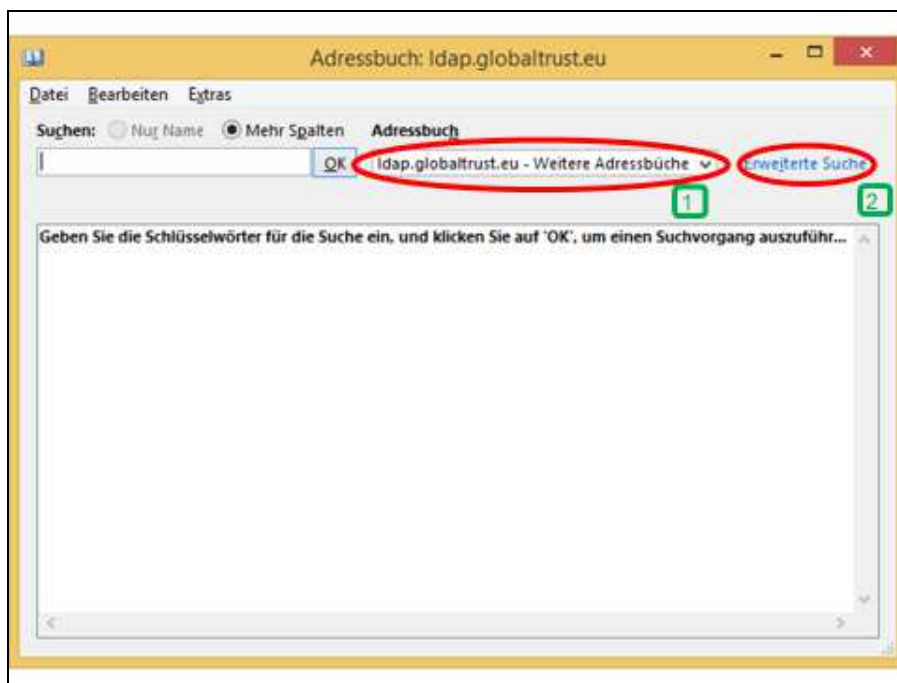
Adressbuch öffnen ⇒



Screen 140: Adressbuch öffnen

1 Im Hauptfenster auf den Button für das Adressbuch klicken.

LDAP Adressbuch wählen ⇒



Screen 141: LDAP-Adressbuch auswählen

- 1 Im Dropdown Menü unter „Weitere Adressbücher“ das Adressbuch „ldap.globaltrust.eu“ auswählen.
- 2 Auf „Erweiterte Suche“ klicken.

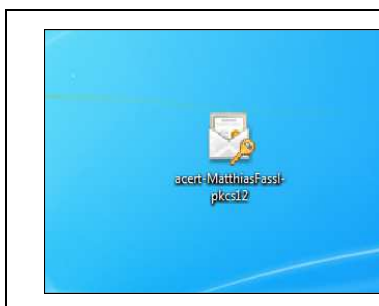
Erweiterte Suche ⇨

Screen 142: LDAP Erweiterte Suche

- 1 Im Feld „Anzeigename“ den Namen der gewünschten Person eingeben.
- 2 In der Kategorie „Suchkriterien“ „Enthält“ auswählen.
- 3 Auf „OK“ klicken um die Suche zu starten. Danach erscheint eine Liste der gefundenen Einträge. Den gewünschten auswählen. ⇨ Fertig

8.2 OUTLOOK 2007/2010 – ZERTIFIKAT INSTALLIEREN UND VERWENDEN

8.2.1 ZERTIFIKAT INSTALLIEREN



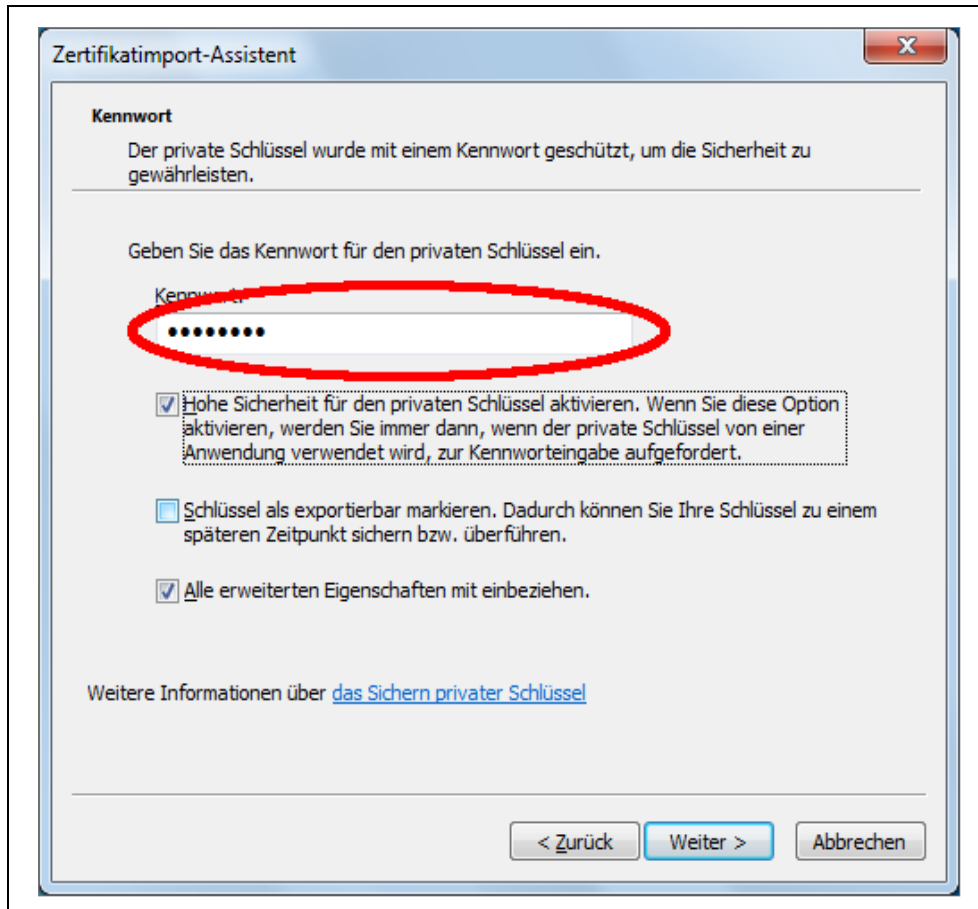
Screen 143: Anzeige PKCS12-Datei

Um die Zertifikatsdatei PKCS#12 Datei zu installieren, genügt es einen Doppelklick auf die Datei auszuführen ⇒



Screen 144: Zertifikats Import-Assistent

Weiter ⇒ Weiter ⇒



Screen 145: Zertifikats Import-Assistent II

Hier müssen Sie das *Schlüsselpasswort/Downloadpasswort* eingeben, welches Sie beim Herunterladen Ihres Zertifikats auf der GLOBALTRUST Webseite angegeben haben.

Falls Sie keine Massensignatur benötigen, können Sie den Punkt „**Hohe Sicherheit für den privaten Schlüssel aktivieren.**“ auswählen.

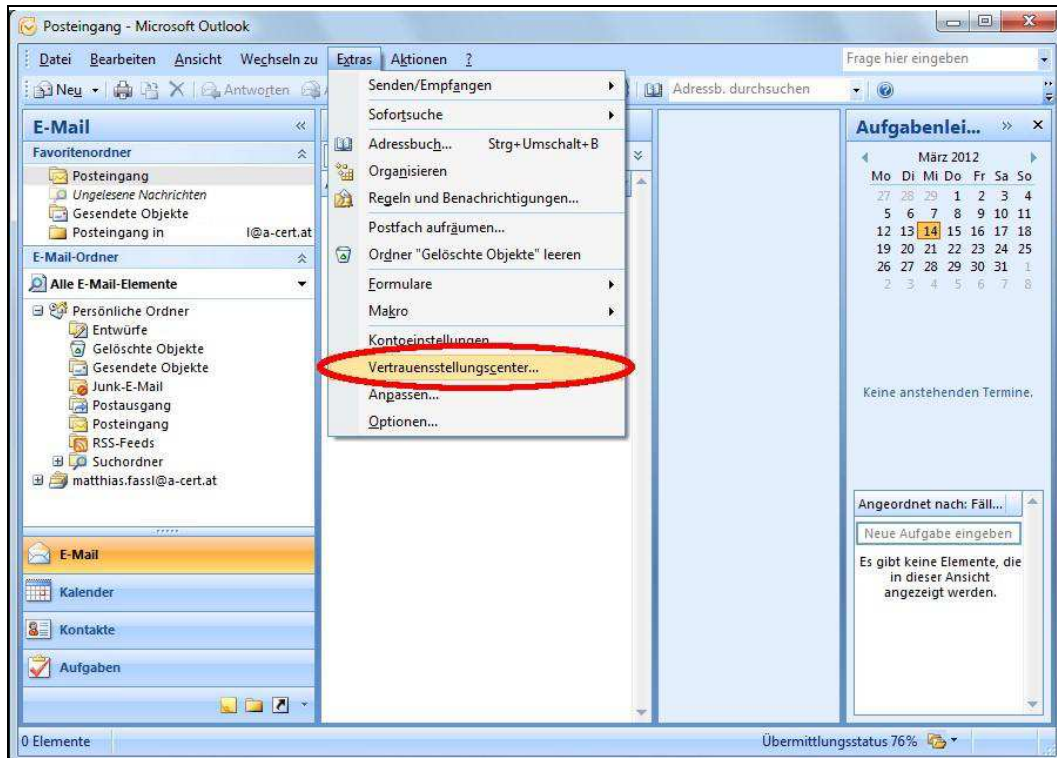
Alle weiteren Fenster im Zertifikatimport-Assistenten können Sie mit „**Weiter >**“ überspringen. Am Ende kommt eine kurze Bestätigung „*Der Importvorgang war erfolgreich*“.

8.2.2 OUTLOOK KONFIGURIEREN - VERTRAUENSSTELLUNGSCENTER ÖFFNEN

Nun können Sie Microsoft Outlook 2007 starten und das Vertrauensstellungscenter öffnen. Sie finden das Vertrauensstellungscenter unter dem Menü-Eintrag Extras.

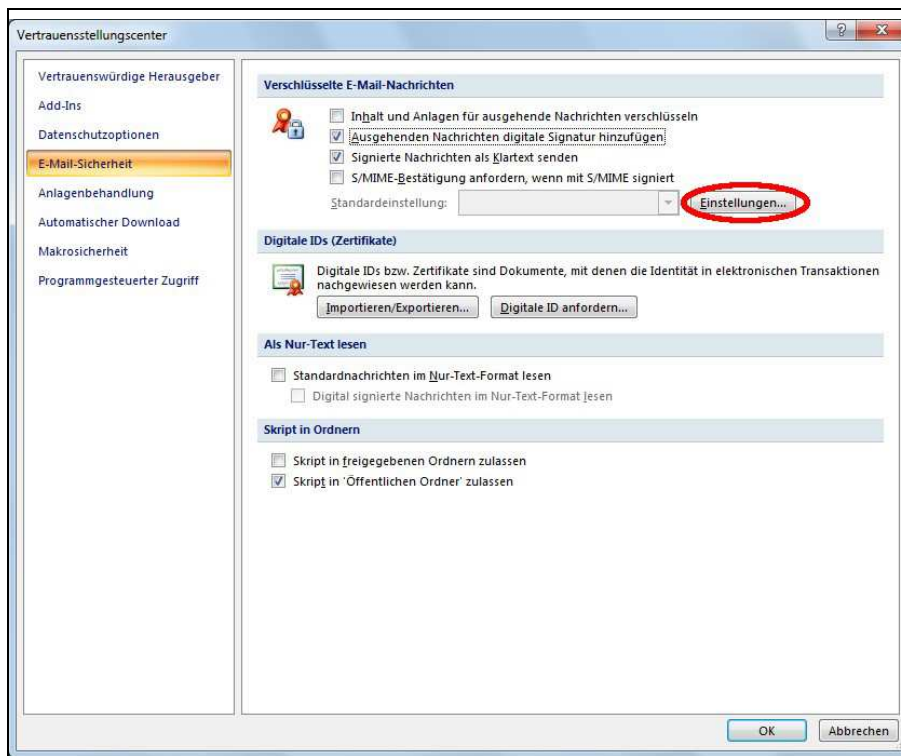
(bei Microsoft Outlook 2010 finden Sie dieses Fenster unter Office Schaltfläche ⇒ Optionen ⇒ Sicherheitscenter ⇒ Einstellungen für das Sicherheitscenter)

Menü ⇒ Extras ⇒



Screen 146: Vertrauenscenter I

Vertrauensstellungscenter... ⇒ E-Mail Sicherheit ⇒



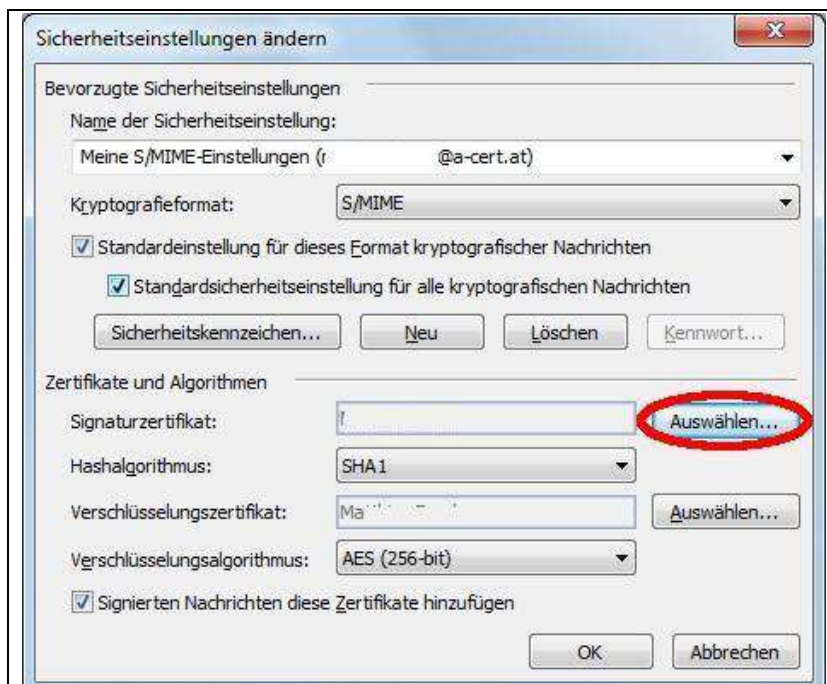
Screen 147: Vertrauenscenter II

Wir empfehlen die Option „**Ausgehenden Nachrichten digitale Signatur hinzufügen**“ auszuwählen, damit alle Ihrer ausgehenden E-Mails signiert werden.

Optional können Sie auch „**Inhalt und Anlagen für ausgehende Nachrichten verschlüsseln**“ auswählen, damit alle Ihre ausgehenden E-Mails (wenn möglich) verschlüsselt werden.

Signatur Zertifikat auswählen

Wenn Sie nun „**Einstellungen...**“ auswählen, kommen Sie zu einem neuen Fenster in dem Sie das Zertifikat für die Signatur Ihrer E-Mails auswählen können.



Screen 148: Sicherheitseinstellungen eintragen

Jetzt können Sie bei dem Punkt „**Signaturzertifikat**“ den Knopf „**Auswählen...**“ auswählen, um zu einer Übersicht Ihrer installierten Zertifikate zu kommen.



Screen 149: Zertifikat auswählen

Hier muss das Zertifikat, welches Sie installiert haben, ausgewählt werden. Das ausgewählte Zertifikat wird jetzt für die Signatur und die Verschlüsselung Ihrer E-Mails verwendet.

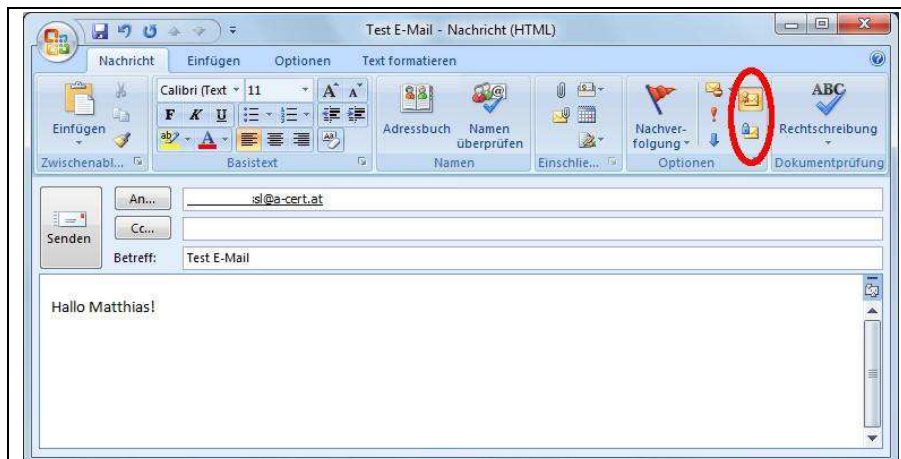
Verschlüsselung Zertifikat auswählen (optional)

Falls Sie zum Verschlüsseln Ihrer E-Mails ein anderes Zertifikat verwenden wollen, müssen Sie dieses separat auswählen.

Dafür klicken Sie auf dem unteren „**Auswählen...**“ Knopf neben dem Feld „**Verschlüsselungszertifikat**“ und wählen ein weiteres Zertifikat aus.

8.2.3 E-MAILS SIGNIEREN UND/ODER VERSCHLÜSSELN

Um nun eine E-Mail die Sie schreiben zu signieren oder zu verschlüsseln können Sie entweder das Icon mit dem versiegelten Brief (um zu signieren) und/oder das Icon mit dem Schloss vor dem Brief auswählen.

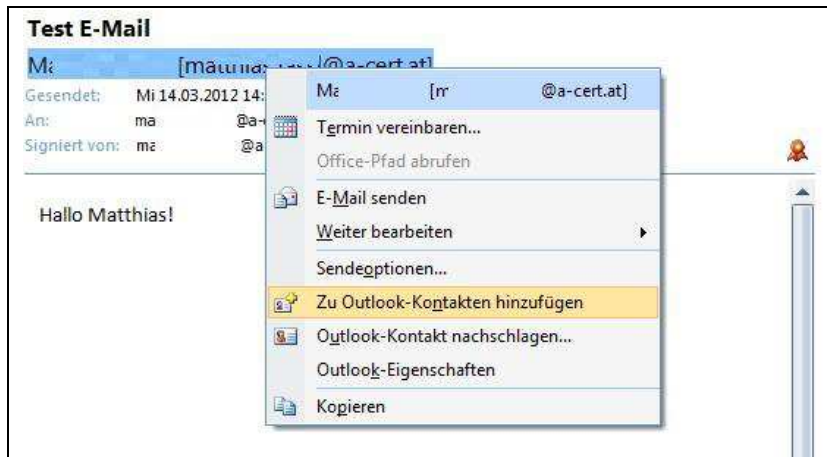


Screen 150: E-Mail schreiben und signieren

Sie finden die beiden Icons im Ribbon unter **Nachricht** ⇒ **Optionen**.

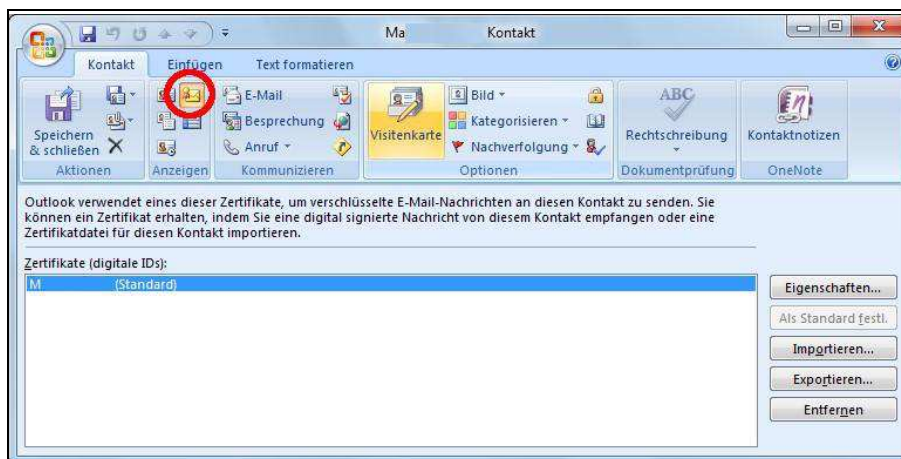
Damit Sie jemanden eine verschlüsselte E-Mail schreiben können, benötigen Sie dessen Zertifikat. Um das Zertifikat einer Kontaktperson abzuspeichern, genügt eine signierte E-Mail dieser Person, dort können Sie nach einem Rechtsklick auf die E-Mail die Option „**Zu Outlook-Kontakten hinzufügen**“ auswählen.

Anschließend können Sie dieser Person verschlüsselte E-Mails schicken.



Screen 151: E-Mail Adresse zu den Kontakten hinzufügen

Um einen Überblick über die Zertifikate zu bekommen, die Outlook für die Verschlüsselung einer E-Mail verwenden kann, öffnet man den Reiter „Kontakt“ und wählt das Icon für Zertifikate, welches Sie im Unterpunkt „Anzeigen“ finden.



Screen 152: Übersicht Outlook Kontaktliste

Signierte und/oder verschlüsselte E-Mails überprüfen

Falls Sie folgendes Symbol sehen, wurde die E-Mail signiert. Wenn Sie zusätzlich noch ein Schloss daneben sehen, wurde die E-Mail auch verschlüsselt.



Screen 153: Test E-Mail