

Signieren und Verschlüsseln von E-Mails mit Outlook ^{*)}

Durch Verwendung eines persönlichen Zertifikates (Benutzerzertifikat) können E-Mails digital unterschrieben (**signiert**) und oder **verschlüsselt** werden. Die digitale Signatur gewährleistet dem Empfänger, dass die versendeten E-Mails vom Versender verfasst und beim Übermitteln nicht verändert wurden. Das Verschlüsseln von E-Mails empfiehlt sich unbedingt für sensible Daten, da diese sonst ungeschützt übertragen werden. Der folgende Text beschreibt die benötigten Arbeitsschritte, um E-Mails mit Outlook zu signieren und zu verschlüsseln (Version Outlook 2016).

- Voraussetzungen
- 1. Installation des persönlichen Zertifikats und Anbindung an das eigene Mailkonto
- 2. Signieren von E-Mails mit Outlook 2016
 - 2.1 Erzeugen einer E-Mail mit persönlicher Signatur
 - 2.2 Prüfen der Signatur einer empfangenen E-Mail
- 3. Verschlüsseln von E-Mails mit Outlook 2016
 - 3.1 Öffentlichen Schlüssel des Empfängers verfügbar machen
 - 3.2 Erzeugen einer verschlüsselten E-Mail
 - 3.3 Lesen einer verschlüsselten E-Mail

Voraussetzungen

1. Ein Mailkonto in Microsoft Outlook 16 oder ähnliche Version (bei der Einrichtung hilft Ihnen Ihr IT-Betreuer).
2. Ein **persönliches Zertifikat** (Benutzerzertifikat) (für den Privatgebrauch gibt es Gratisanbieter von Zertifikaten wie zB Comodo; für geschäftlichen Gebrauch sind Zertifikate bei GlobalSign, a-trust und andere Dienstanbieter erhältlich; wenden Sie sich bitte an Ihren IT-Betreuer; es handelt sich um ein sogenanntes S/MIME-Zertifikat).
3. Im ersten Schritt wird beschrieben, wie das **persönliche Zertifikat** unter Outlook 2016 installiert wird. Dieser Schritt ist zwingend notwendig, um E-Mails zu signieren und oder zu verschlüsseln. Das Installationsverfahren und die Anbindung an das eigene E-Mailkonto wird im Folgenden beschrieben:

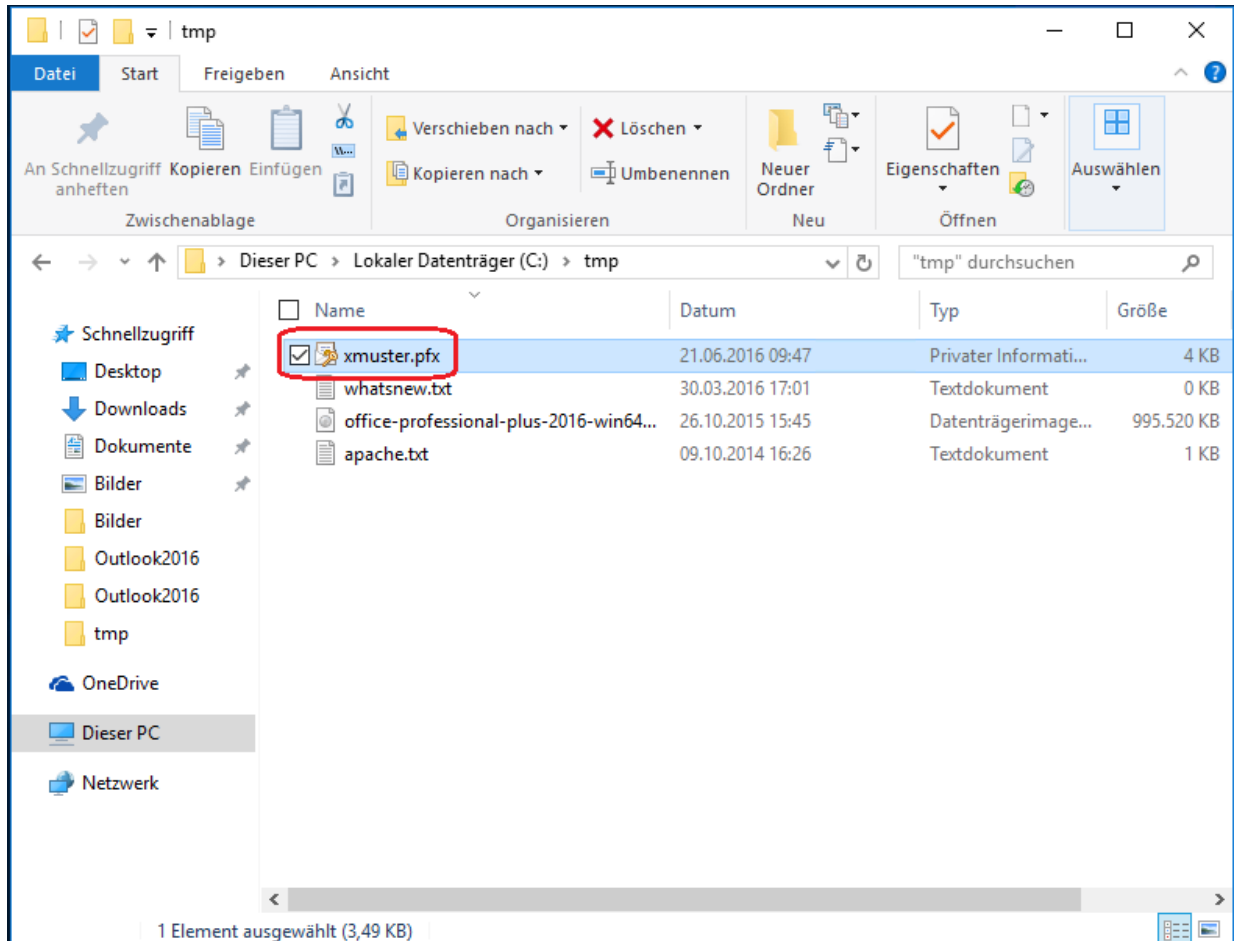
1. Installation des persönlichen Zertifikats und Anbindung an das eigene Mailkonto

Für die Beschaffung und Installation des persönlichen Zertifikates wenden Sie sich bitte bei Bedarf an ihren IT-Betreuer. Ablage des Zertifikates im Zertifikatsspeicher.

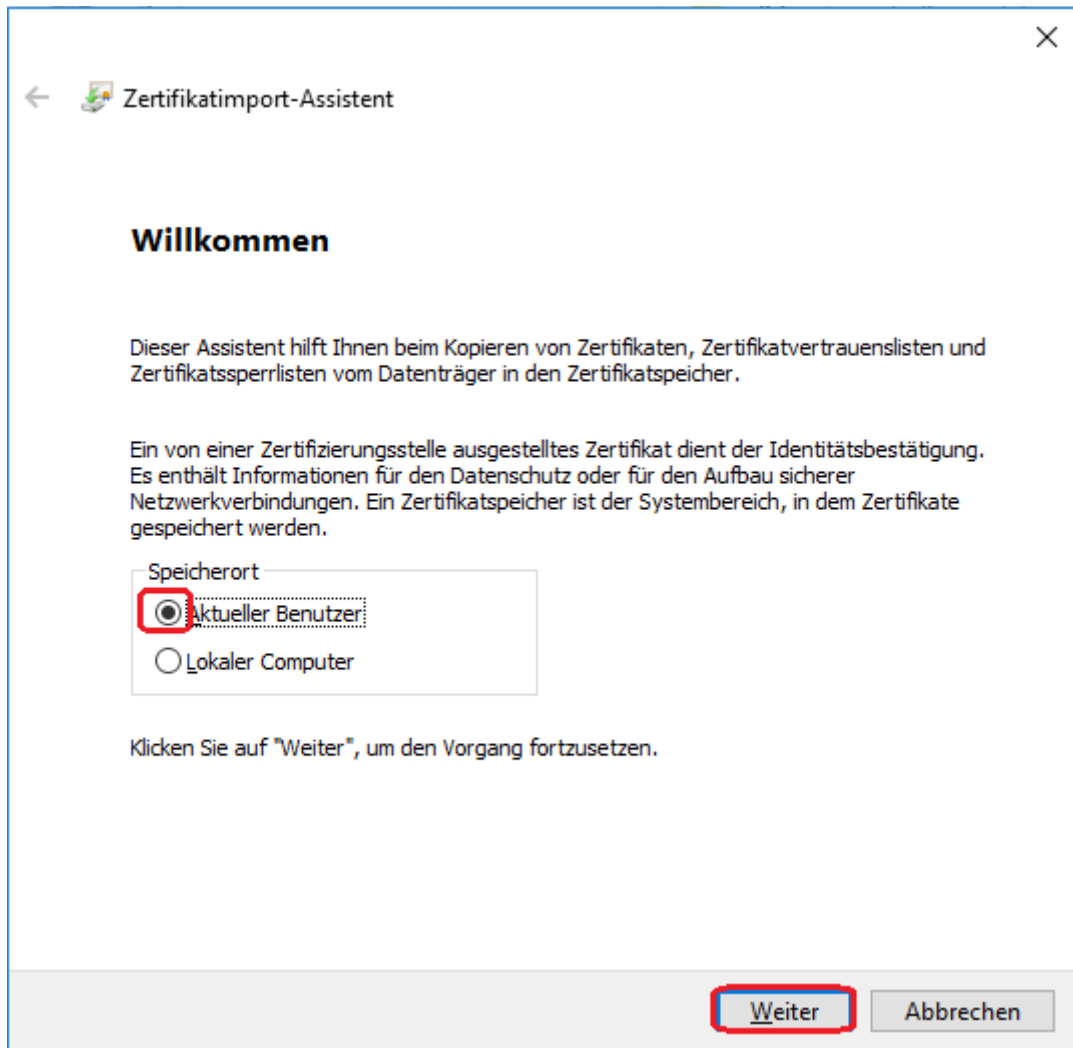
Hinweis: Wurde zum Beantragen des persönlichen Zertifikates und zum Importieren des persönlichen Zertifikates der **Internet Explorer** als Browser genutzt, erübrigen sich der Export des Zertifikates sowie die Arbeitsschritte 1 bis 7 des anschließenden Abschnittes, da das persönliche Zertifikat bereits an der richtigen Stelle im Zertifikatsspeicher vorliegt. In diesem Fall geht es bei Punkt 8 mit der Anbindung des Zertifikates an das Mailkonto weiter. Wurde zum Beantragen des persönlichen Zertifikates ein anderer Browser genutzt, muss dieses als Datei im **PKCS#12-Format** (dies entspricht den Dateitypen **pxf** beziehungsweise **p12**) vorliegen. Dazu wird es aus dem Browser exportiert, über den es beantragt wurde. (siehe: Zertifikate aus Browsern exportieren)

Nachdem das persönliche Zertifikat exportiert als Datei vorliegt (hier: **xmustercerkey.pfx**), erfolgt die Installation.

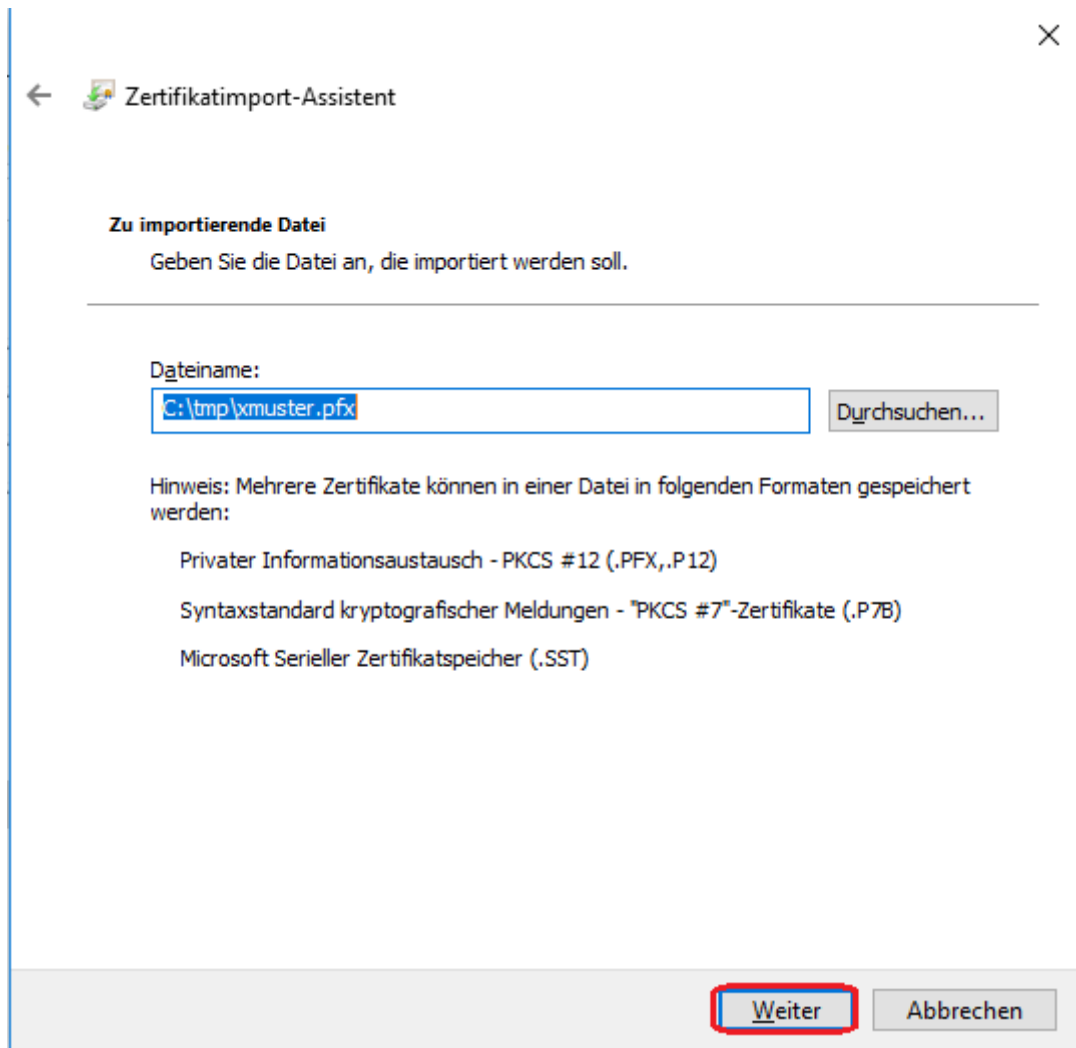
1. Dazu wird im ersten Schritt über den Datei-Browser (Windows Explorer) die Zertifikatsdatei "**xmustercertkey.pfx**" aus dem Verzeichnis **C:\tmp** (siehe: Zertifikate aus Browsern exportieren) doppelt angeklickt.



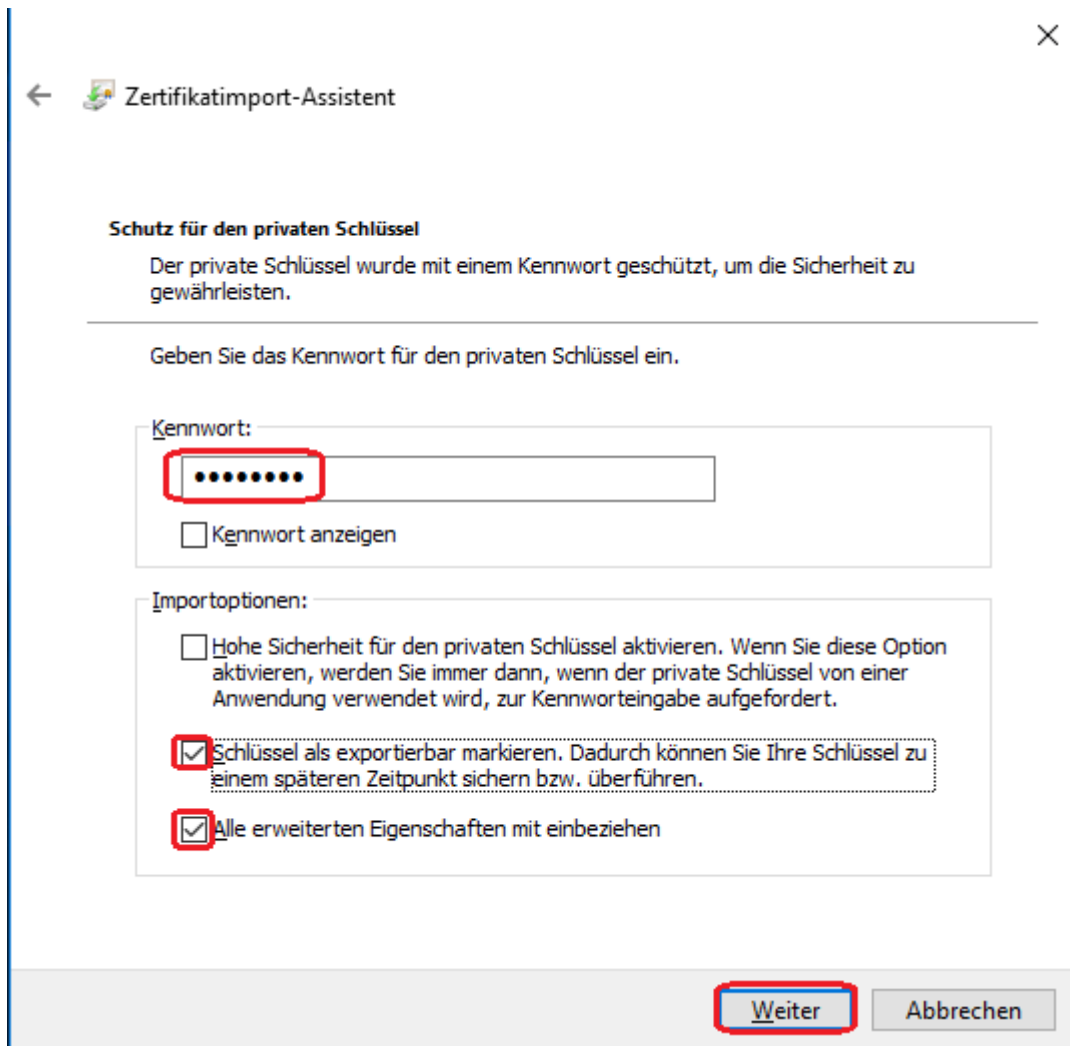
2. Es startet der "**Zertifikatimport-Assistent**". Hier ist die Option "**Aktueller Benutzer**" zu selektieren und mit "**Weiter**" zu bestätigen.



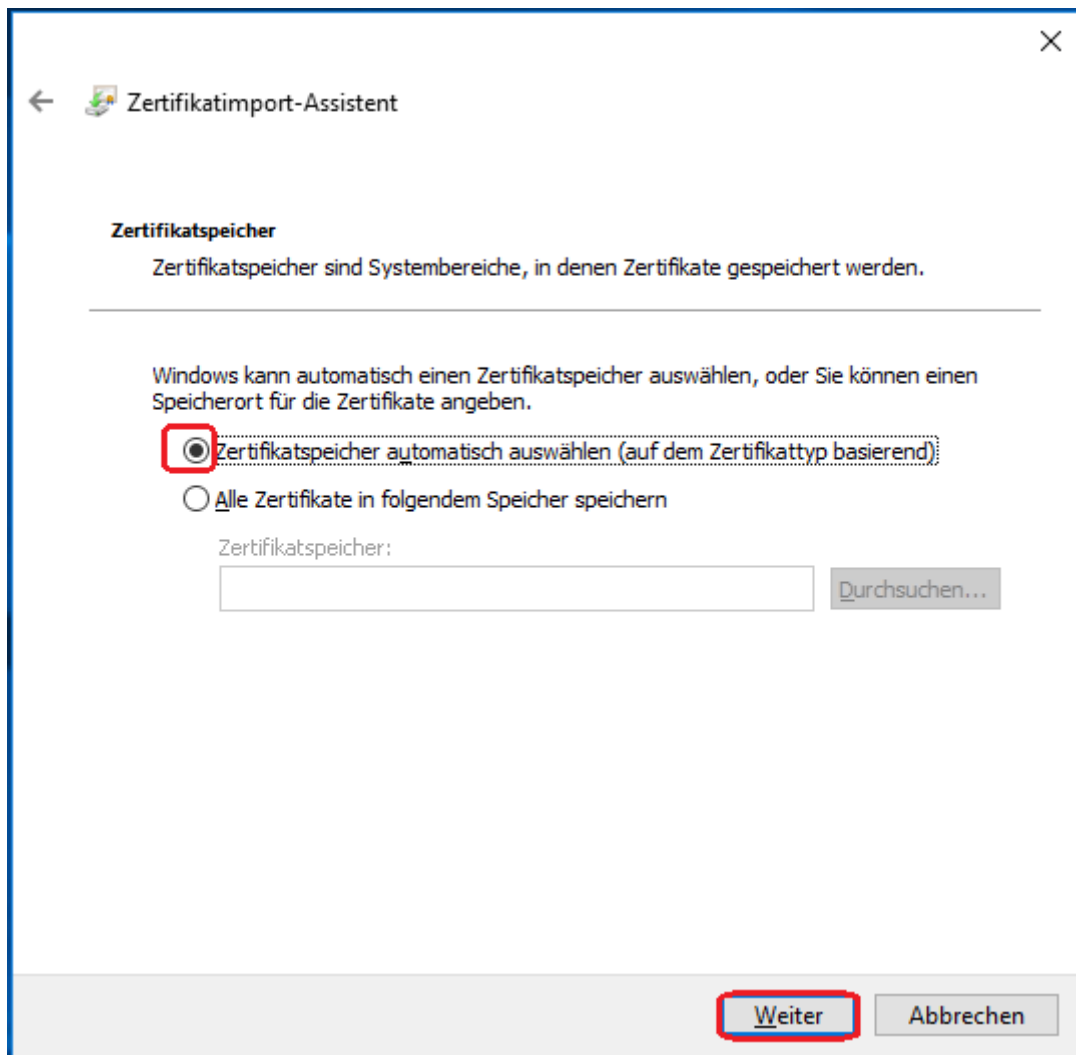
3. Im Eingabefeld "**Dateiname:**" wird die zu importierende Datei mit vollständiger Pfadangabe (hier: **C:\tmp\xmustercertkey.pfx**) angezeigt. Über "**Weiter >**" startet das nächste Dialogfenster.



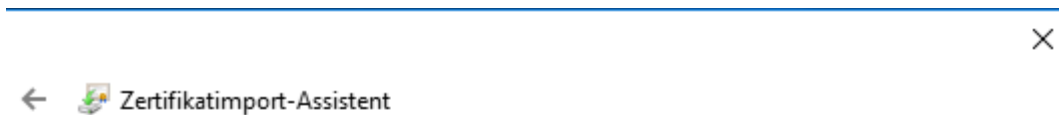
4. Das Eingabefeld "**Kennwort:**" erwartet das Passwort, das beim Export des Zertifikates (**siehe:** Zertifikate aus Browsern exportieren) vergeben wurde. Zusätzlich empfiehlt es sich, die Optionsfelder "**Schlüssel als exportierbar markieren ...**" und "**Alle erweiterten Eigenschaften mit einbeziehen**" auszuwählen. Zum Schluss wird die Schaltfläche "**Weiter >**" angeklickt.



5. Im nächsten Schritt des **"Zertifikatimport-Assistenten"** ist die Option **"Zertifikatspeicher automatisch auswählen..."** zu markieren und mit **"Weiter >"** zu bestätigen.



6. Der "**Zertifikatimport-Assistent**" zeigt jetzt noch einmal die getroffenen Einstellungen. Der Import des Zertifikates wird über "**Fertig stellen**" gestartet.

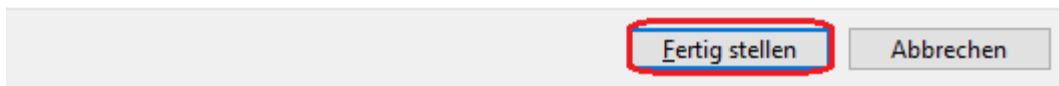


Fertigstellen des Assistenten

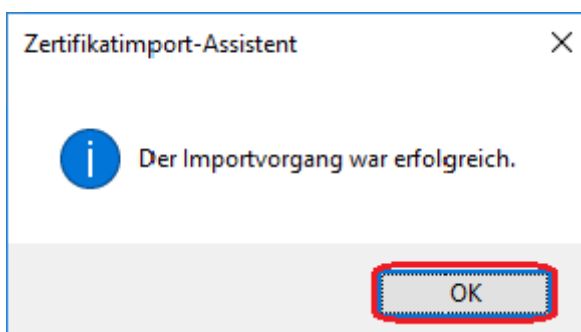
Das Zertifikat wird importiert, nachdem Sie auf "Fertig stellen" geklickt haben.

Sie haben folgende Einstellungen ausgewählt:

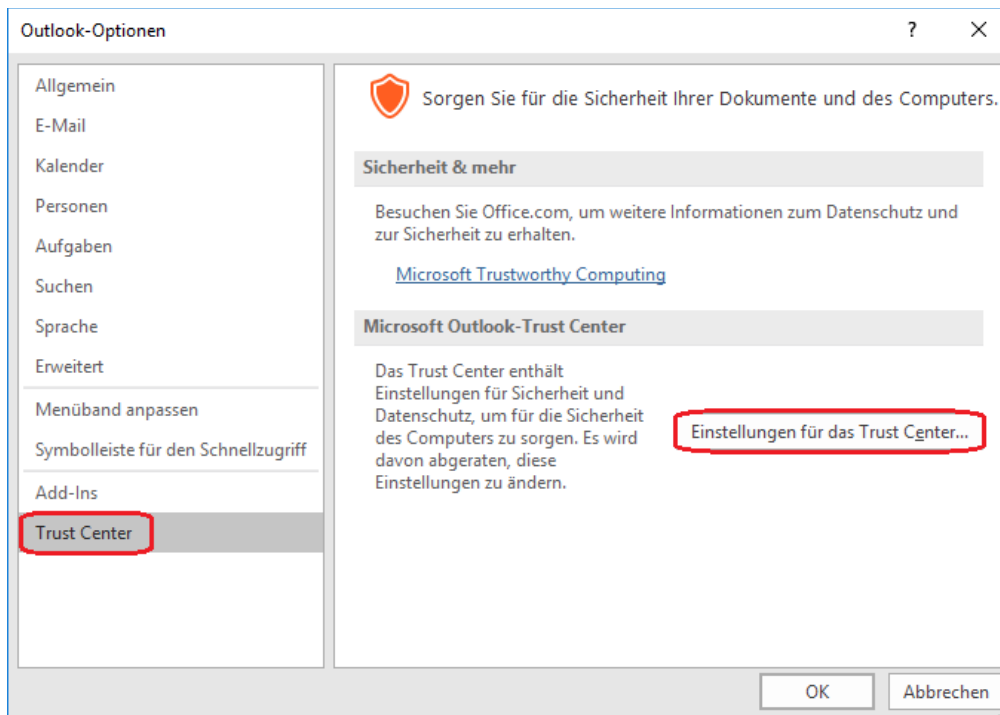
Gewählter Zertifikatspeicher	Auswahl wird vom Assistenten automatisch festgelegt
Inhalt	PFX
Dateiname	C:\tmp\xmuster.pfx



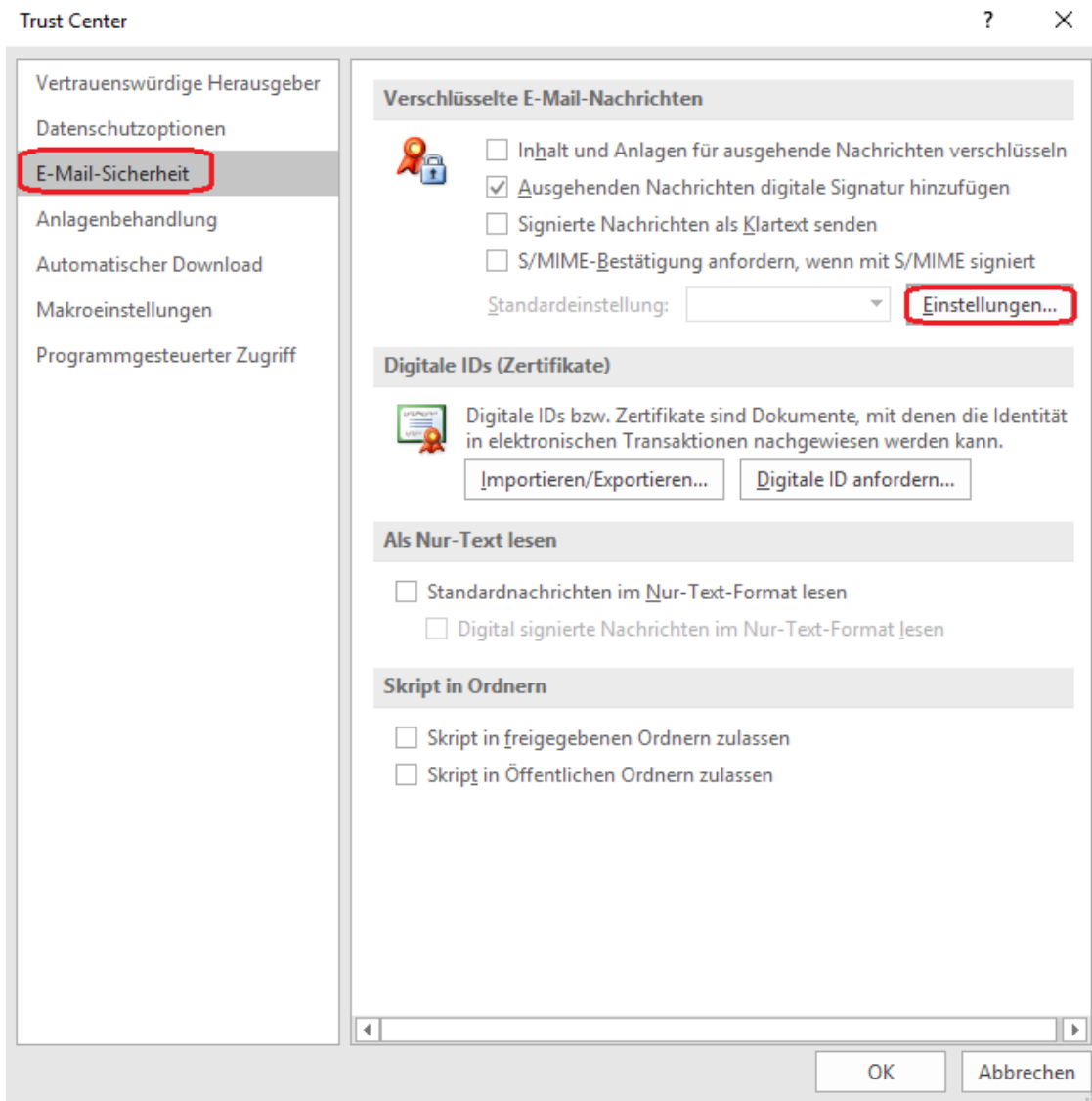
7. Das letzte Bild des "**Zertifikatimport-Assistenten**" bestätigt den erfolgreichen Importvorgang und wird mit "**OK**" bestätigt.



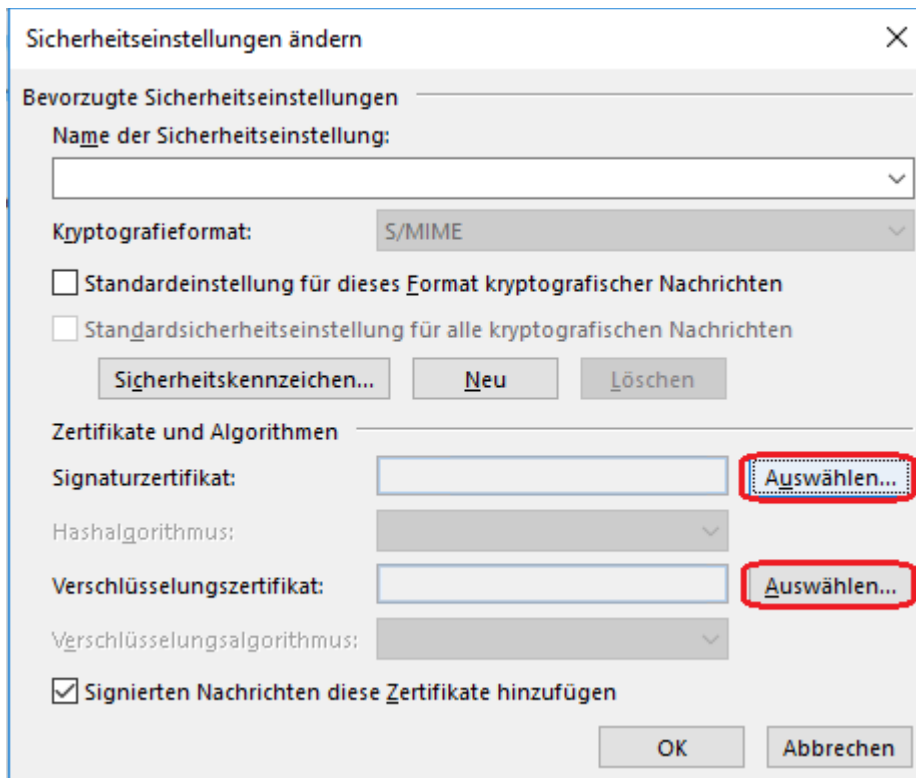
8. Das Zertifikat muss nun an das persönliche E-Mailkonto (hier: **Xaver Muster**) gebunden werden.
Dazu wird nach dem Start von Outlook 2016 auf der Karteikarte "**Datei**" der Menüpunkt "**Optionen...**" aufgerufen.
Im linken Fenster wird das "**Trust-Center**" selektiert. Im rechten Fenster wird die Schaltfläche "**Einstellungen für das Trust-Center**" angeklickt.



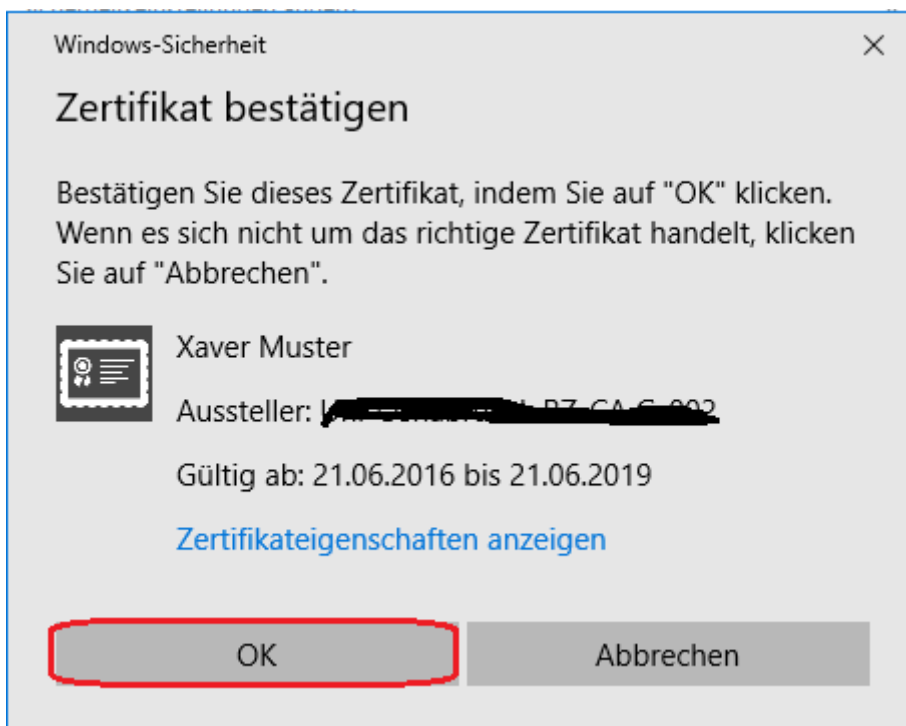
9. Im linken Fenster des **Trust Centers** wird der Top "**E-Mail-Sicherheit**" ausgewählt. Im rechten Teil des Dialogfensters wird in der Kategorie "**Verschlüsselte E-Mail-Nachrichten**" die Schaltfläche "**Einstellungen**" selektiert.



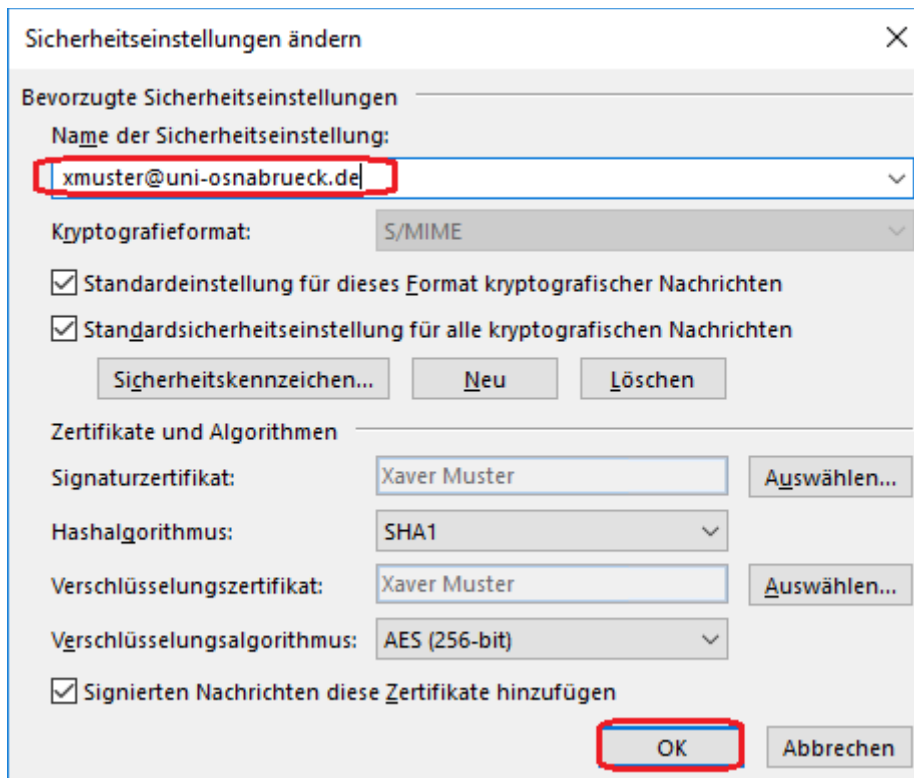
10. Im Dialogfenster "**Sicherheitseinstellungen ändern**" muss das zu verwendende Zertifikat für die Felder "**Signaturzertifikat**" und "**Verschlüsselungszertifikat**" ausgewählt werden.



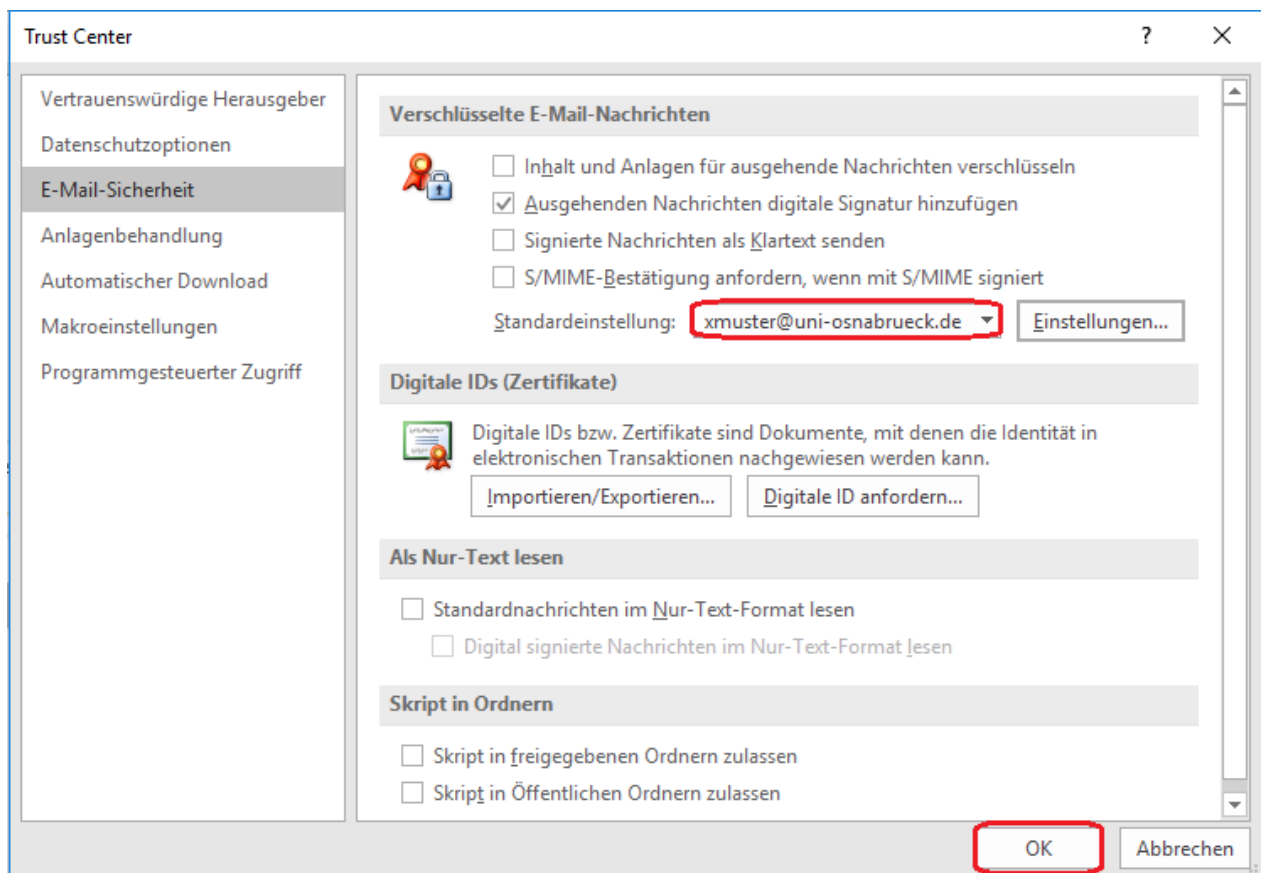
11. Das vorhandene Benutzerzertifikat wird jetzt angezeigt (hier: **PN: Xaver Muster**) und muss über **OK** bestätigt werden..



12. Das Eingabefeld "Name der Sicherheitseinstellung" erwartet einen Bezeichner (hier: **xmuster@uni-osnabrueck.de**). Über "OK" wird das Zertifikat von Xaver Muster an sein Mailkonto gebunden.



13. Das "Trust Center" wird mit "OK" beendet.



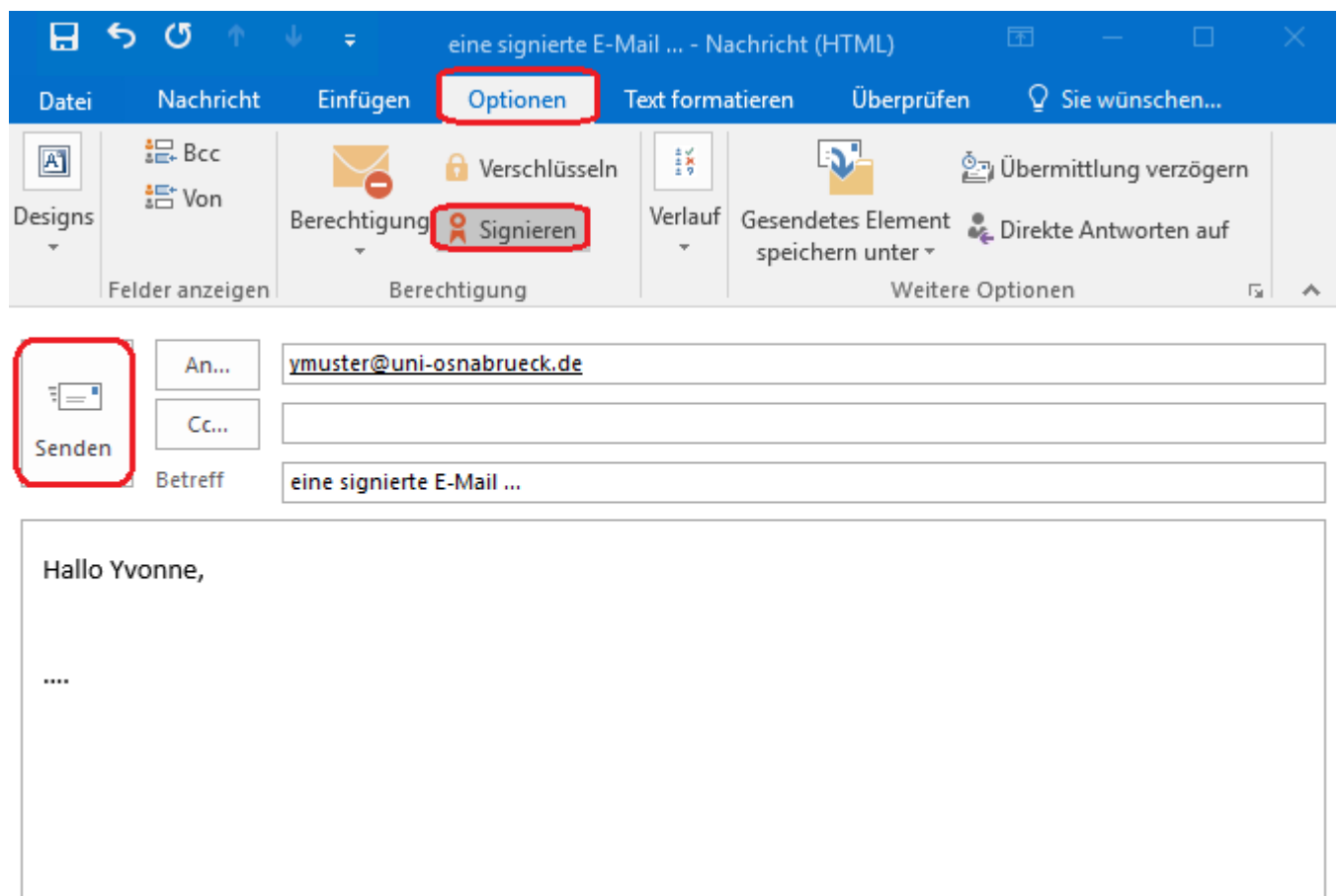
2. Signieren von E-Mails mit Outlook 2016

Nachdem das persönliche Zertifikat importiert worden ist, können E-Mails beim Versenden mit einer Signatur versehen werden. Das folgende Beispiel beschreibt, wie der fiktive Benutzer **Xaver Muster** der fiktiven Benutzerin **Yvonne Muster** eine signierte E-Mail zusendet.

2.1 Erzeugen einer E-Mail mit persönlicher Signatur

Xaver Muster erzeugt zunächst eine neue E-Mail. Damit diese Nachricht signiert wird, muss er auf der Registerkarte "**Optionen**" die Schaltfläche "**Signieren**" auswählen.

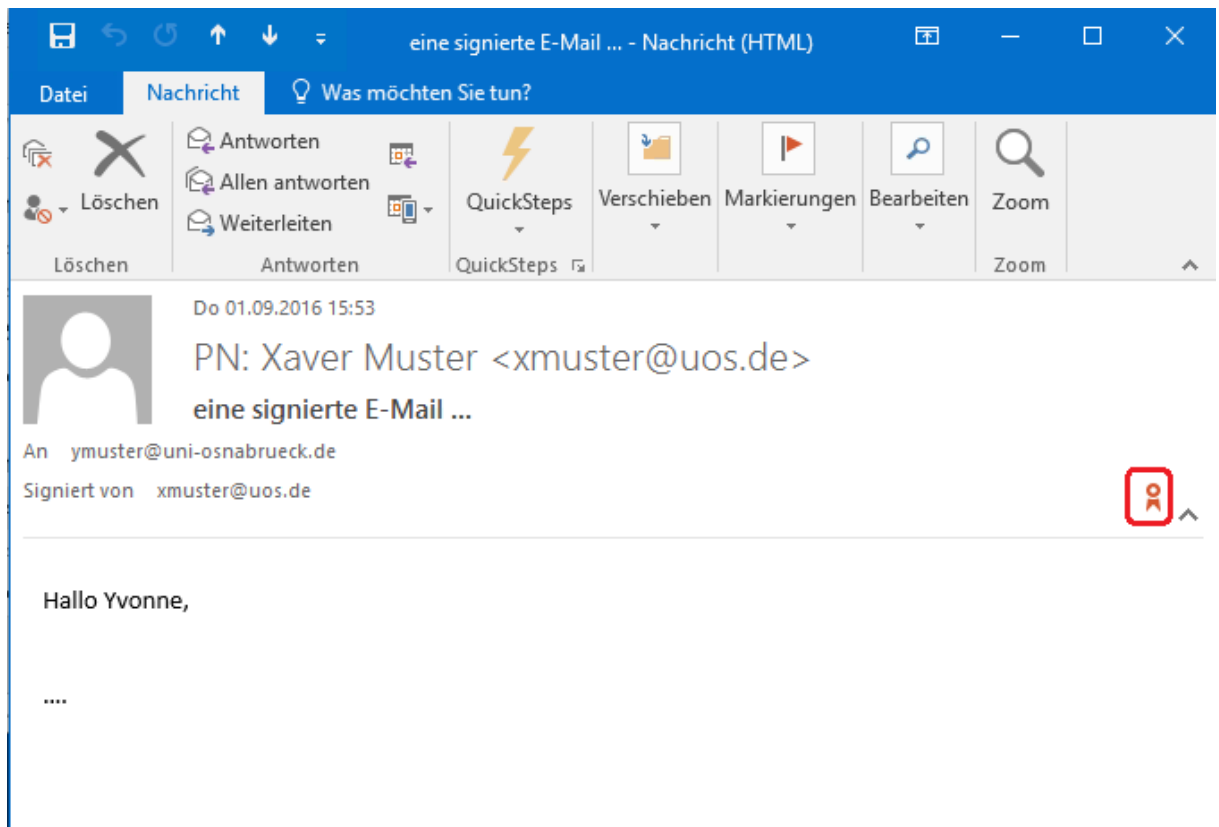
Hinweis: Outlook 2016 kann so konfiguriert werden, dass für jede neue E-Mail standardmäßig eine Signatur vergeben wird. (siehe: Installation des persönlichen Zertifikates unter Punkt 10 --> Das Optionsfeld "**Ausgehenden Nachrichten digitale Signatur hinzufügen**" markieren)



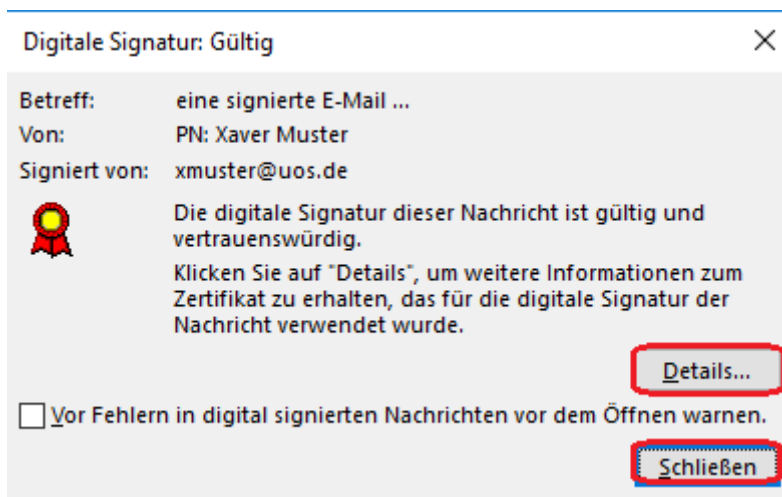
2.2 Prüfen der Signatur einer empfangenen E-Mail

Das folgende Beispiel beschreibt, wie Yvonne Muster die **Signatur** einer E-Mail **prüft**.

Yvonne Muster öffnet die E-Mail, die Xaver ihr gesendet hat. In der E-Mail befindet sich das Signatur-Symbol (hier: **rot eingekreist**), das anzeigt, dass die E-Mail signiert wurde. Durch Klicken auf das Signatur-Symbol werden die Informationen zur Signatur des Absenders (hier: **Xaver Muster**) angezeigt.



- Es öffnet sich das Dialogfenster "**Digitale Signatur: Gültig**", über das alle Informationen zur Signatur von Xaver Muster eingesehen werden können.



3. Verschlüsseln von E-Mails mit Outlook 2016

E-Mails werden immer mit dem "**öffentlichen Schlüssel**" aus dem persönlichen Zertifikat des Empfängers verschlüsselt.

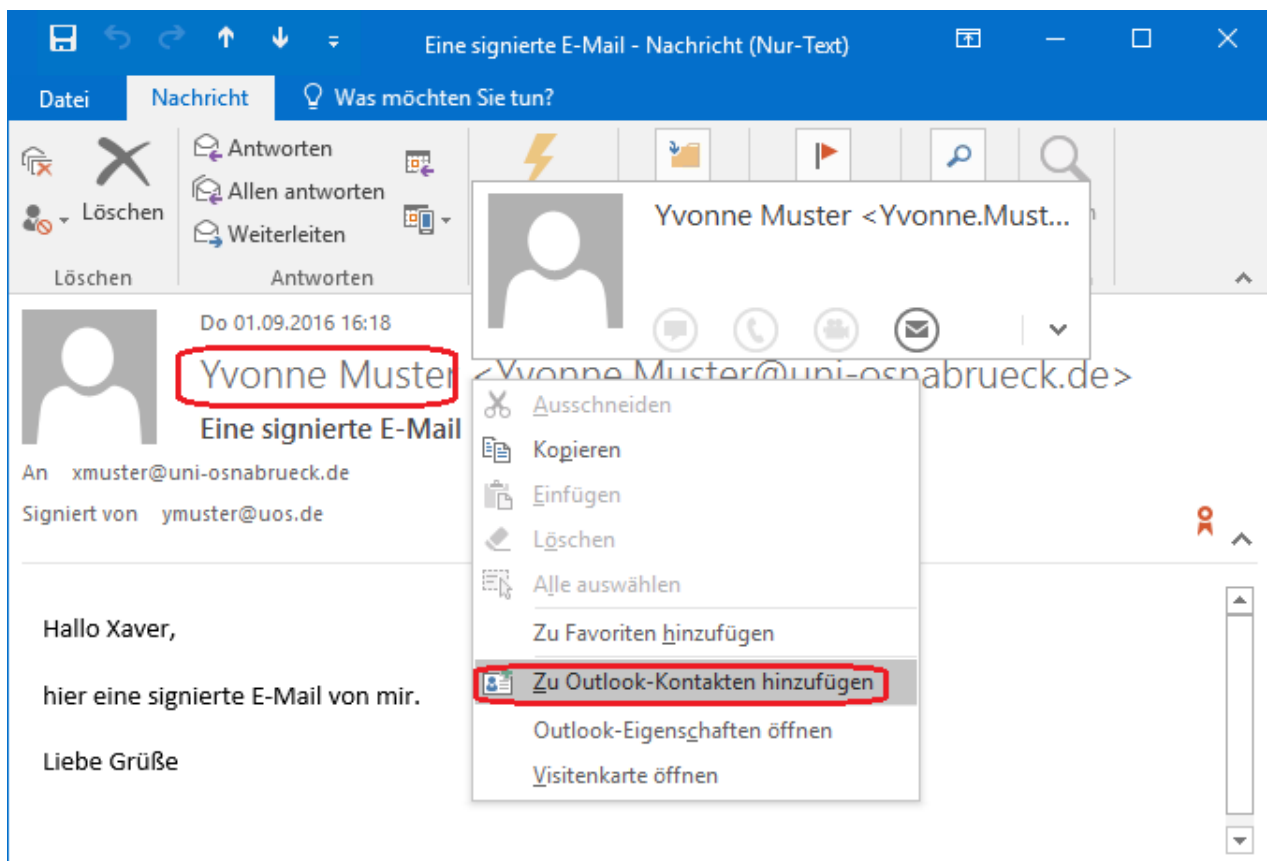
Wenn beispielsweise Xaver Muster eine verschlüsselte E-Mail an Yvonne Muster senden will, benötigt er dazu den "**öffentlichen Schlüssel**" des persönlichen Zertifikates von Yvonne Muster.

3.1 Öffentlichen Schlüssel des Empfängers verfügbar machen

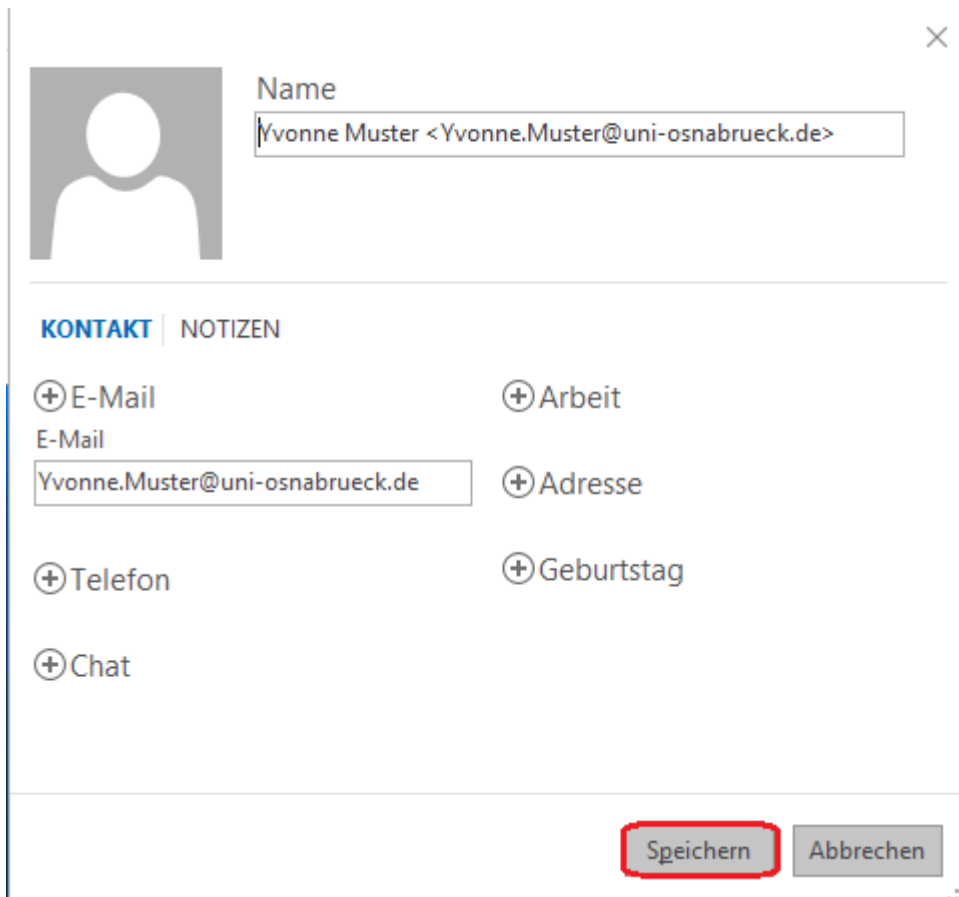
Wie kommt Xaver Muster an den "**öffentlichen Schlüssel**" aus dem persönlichen Zertifikat von Yvonne Muster?

Es gibt verschiedene Methoden, "**öffentliche Schlüssel**" verfügbar zu machen. Hier wird ein möglicher Weg für **Outlook 2016** beschrieben.

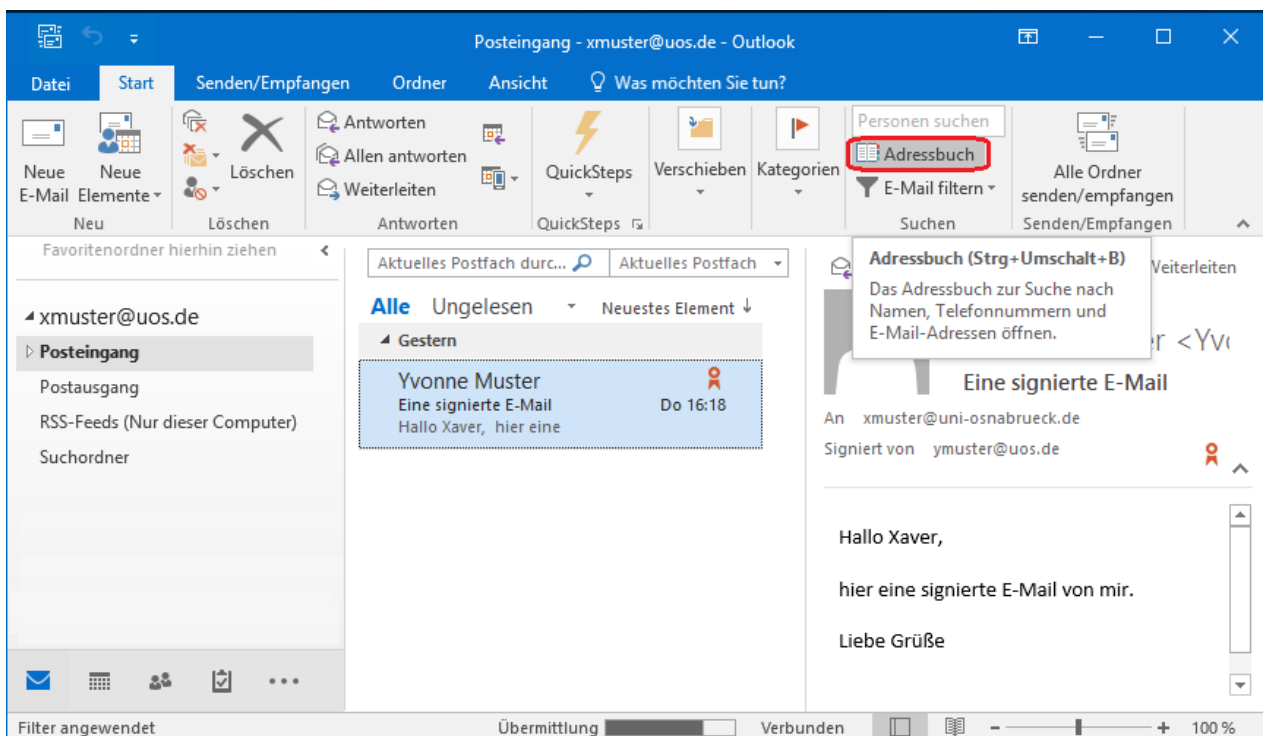
- Xaver lässt sich eine signierte E-Mail von Yvonne zusenden. Nach dem Öffnen der **signierten E-Mail** fügt er die Adresse des Absenders (hier: **Yvonne Muster [ymuster@uni-osnabrueck.de]**) zu seinen Outlook-Kontakten hinzu. Dazu drückt er die rechte Maustaste, sobald sich der Mauszeiger über der E-Mail-Adresse von Yvonne Muster befindet. Aus dem Kontextmenü wählt er den Untermenüpunkt "**Zu Outlook-Kontakten hinzufügen**" aus.



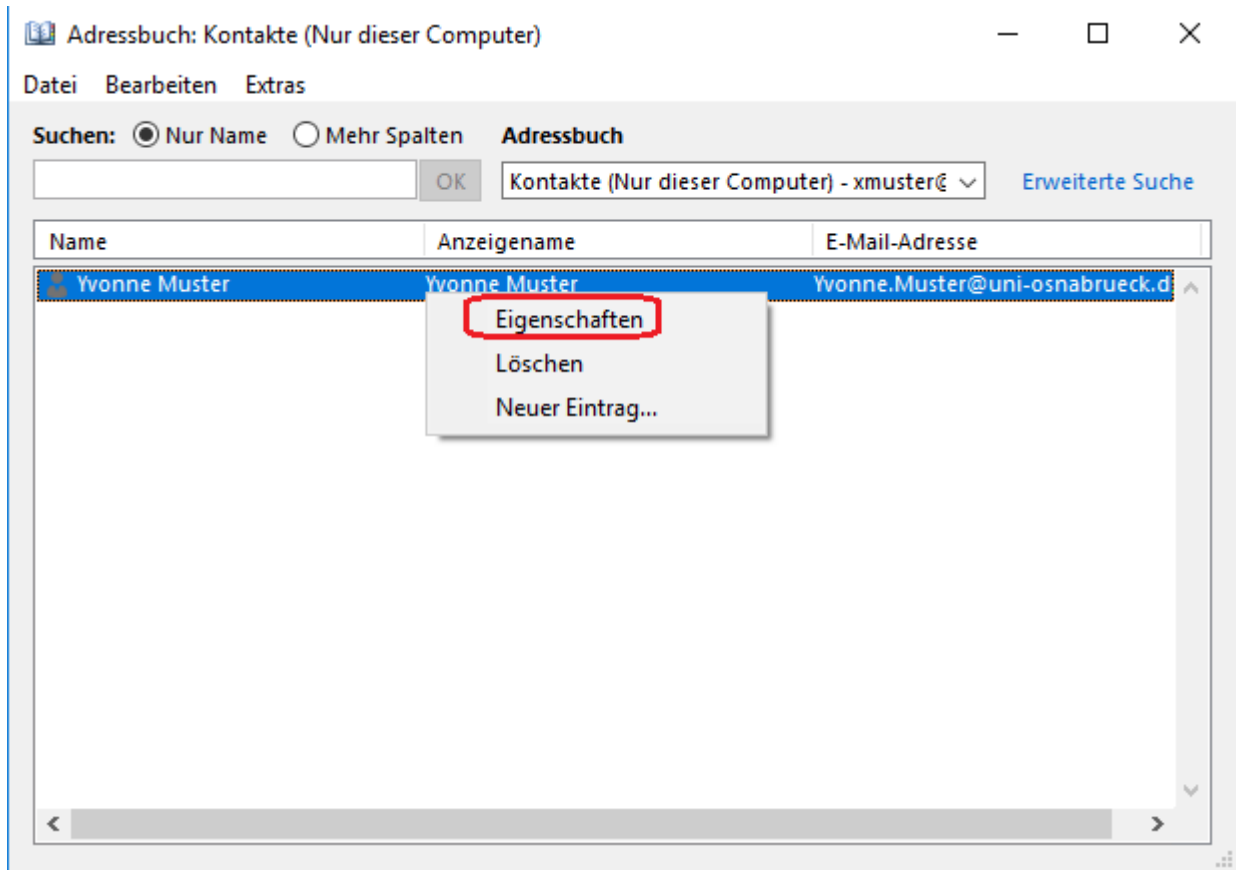
- Der Kontakt wird angezeigt und über "**Speichern**" zu den Kontakten hinzugefügt. Der öffentliche Schlüssel wird dabei **automatisch** mit gespeichert.



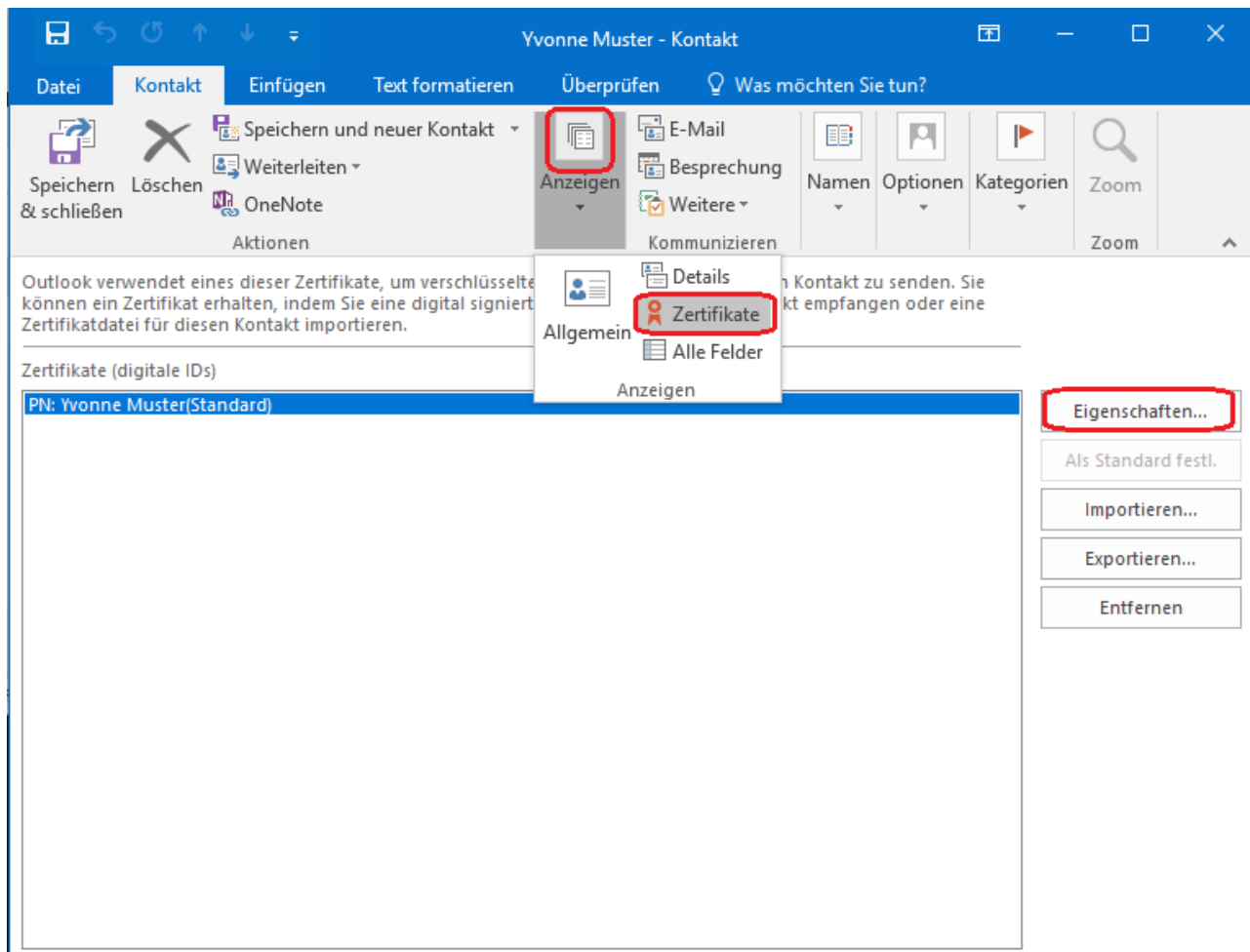
- Wenn Xaver Muster die Zertifikatsinformationen einsehen will, muss er zunächst im Menü "Start" das Adressbuch aufrufen.



- Hier selektiert er den Kontakteintrag von "Yvonne Muster" mit der linken Maustaste und wählt dann aus dem Kontextmenü den Menüpunkt "**Eigenschaften**" aus.



- Jetzt kann Xaver im "**Kontakt**"-Menü in der Kategorie "**Anzeigen**" den Menüpunkt "**Zertifikate**" auswählen. Danach wählt er das "**Eigenschaften**"-Symbol aus und bekommt die Zertifikatseigenschaften angezeigt.

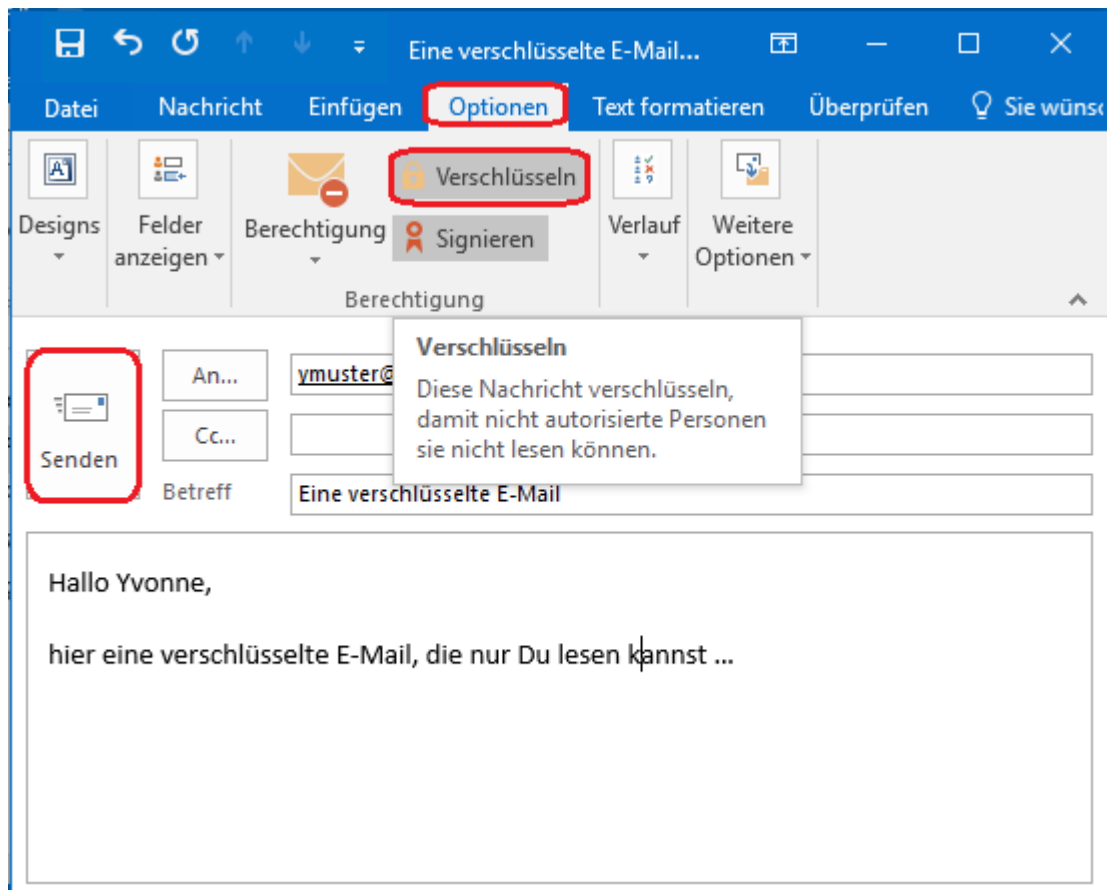


3.2 Erzeugen einer verschlüsselten E-Mail

Xaver Muster besitzt jetzt den **"öffentlichen Schlüssel"** des persönlichen Zertifikats von Yvonne Muster. Mit ihm kann er jetzt E-Mails an Yvonne Muster verschlüsseln. Der folgende Abschnitt beschreibt die dafür nötigen Arbeitsschritte.

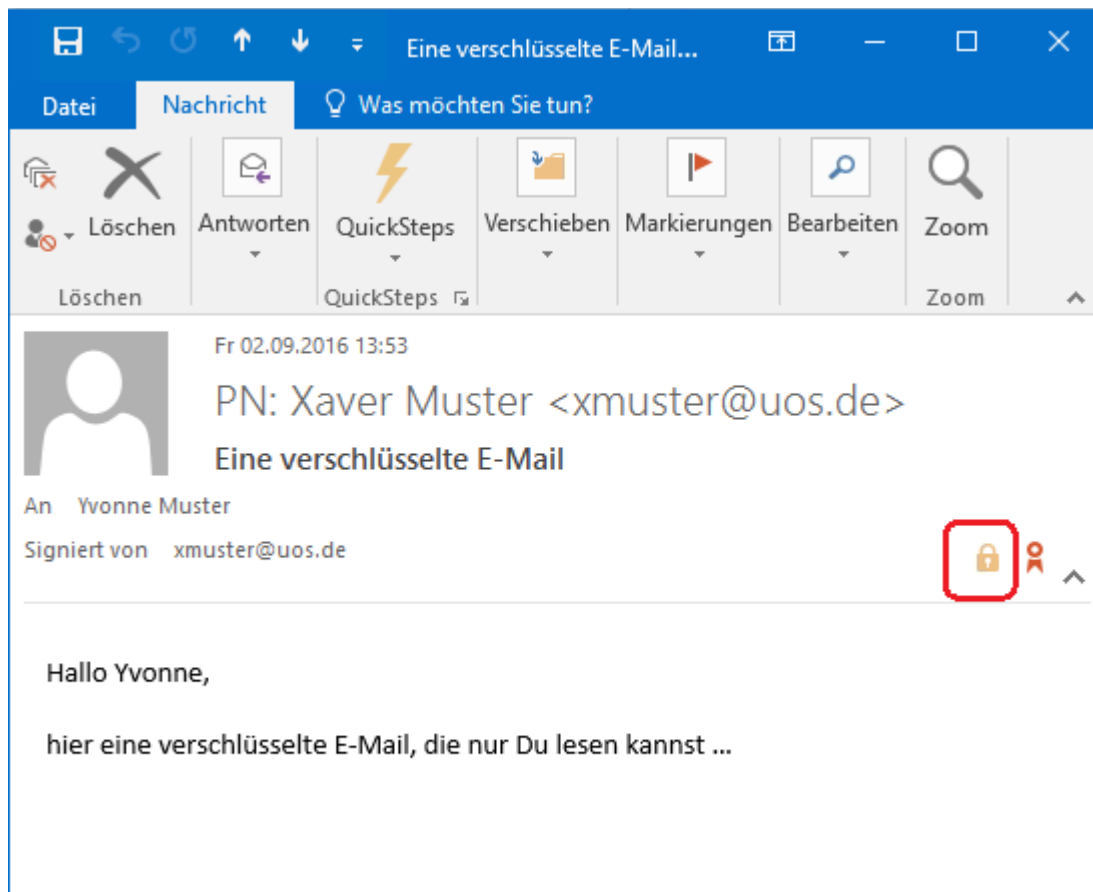
Nachdem Xaver Muster eine E-Mail an Yvonne Muster verfasst hat, klickt er unter **"Optionen"** auf die Schaltfläche **"Verschlüsseln"**. Anschließend schickt er die E-Mail über **"Senden"** ab.

Hinweis: Die E-Mail-Adresse des Empfängers muss exakt so geschrieben werden, wie sie im persönlichen Zertifikat des Empfängers enthalten ist. Verfügt das Zertifikat über mehrere E-Mail-Alias-Adressen, [sie werden im Zertifikat als **"Alternative Names"** bezeichnet (im Beispiel: xmuster@uni-osnabrueck.de, xmuster@uos.de, Xaver.Muster@uni-osnabrueck.de und Xaver.Muster@uos.de)] müssen diese in Outlook zur Kontaktkarte mit eingetragen werden, da sonst das Verschlüsseln beim Versenden an eine der genannten E-Mail-Adressen scheitert. Es können maximal drei E-Mail-Adressen pro Kontakt eingetragen werden.



3.3 Lesen einer verschlüsselten E-Mail

Sobald Yvonne die E-Mail von Xaver öffnet, wird diese **automatisch** entschlüsselt. Dazu benutzt Outlook den "**privaten Schlüssel**" des persönlichen Zertifikates von Yvonne Muster. Das **Schloss-Symbol** zeigt an, dass die E-Mail vom Absender (hier: **Xaver Muster**) verschlüsselt wurde.



*) Dieser Leitfaden wurde uns, Fritzenwallner-Gandler GmbH, mit freundlicher Unterstützung der UNI Osnabrück zur Verfügung gestellt.