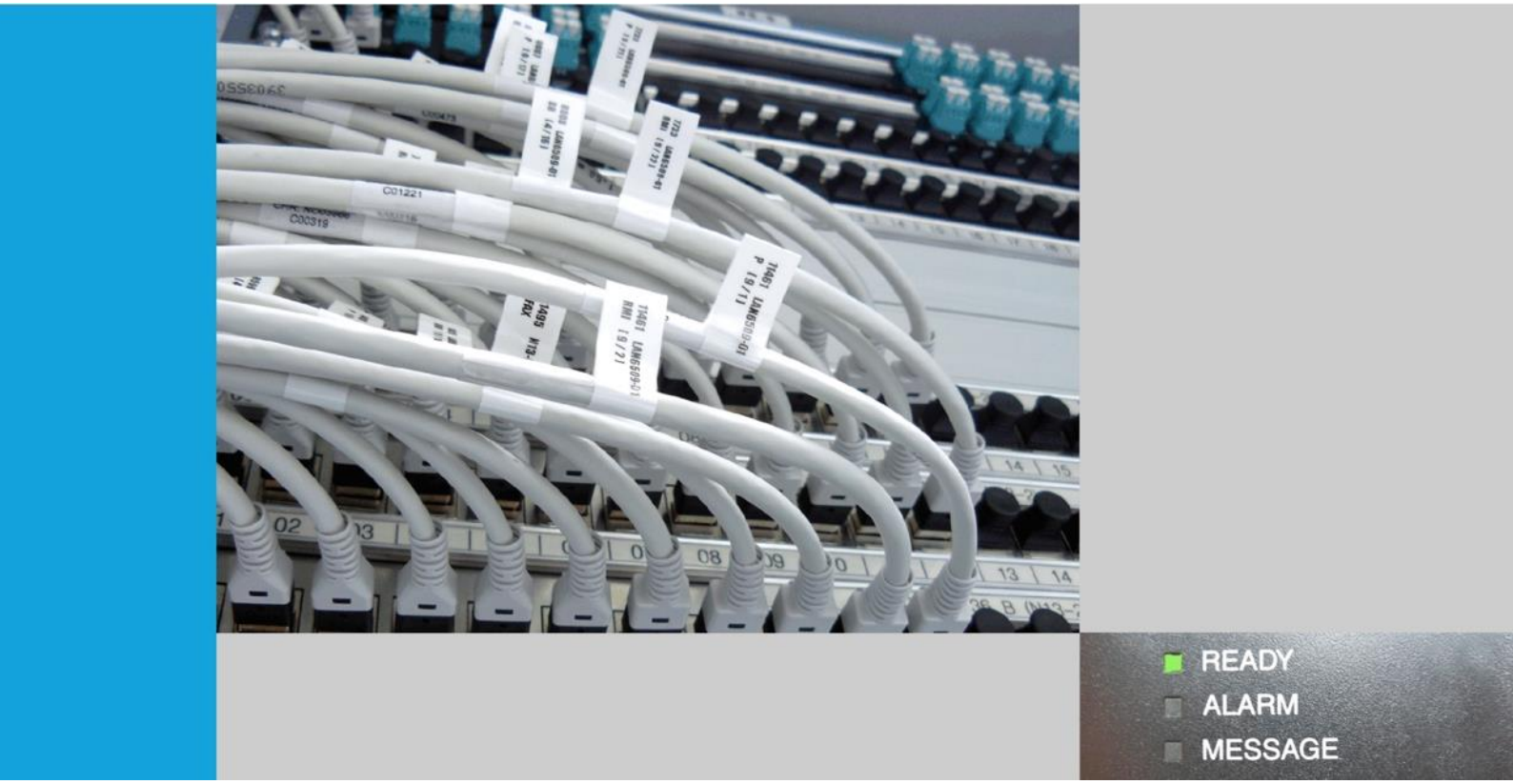
Landesamt für Digitalisierung,
Breitband und Vermessung

IT-Dienstleistungszentrum des Freistaats Bayern



Handbuch für Nutzung von Zertifikaten der Bayern-PKI für die Sicherung von E-Mails im Bayerischen Behördennetz (BYBN)

Outlook 2019 unter Windows 10

Überblick

Für die Sicherung von E-Mails mit dem Verfahren S/MIME benötigen Sie zwei Zertifikate, eines zur Ver- bzw. Entschlüsselung und eines für die elektronische Signatur von E-Mails.

Sie haben diese beiden Zertifikate über das Zertifikatsverwaltungssystem PRIME der Bayern-PKI beantragt und die Zertifikate und das zugehörige Schlüsselmaterial per E-Mail von der Bayern-PKI erhalten.

Damit Sie Ihre neuen Zertifikate nutzen können, um E-Mails mit Outlook 2019 unter Windows 10 zu verschlüsseln bzw. entschlüsseln und zu signieren, sind vier Schritte erforderlich, die in den nachfolgenden Kapiteln genauer beschrieben werden:

1. Empfang der Zertifikate per E-Mail
2. Import der Zertifikate und Schlüssel in Windows 10
3. Einstellung von Outlook 2019
4. Nutzung sicherer E-Mails bei der täglichen Arbeit

Unter Umständen kann Ihr Administrator Ihnen Teile der Einrichtung durch eine passende Vorkonfiguration Ihres Zertifikatsspeichers und Ihrer Outlook Anwendung abnehmen. Entsprechende Hinweise für den Administrator finden sich am Ende dieses Handbuchs.

Auf der letzten Seite des Handbuchs finden Sie schließlich die Kontaktinformationen des PKI-Supports der Bayern-PKI.

1 Empfang der Zertifikate per E-Mail

Die E-Mail, die Sie von der Bayern-PKI erhalten haben, enthält als Anhang Ihre privaten Schlüssel und die zugehörigen Zertifikate in zwei Dateien mit den Dateinamen:

- `enc_Vorname_Nachname.p12` (Verschlüsselungszertifikat)
- `sig_Vorname_Nachname.p12` (Signaturzertifikat)

Die Dateiendung `.p12` steht dabei für einen Datei-Typ, der den privaten Schlüssel für die Entschlüsselung von Nachrichten bzw. für die elektronische Signatur von Nachrichten zusammen mit dem zugehörigen Zertifikaten enthält und per PIN geschützt ist. Die Transport-PIN für Ihre beiden `.p12` Schlüsseldateien können Sie nach Ihrer Anmeldung im Zertifikatsverwaltungssystem PRIME sowie der Auswahl des Zertifikates in Ihrer Übersicht über den entsprechenden Menüpunkt erhalten.

Speichern Sie die beiden Schlüsseldateien in einem nur Ihnen zugänglichen Ordner, z. B. auf dem Festplattenlaufwerk `C:`, ab.

Wichtig: Weder den privaten Schlüssel noch die zugehörige PIN dürfen Sie an Dritte (auch nicht an Administratoren) weitergeben.

2 Import der Zertifikate und Schlüssel in Windows 10

2.1 Vorbemerkung zu den Optionen beim Schlüsselimport

Beim Import eines privaten Schlüssels erlaubt Windows die Wahl zwischen drei Stufen, wie stark Ihr privater Schlüssel gegen Missbrauch geschützt werden soll:

- In Stufe **einfach** wird der private Schlüssel ohne Nachfrage zum Entschlüsseln oder Signieren von E-Mail genutzt, solange sie am Windows-Arbeitsplatz angemeldet sind.
- In Stufe **mittel** erscheint vor jeder Nutzung des Schlüssels – d. h. beim Entschlüsseln einer verschlüsselten E-Mail bzw. beim Absenden einer signierten E-Mail – ein Fenster, in dem Sie Ihre Zustimmung geben müssen. Falls nicht Sie selbst gerade eine verschlüsselte E-Mail Lesen oder eine ausgehende E-Mail signieren wollen, sollten Sie die Nutzung des privaten Schlüssels verweigern. Dadurch wird verhindert, dass eine Anwendung oder Schadsoftware im Hintergrund den privaten Schlüssel in Ihrem Namen missbraucht.
- In Stufe **hoch** werden Sie vor jeder Nutzung des Schlüssels – d. h. beim Entschlüsseln einer verschlüsselten E-Mail bzw. beim Absenden einer signierten E-Mail – nach einem beim Import des Schlüssels von Ihnen vergebenen Passwort gefragt.
  Dadurch wird zusätzlich verhindert, dass Dritte – bspw. jemand, der unbeaufsichtigt Zugang zu Ihrem Windows-Arbeitsplatz bekommt, oder Administratoren – unbefugt Ihre vertraulichen E-Mails lesen oder in Ihrem Namen signierte E-Mails versenden können.

U. U. hat auch Ihr Administrator bereits eingeschränkt, welche dieser Schutzstufen Sie beim Import der Schlüsseldatei auswählen können (vgl. Hinweise für den Administrator am Ende dieses Handbuchs).

Wichtig: Für Zertifikate und Schlüssel der Bayern-PKI ist die Schutzstufe **hoch** zu verwenden. Dies ist in der folgenden Anleitung berücksichtigt.

Neben der Schutzstufe erlaubt Windows, bei der Installation einer Schlüsseldatei auszuwählen, ob der Schlüssel später wieder aus dem Windows-Schlüsselspeicher exportiert werden kann.

- Falls Sie den Schlüssel als **exportierbar** markieren, können Sie zu einem späteren Zeitpunkt den betreffenden Schlüssel und das zugehörige Zertifikat wieder in eine `.p12` Datei – vergleichbar derjenigen, in der sie Zertifikat und Schlüssel von der Bayern-PKI erhalten haben – exportieren.
- Falls Sie den Schlüssel **nicht** als **exportierbar** markieren, bleibt der Schlüssel in jedem Fall geschützt im Windows-Schlüsselspeicher gespeichert.

Empfehlung: Im Regelfall sollten Sie den Schlüssel **nicht** als **exportierbar** markieren. Dies ist in der folgenden Anleitung berücksichtigt.

Falls Sie Ihre Zertifikate und Schlüssel in ein anderes System importieren müssen (bspw. auf einem anderen Rechner oder in einen anderen E-Mail-Client wie Thunderbird), können Sie dazu die originalen Schlüsseldateien und die Transport-PIN verwenden, die Sie von der Bayern-PKI erhalten haben.

Sollten zu einem späteren Zeitpunkt diese Schlüsseldateien und die E-Mail, in der Sie sie empfangen haben, bereits gelöscht sein, können Sie für den Import in weitere Systeme über das Zertifikatsverwaltungssystem PRIME Ihr Verschlüsselungszertifikat erneut abrufen und ein neues Signaturzertifikat beantragen.

2.2 Import der Schlüsseldateien

Nun können Sie Ihre neuen Schlüssel und Zertifikate aus den Schlüsseldateien, die sie im vorigen Schritt in einem lokalen Ordner abgespeichert haben, in Ihren persönlichen Zertifikatsspeicher importieren. Dabei ist es egal, mit welcher der beiden Dateien (`enc_Vorname_Nachname.p12` bzw. `sig_Vorname_Nachname.p12`) Sie beginnen.

Zum Import öffnen Sie mit einem Doppelklick die Schlüsseldatei. Dadurch erscheint die Startseite des Zertifikatimport-Assistenten. Belassen Sie die Vorauswahl auf `Aktueller Benutzer` und klicken Sie auf `Weiter`.

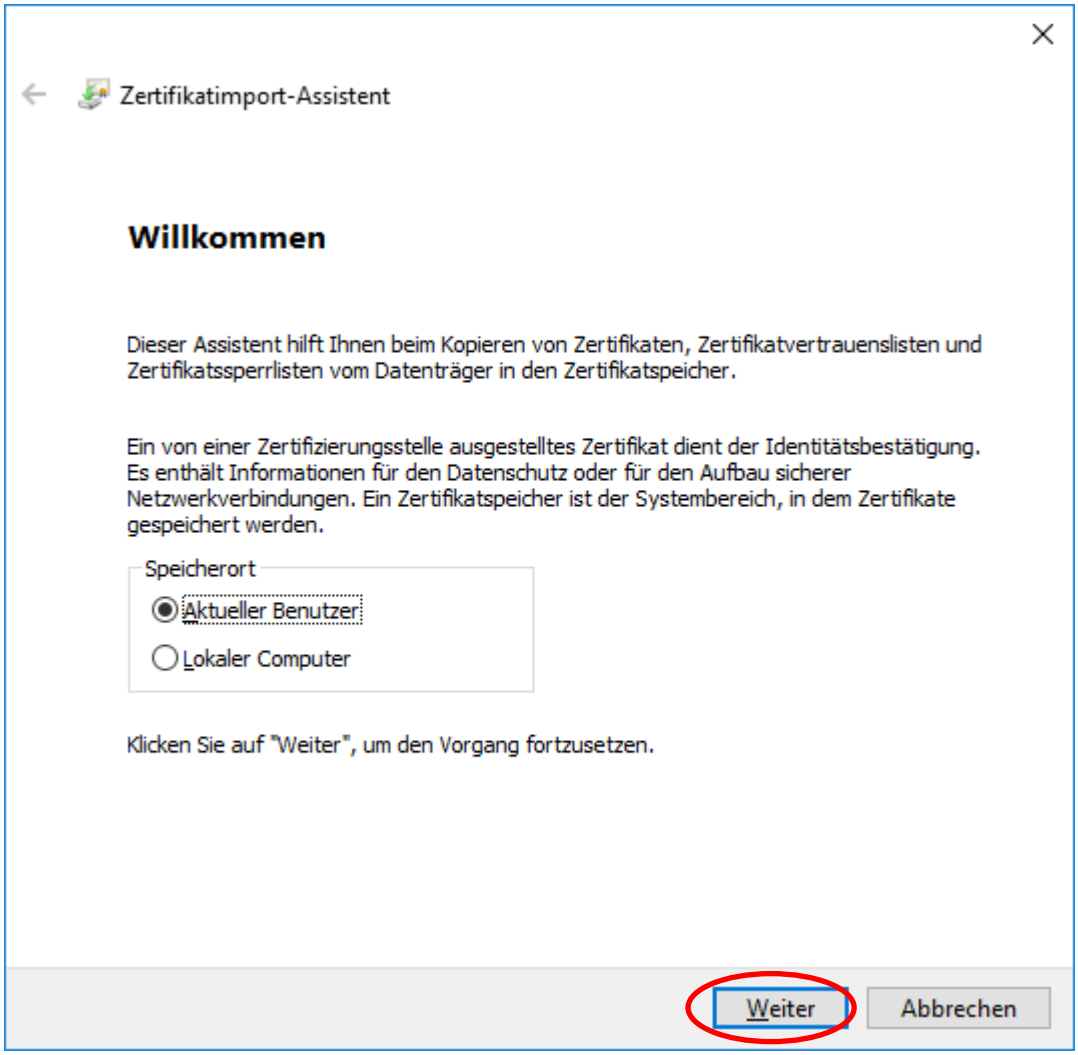


Abbildung 1:Startseite des Zertifikatimport-Assistenten

Im folgenden Schritt des Assistenten ist die Zertifikatsdatei bereits vorausgewählt. Klicken Sie auf `Weiter`.

Hinweis: Falls der Assistent nicht durch Doppelklick auf eine Schlüsseldatei aufgerufen wurde, müssen Sie in diesem Schritt per `Durchsuchen…` die richtige Schlüsseldatei auswählen.

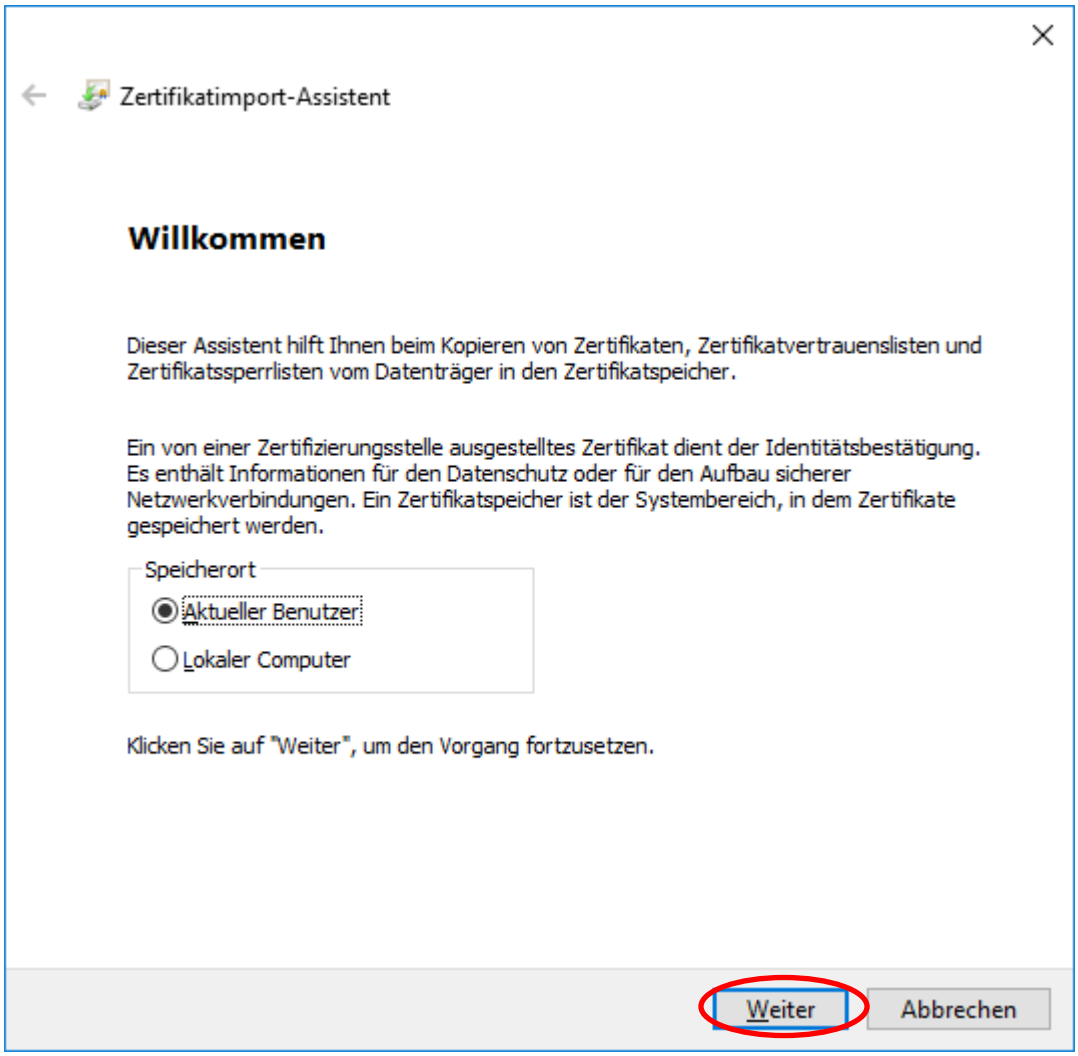


Abbildung 2:Vorausgewählte Schlüsseldatei

Nun geben Sie als `Kennwort` die Transport-PIN zu Ihrer Schlüsseldatei ein. Setzen Sie das Häkchen, um die Option `Hohe Sicherheit für den privaten Schlüssel` zu aktivieren. Belassen Sie die Option Schlüssel als exportierbar markieren deaktiviert. Klicken Sie dann auf `Weiter`.

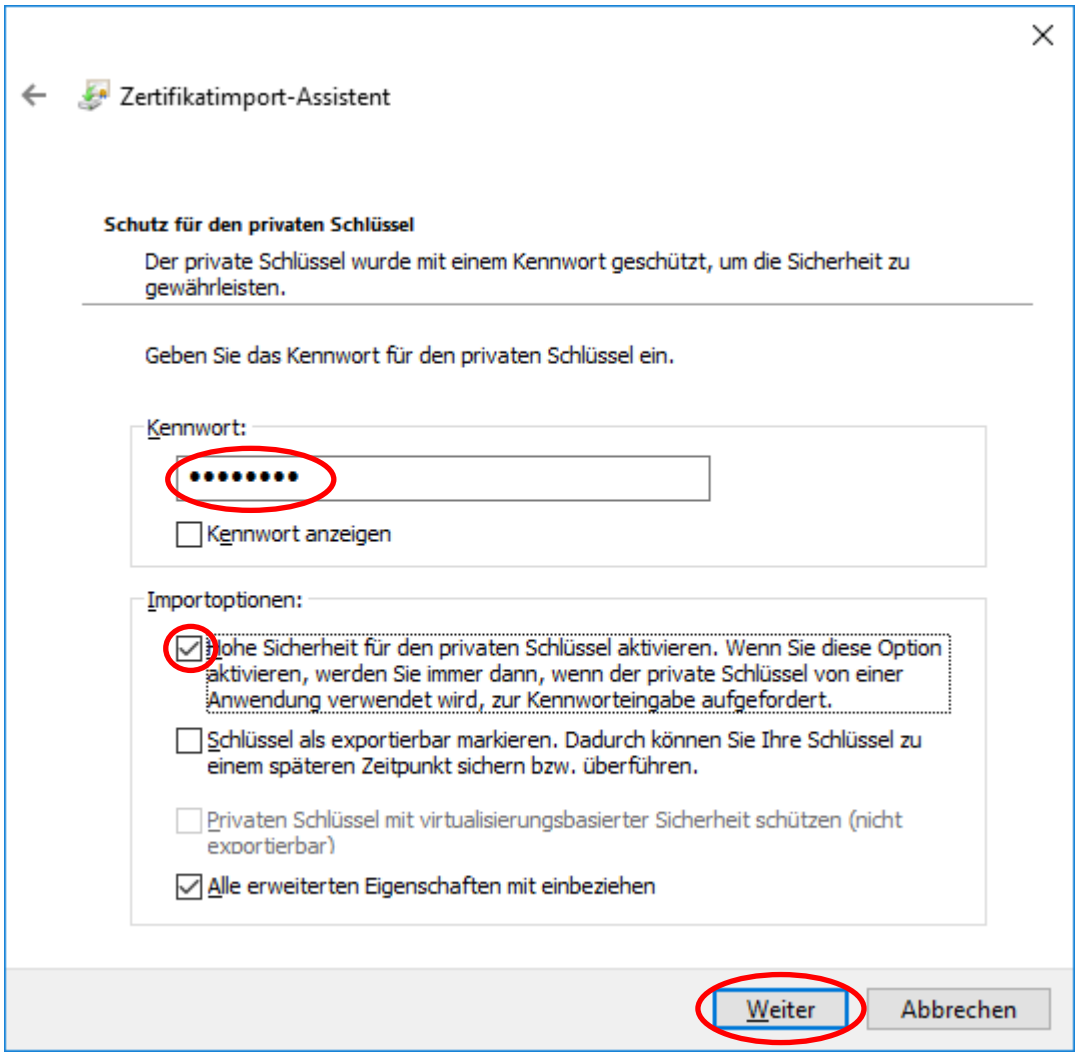


Abbildung 3:Eingabe der Transport-PIN und Auswahl der Schutzstufe

Hinweis: Falls Ihr Administrator eingeschränkt hat, welche Schutzstufen Sie beim Import der Schlüsseldatei auswählen können, ist U. U. die Option `Hohe Sicherheit für den privaten Schlüssel` bereits aktiviert und ausgegraut.

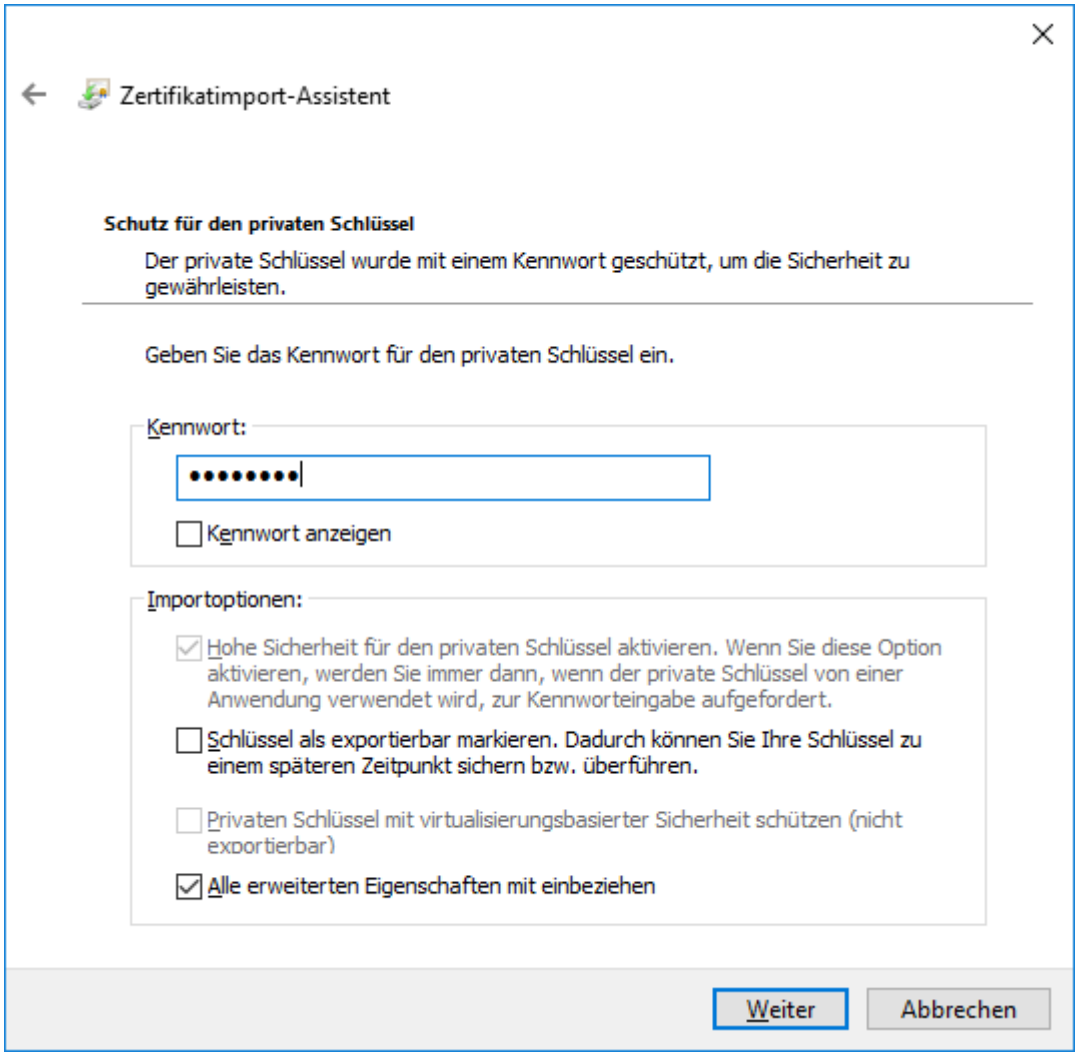


Abbildung 4:Bei Einschränkung der zulässigen Schutzstufen durch den Administrator

Belassen Sie im nächsten Schritt des Assistenten die Vorauswahl bei `Zertifikatsspeicher automatisch auswählen` und klicken Sie auf `Weiter`.

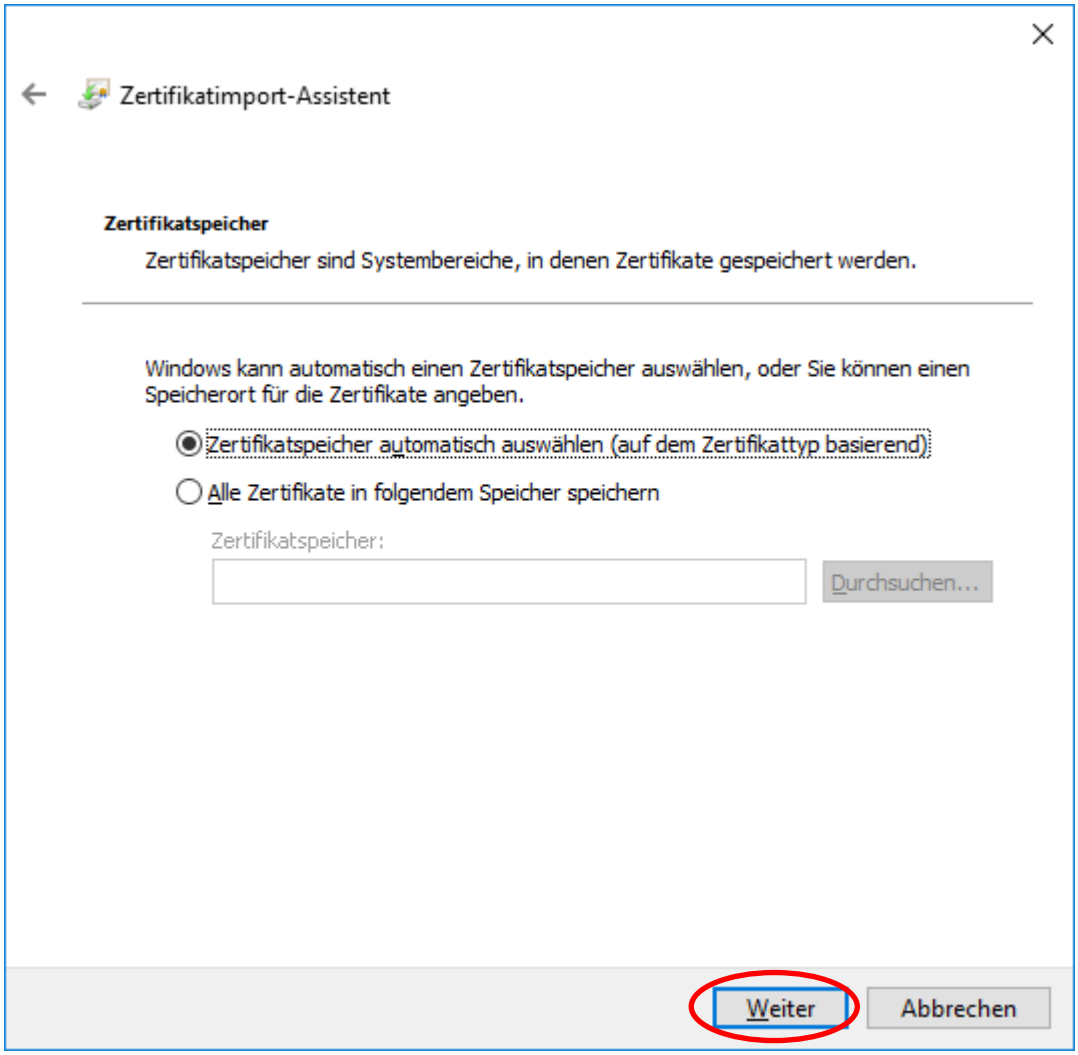


Abbildung 5:Automatische Auswahl des Zertifikatsspeichers

Klicken Sie bei der Zusammenfassung Optionen auf `Fertig stellen`.

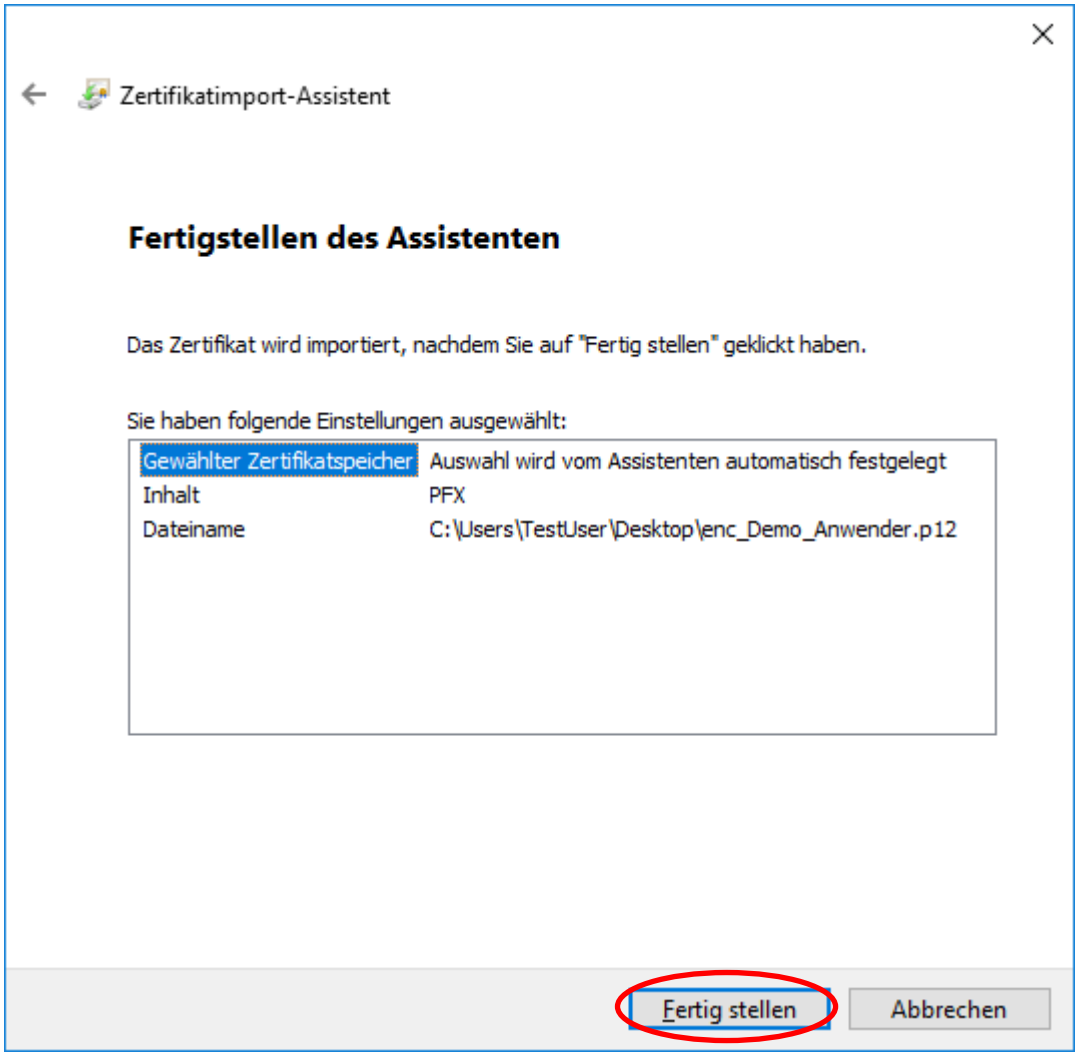


Abbildung 6:Zusammenfassung der gewählten Optionen

Im nächsten Schritt des Assistenten können Sie das Passwort zum Schutz Ihres privaten Schlüssels vergeben. Geben Sie zweimal das von Ihnen gewählte Passwort ein. Klicken Sie zum Abschluss auf `OK`.

Empfehlung: Vergeben Sie für das Verschlüsselungs- und das Signaturzertifikat dasselbe Passwort, um spätere Verwechslungen zu vermeiden.

Hinweis: U. U. erscheint dieser Dialog zwar auf Ihrem Bildschirm, hat aber nicht den Eingabefokus. Klicken Sie in diesem Fall zuerst auf das Fenster, damit Sie das Kennwort eingeben können.

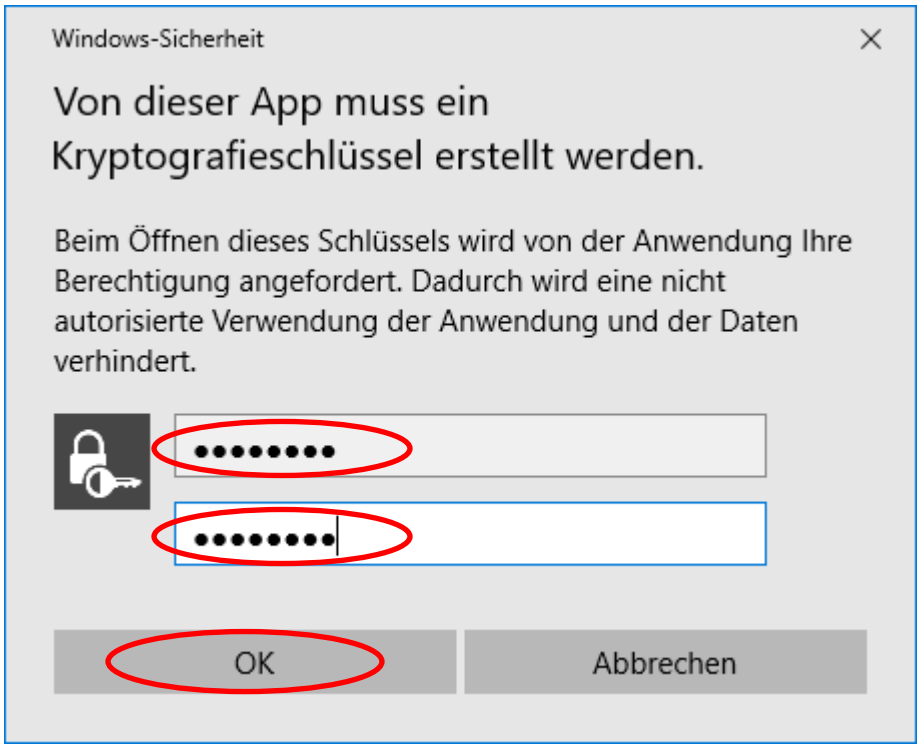


Abbildung 7:Festlegen des Passworts für die Nutzung des importierten Schlüssels

Beenden Sie nach erfolgreichem Abschluss den Zertifikatimport-Assistenten durch einen Klick auf `OK` und führen Sie die gleichen Schritte anschließend mit Ihrer zweiten Schlüsseldatei durch.

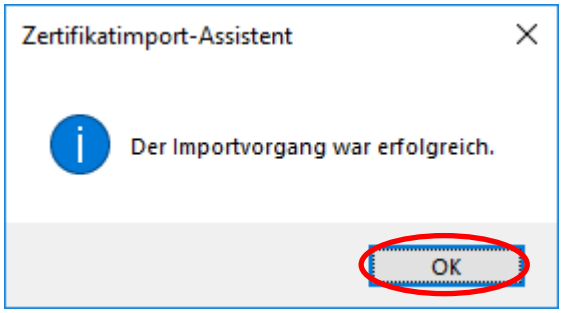


Abbildung 8:Abschluss des Zertifikatimport-Assisitenten

Wichtig: Nach erfolgreichem Import der Zertifikate ins System sollten Sie die beiden `.p12` Dateien, die sie im vorigen Schritt angelegt haben, wieder löschen.

3 Einstellung von Outlook 2019

3.1 Einstellungen für die Nutzung der Zertifikate

Bevor Sie E-Mails verschlüsseln oder signieren können, müssen Sie Ihr Outlook so einstellen, dass es Ihre neuen, im vorigen Schritt in den Windows-Zertifikatsspeicher importierten Zertifikate der Bayern-PKI dafür nutzt.

Hinweis: Möglicherweise hat Ihr Administrator Outlook bereits so voreingestellt, dass es Ihre Zertifikate automatisch nutzt. In diesem Fall können Sie die folgenden Schritte dieses Kapitels überspringen und direkt zum Einrichten der LDAP-Verbindung zum Verzeichnisdienst des BYBN übergehen.

Um zu prüfen, ob dies der Fall ist, erstellen Sie eine neue E-Mail (die Sie nicht absenden müssen) und prüfen Sie im Fenster dieser neuen E-Mail, ob unter `Optionen` bereits die beiden Symbole für `Verschlüsseln` und `Signieren` angezeigt werden.

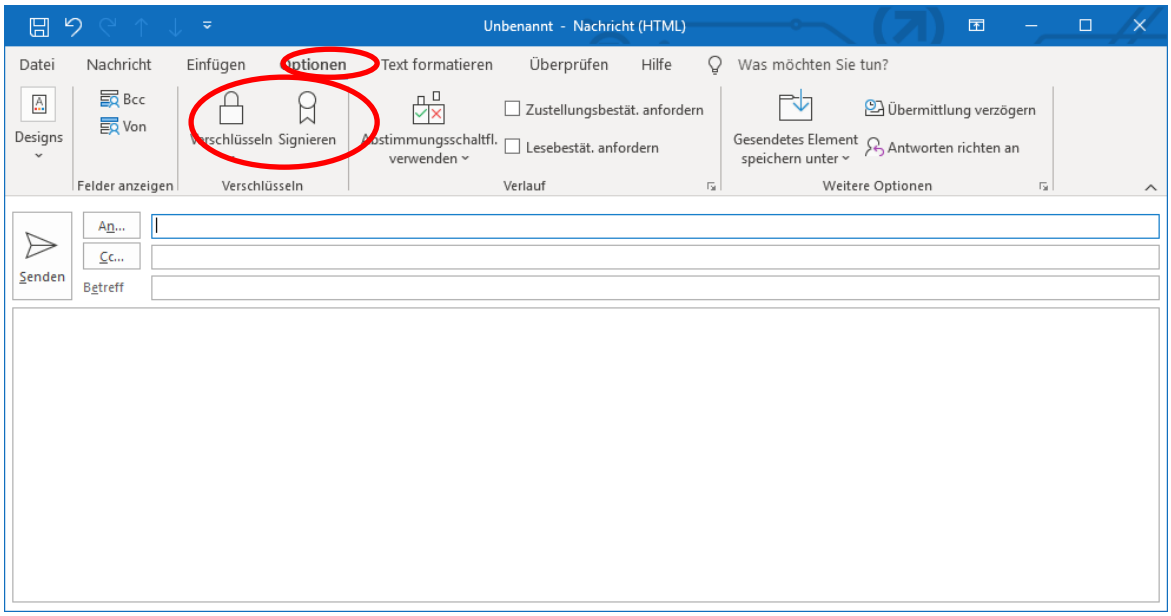
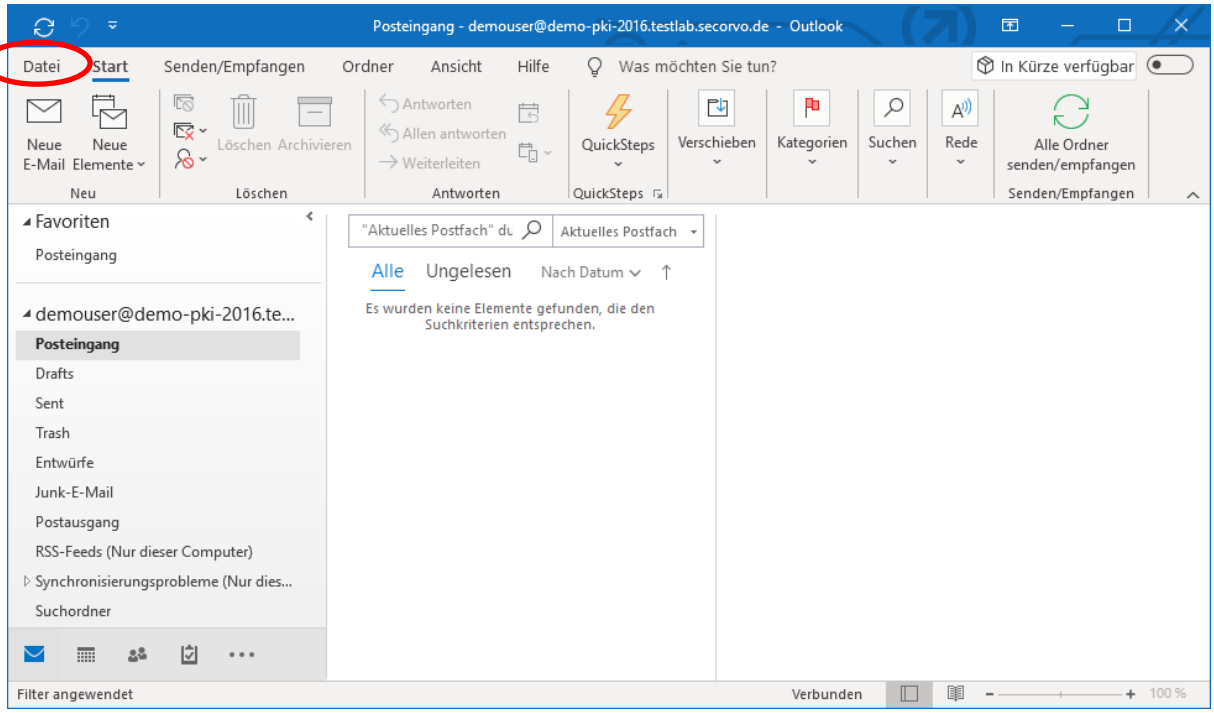


Abbildung 9: Angezeigte Optionen „Verschlüsseln“ und „Signieren“ für eine neue E-Mail bei passender Voreinstellung von Outlook durch den Administrator

Falls diese beiden Symbole nicht angezeigt werden, führen Sie die Schritte der nachfolgenden Anleitung durch.

Klicken Sie im Hauptfenster von Outlook auf `Datei` und dann auf `Optionen`.



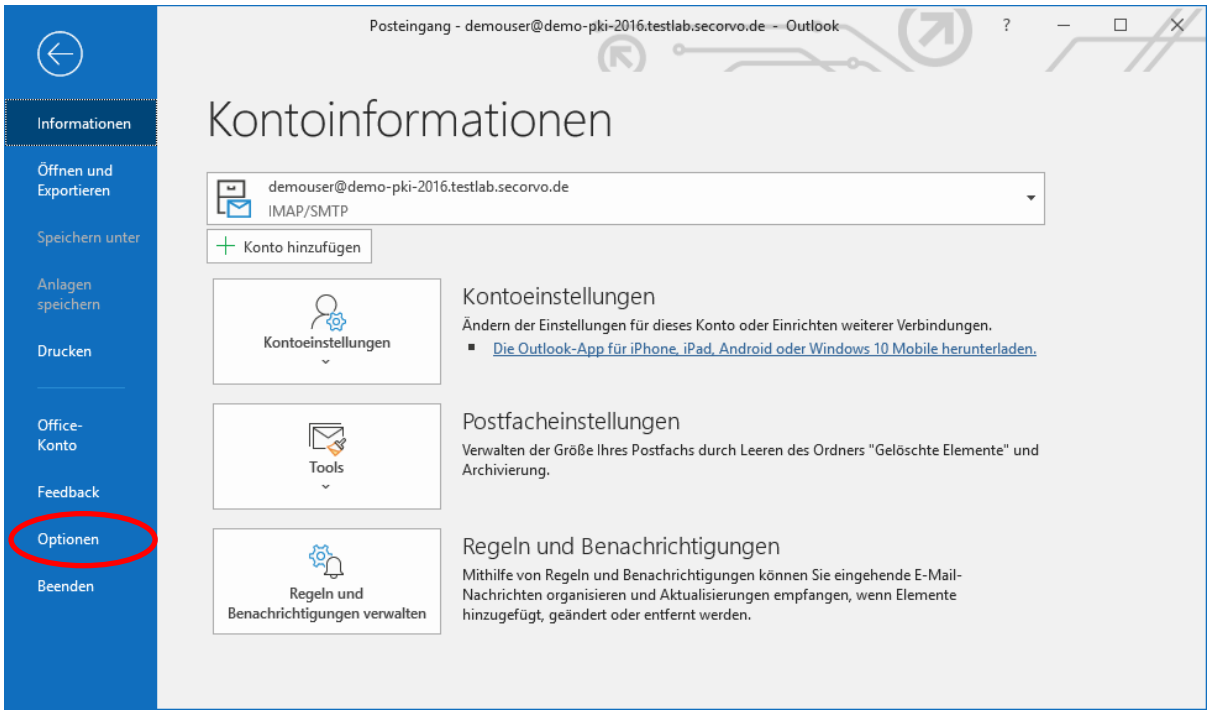


Abbildung 10: Aufruf der Outlook-Optionen

Klicken Sie bei den Outlook-Optionen auf `Trust Center` und dann auf `Einstellungen für das Trust Center...`.

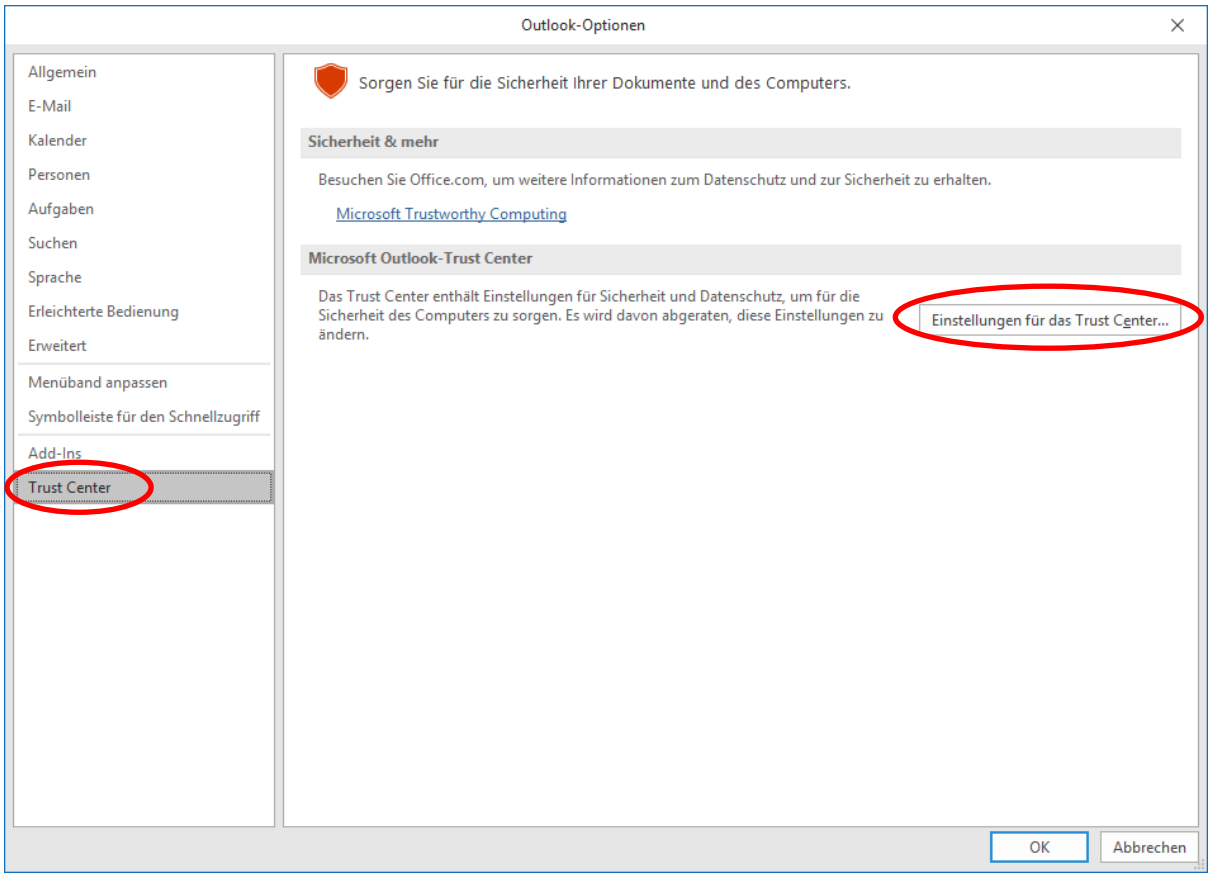


Abbildung 11: Aufruf der Trustcenter-einstellungen

Klicken Sie im Fenster des Trust Centers auf `E-Mail-Sicherheit` und dann auf `Einstellungen...`.

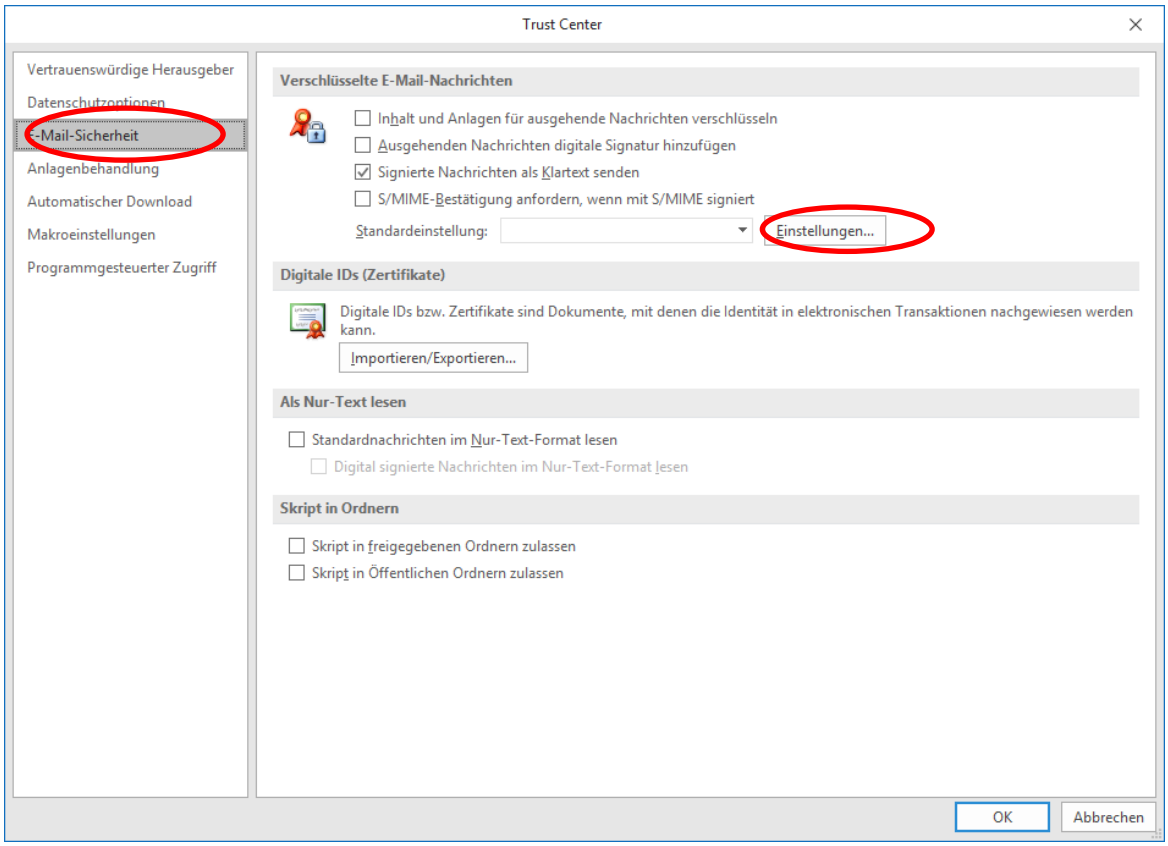


Abbildung 12: Aufruf der Einstellungen für die E-Mail-Verschlüsselung

Prüfen Sie, dass in den Sicherheitseinstellungen unter `Signaturzertifikat` und `Verschlüsselungszertifikat` bereits Ihr Name voreingestellt ist, der aus Ihren neuen Zertifikaten ausgelesen wurde.

Wählen Sie unter `Hashalgorithmus` das `SHA256` Verfahren aus. Übernehmen Sie die Einstellungen durch Klick auf `Ok`.

Hinweis: Falls unter `Signaturzertifikat` und/oder `Verschlüsselungszertifikat` noch kein Name oder ein anderer Name voreingestellt erscheint, dann können Sie durch Klick auf die Schaltfläche `Auswählen…` neben dem jeweiligen Zertifikatstyp eine Liste der jeweils verfügbaren, nutzbaren Zertifikate anzeigen lassen. Wählen Sie aus dieser Liste Ihr neues Zertifikat der Bayern-PKI aus und bestätigen Sie die Auswahl durch Klick auf OK. Wenn Sie in der Liste Ihr Zertifikat nicht entdecken können, wiederholen Sie bitte den Zertifikatsimport wie in Kapitel 2.2 beschrieben. Sollte der Fehler danach wieder auftauchen, wenden Sie sich bitte an den PKI-Support der Bayern-PKI (die Kontaktinformationen finden Sie am Ende des Handbuchs).

Hinweis: Falls Sie signierte E-Mails an Empfänger senden wollen, von denen Sie sicher wissen, dass sie noch Outlook 2003 oder Outlook 2007 unter Windows XP einsetzen, dann belassen Sie den `Hashalgorithmus` bei `SHA1`.

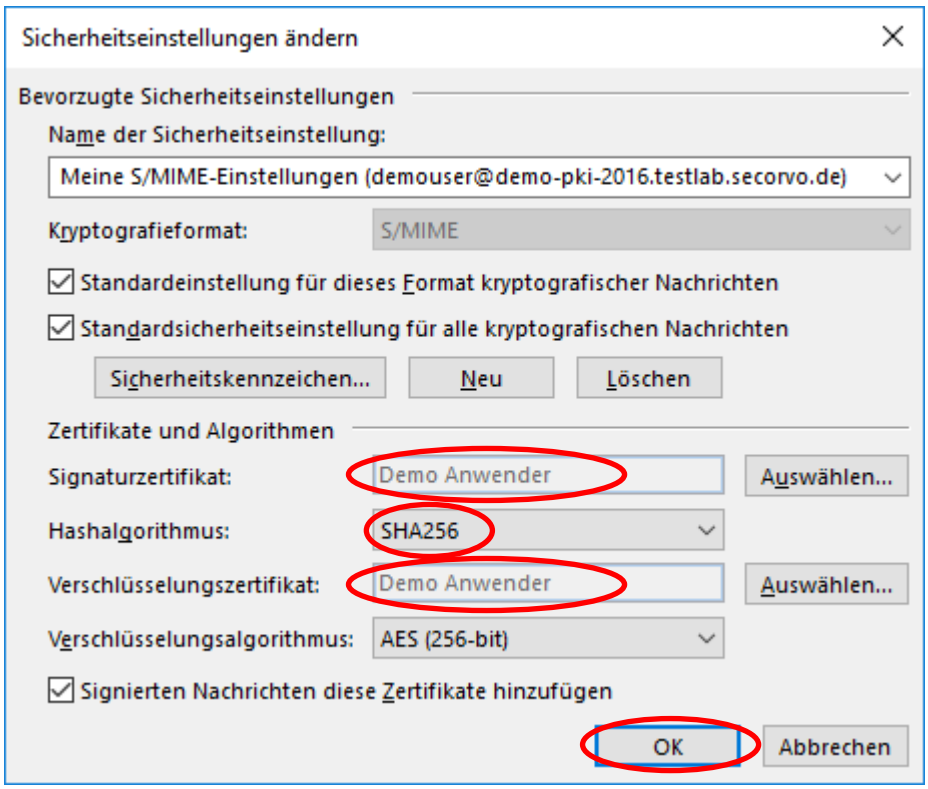


Abbildung 13: Prüfen der vorausgewählten Zertifikate und Einstellung des Hashalgorithmus

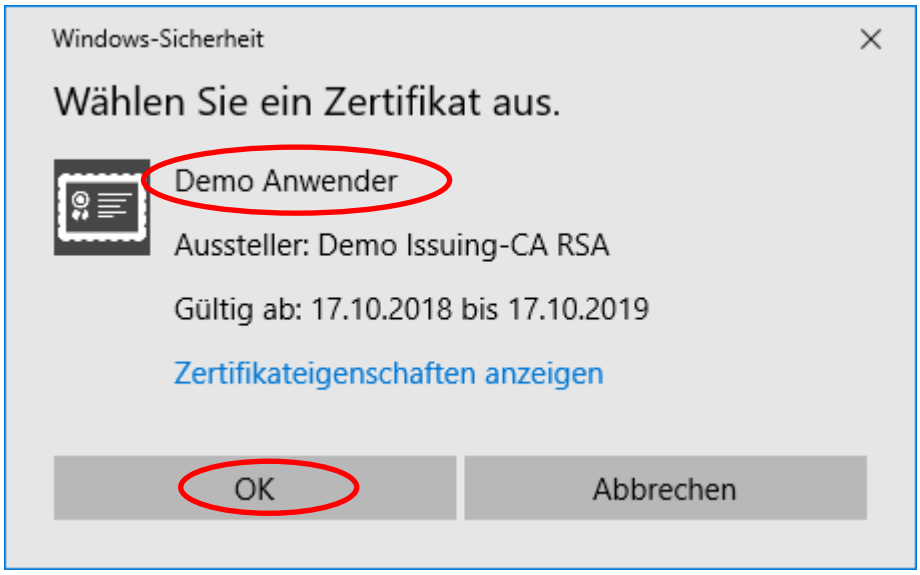


Abbildung 14: Explizite Auswahl eines Zertifikats (nur im Bedarfsfall)

Schließen Sie zuletzt die beiden Fenster des Trust Centers und der Outlook-Optionen durch Klick auf `OK`.

3.2 Einrichten der LDAP-Verbindung zum Verzeichnisdienst des BYBN

Die E-Mail-Zertifikate, die von der Bayern-PKI für Mitarbeiter in der öffentlichen Verwaltung erstellt wurden, werden zentral in einem internen LDAP Verzeichnisdienst des Bayerischen Behördennetzes BYBN veröffentlicht.

Sofern der Zertifikatsinhaber einer externen Veröffentlichung zugestimmt hat, werden die E-Mail-Zertifikate zusätzlich in einem per Internet zugänglichen externen LDAP Verzeichnisdienst veröffentlicht.

Um Anwendern im BYBN eine verschlüsselte E-Mail zu senden, benötigt Ihr Outlook deren Verschlüsselungszertifikate. Outlook sucht jedoch standardmäßig nicht in den Verzeichnisdiensten der Bayern-PKI nach diesen Zertifikaten. Dazu muss zunächst eine Verbindung zu den Verzeichnisdiensten eingerichtet werden.

Welcher Verzeichnisdienst (intern, extern oder beide) konfiguriert werden sollte, richtet sich danach, ob Sie immer, nie bzw. zweitweise Zugang zum BYBN haben.

Hinweis: Die jeweils aktuellen Konfigurationsdaten zu diesen Verzeichnisdiensten (Servername, Port, Suchbasis etc.) finden Sie unter https://www.pki.bayern.de/vpki/allg/zertabruf/index.html
Nachfolgend werden die Konfigurationsdaten verwendet, die zum Zeitpunkt der Erstellung dieses Handbuchs für den Verzeichnisdienst im BYBN (`directory.bybn.de`) aktuell waren. Für den im Internet erreichbaren Verzeichnisdienst (`directory.bayern.de`) verfahren Sie analog.

Klicken Sie im Hauptfenster von Outlook auf `Datei`, dann auf `Kontoeinstellungen`, und schließlich nochmals auf `Kontoeinstellungen…` .

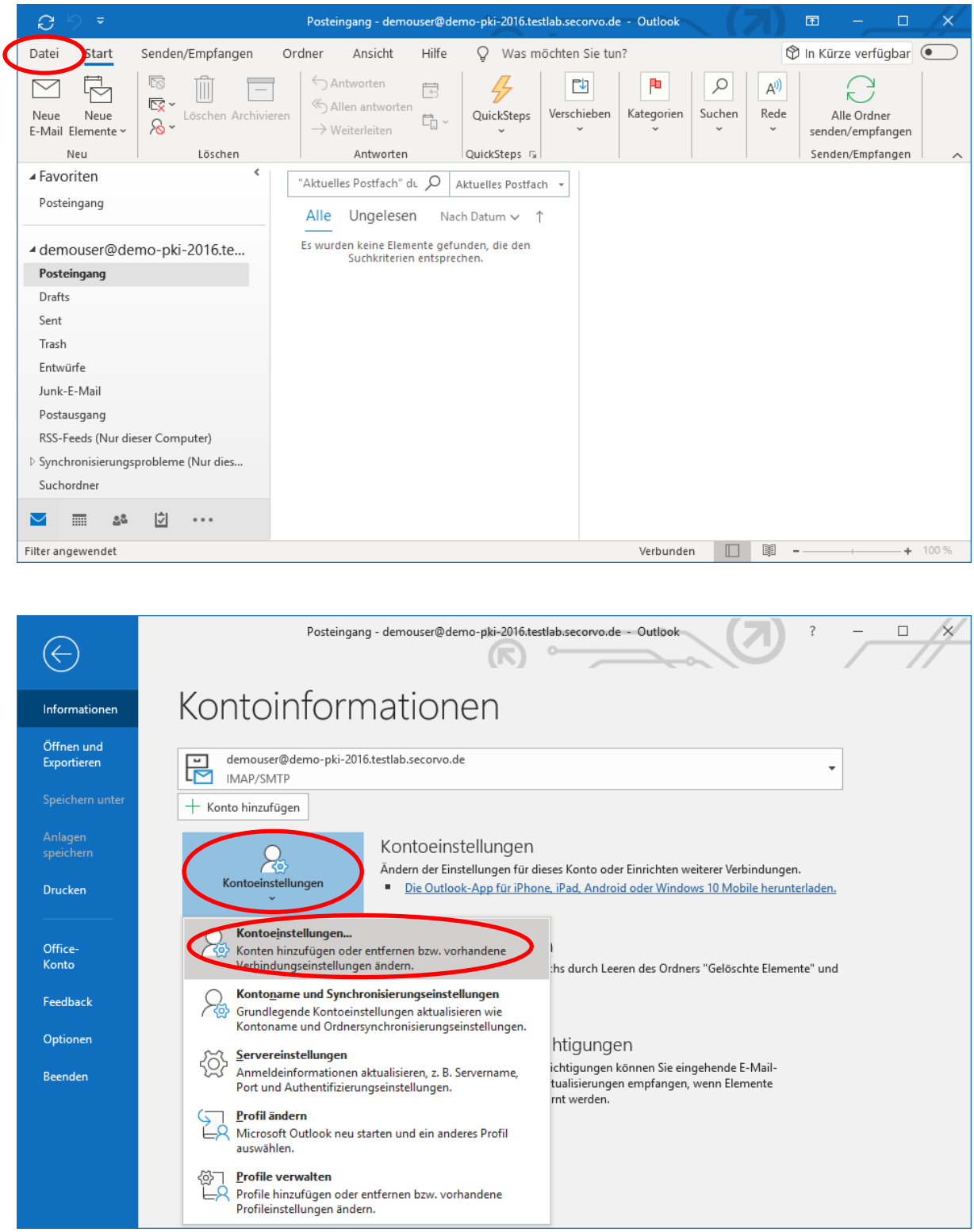


Abbildung 15: Aufruf der Kontoeinstellungen in Outlook

Wählen Sie den Kontoeinstellungen `Adressbücher` aus und klicken Sie dann auf `Neu...`.

Hinweis: Möglicherweise hat Ihr Administrator bereits die LDAP-Verbindung zu im internen und/oder externen Verzeichnisdienst eingerichtet. Falls an dieser Stelle bereits ein Adressbuch mit dem Namen `directory.bybn.de` oder `directory.bayern.de` und Typ `LDAP` angezeigt wird (siehe Abbildung 23), dann können Sie die restlichen Schritte in diesem Kapitel überspringen.

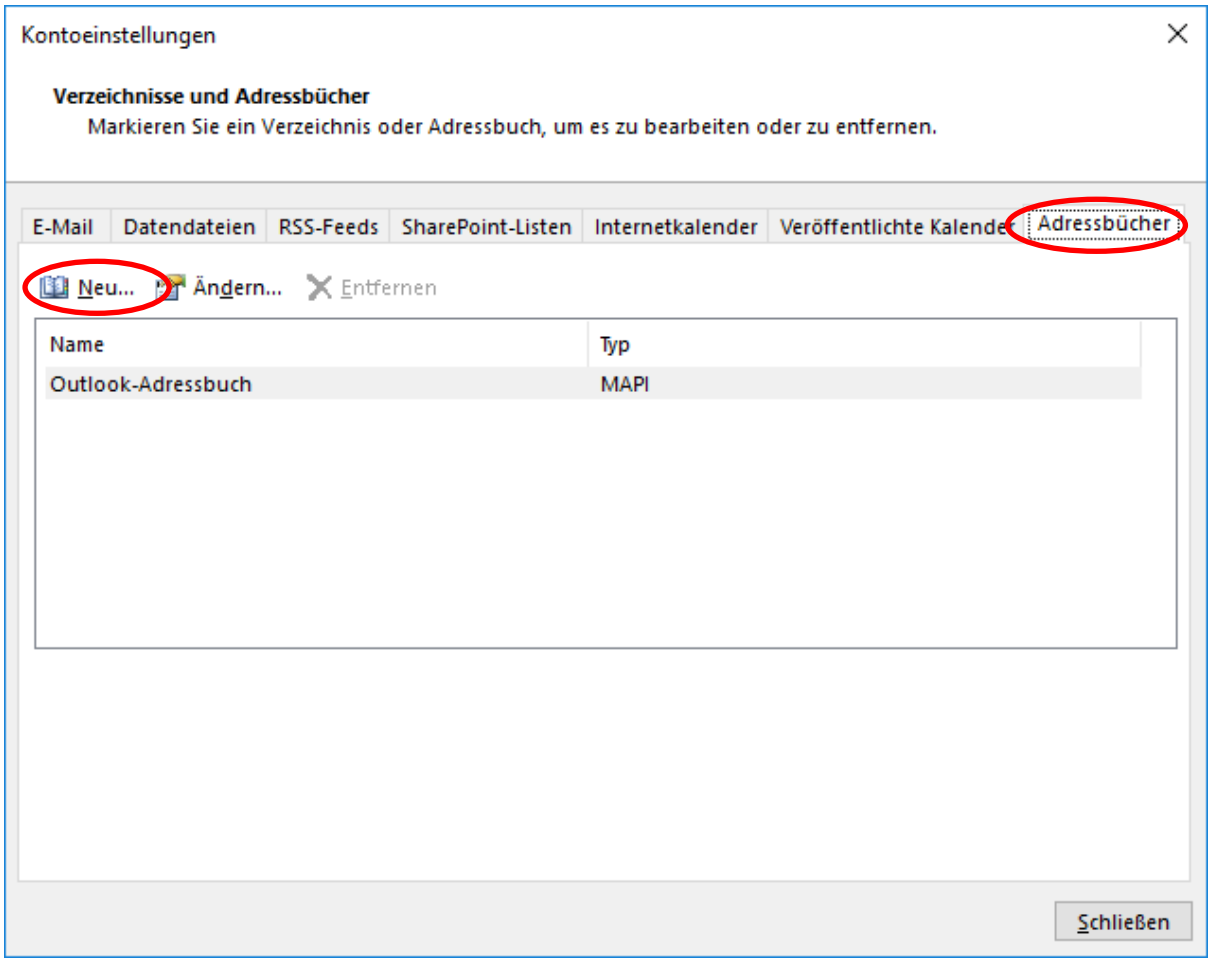


Abbildung 16: Hinzufügen einer Verbindung zum LDAP-Server als Outlook-Adressbuch

Belassen Sie die Vorauswahl `Internetverzeichnisdienst (LDAP)` und klicken Sie auf `Weiter >`.

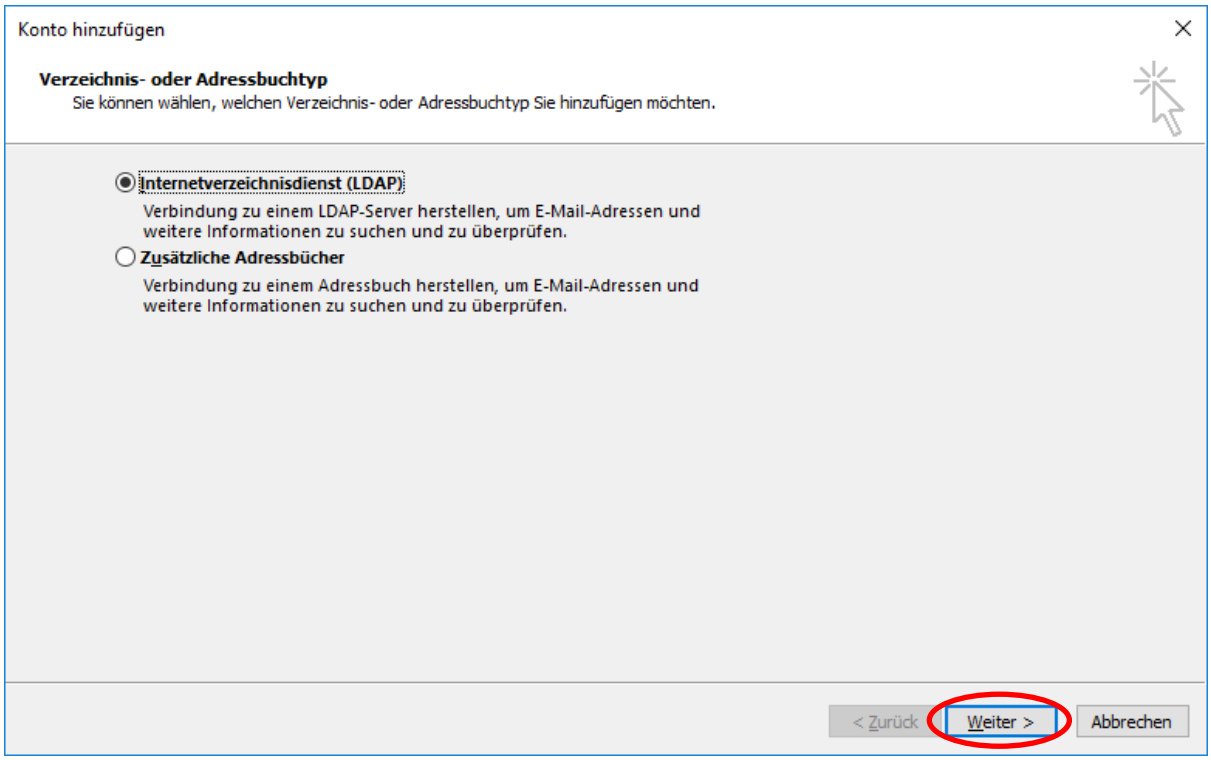


Abbildung 17: Auswahl von LDAP als Schnittstelle zum Verzeichnisdienst

Geben Sie bei `Servername` `directory.bybn.de` bzw. für den externen Verzeichnisdienst `directory.bayern.de` ein. Die Option `Server erfordert Anmeldung` bleibt deaktiviert. Klicken Sie dann auf `Weitere Einstellungen...`.

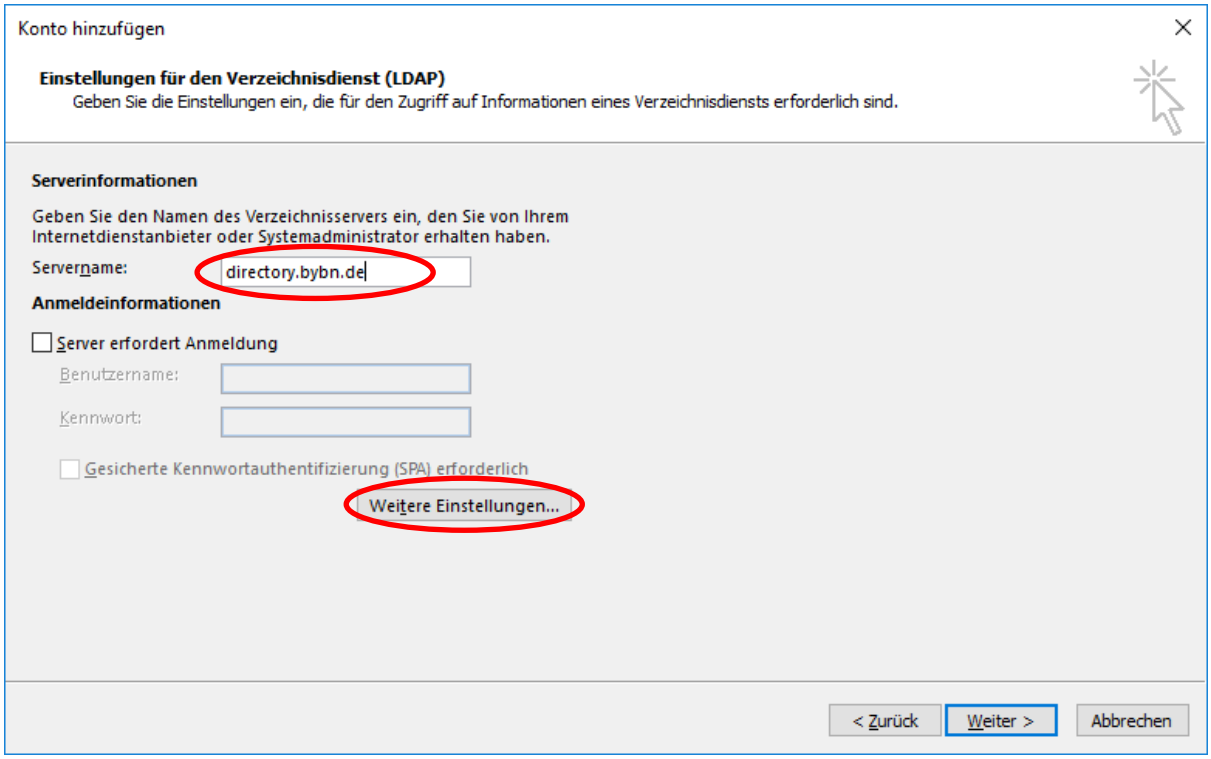


Abbildung 18: Einstellen des Servernamens

Hinweis: Unter Umständen erscheint nach dem Klick auf `Weitere Einstellungen...` ein Hinweis, dass Outlook nach dieser Änderung neu gestartet werden muss. Bestätigen Sie diesen Hinweis ggf. mit `OK`.

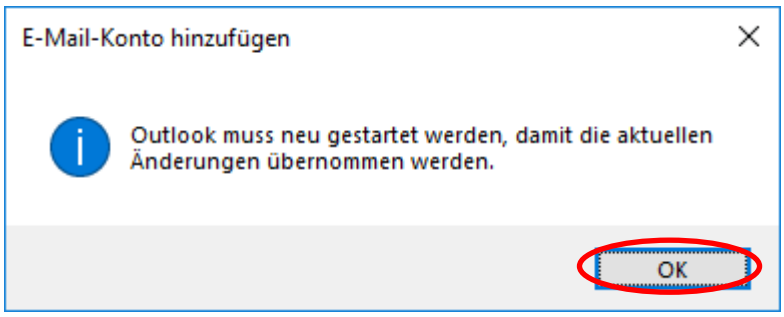


Abbildung 19: Hinweis auf den erforderlichen Neustart von Outlook

In den Einstellungen des LDAP-Servers klicken Sie auf `Suche`. Wählen Sie die `Suchbasis` `Benutzerdefiniert` und geben Sie als Wert für die Suchbasis `ou=pki-teilnehmer,dc=pki,dc=bybn,dc=de` ein. Schließen Sie das Einstellungsfenster mit `OK`.

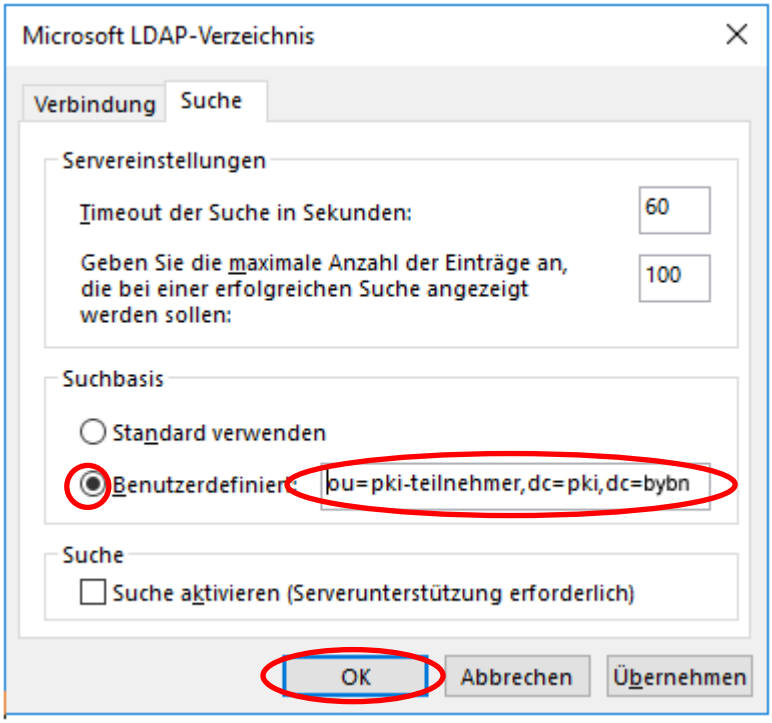


Abbildung 20: Einstellung der Suchbasis

Klicken Sie jetzt im Fenster des Assistenten zum Hinzufügen eines Adressbuchs auf `Weiter >`.

Hinweis: Nach dem Klick auf `Weiter >` wird die u. U. eingestellte Verbindung zum Verzeichnisdienst getestet. Abhängig von der Netzwerkverbindung kann es dann zu einer spürbaren Verzögerung kommen, bis sich das nächste Fenster komplett aufgebaut hat.

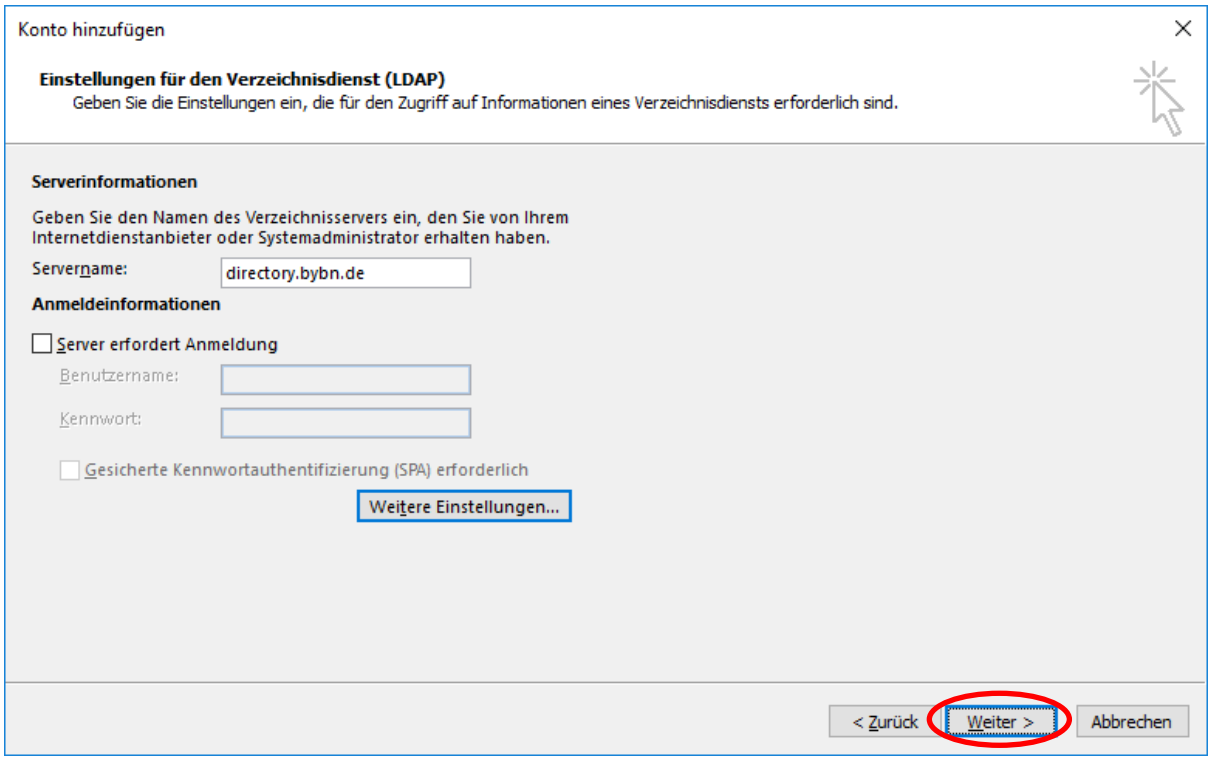


Abbildung 21: Fortsetzen des Assistenten zum Hinzufügen eines Adressbuchs

Entfernen Sie das Häkchen bei `Outlook Mobile auch auf meinem Telefon einrichten` und beenden Sie den Assistenten zum Hinzufügen eines Adressbuchs durch Klick auf `Fertig stellen`.

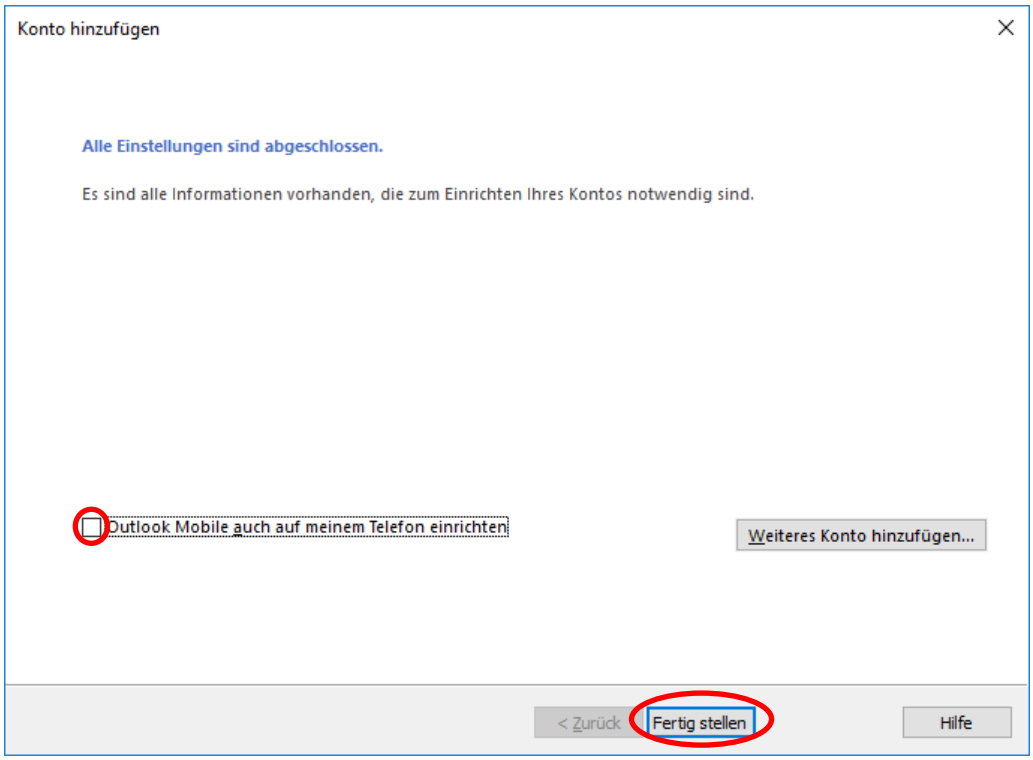


Abbildung 22: Rückmeldung des Assistenten zum Hinzufügen eines Adressbuchs

In den Kontoeinstellungen taucht jetzt die neu eingerichtete LDAP-Verbindung auf. Klicken Sie zuletzt auf `Schließen`.

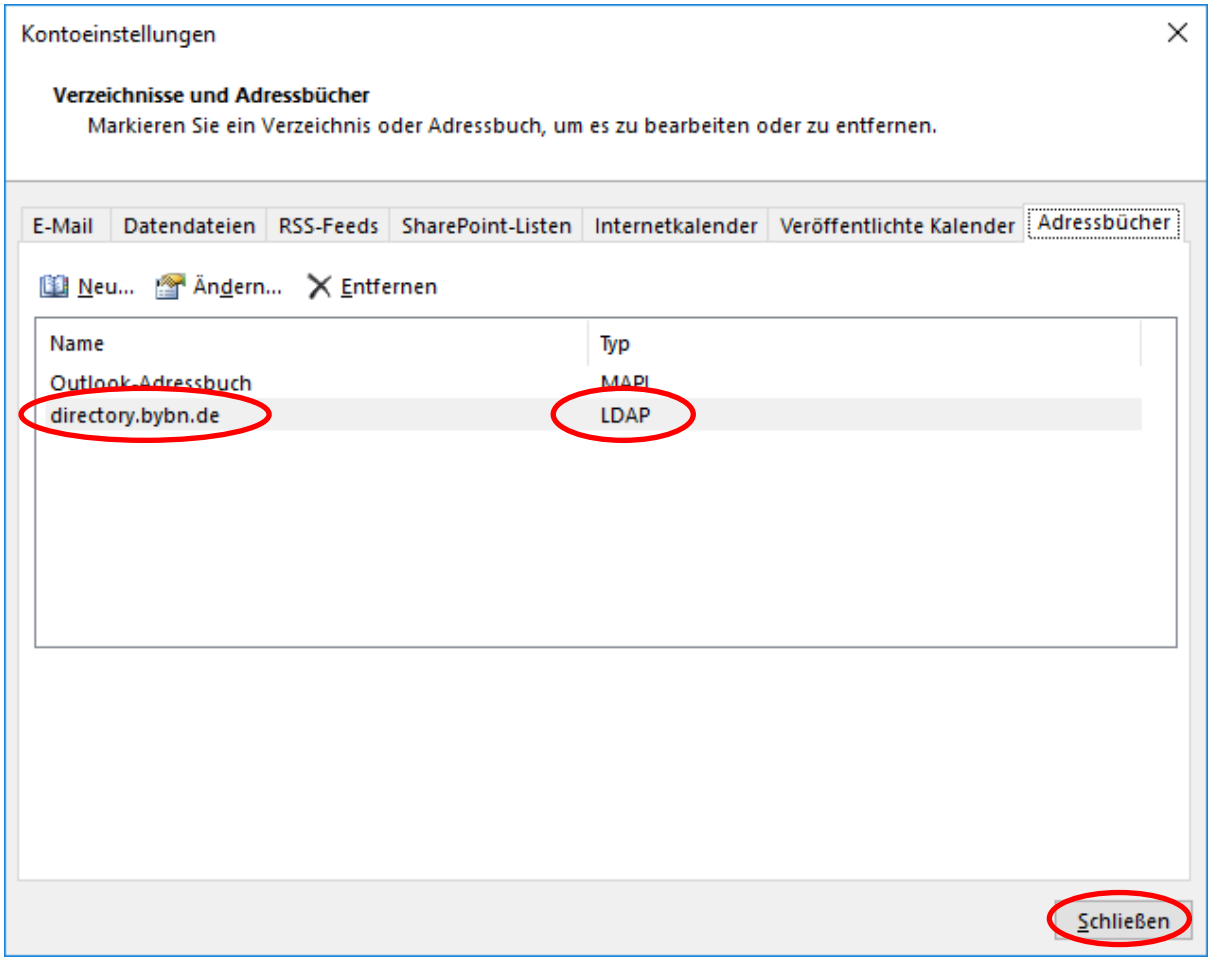


Abbildung 23: Neue LDAP-Verbindung in der Liste der Adressbücher

Beenden Sie nach Abschluss dieser Einstellungen Outlook und starten Sie es neu.

4 Nutzung sicherer E-Mails bei der täglichen Arbeit

Wenn alle in den vorigen Kapiteln aufgeführten Einrichtungsschritte erfolgreich durchgeführt wurden, können Sie im täglichen Betrieb – wann immer dieser Grad an Sicherheit benötigt wird – Ende-zu-Ende verschlüsselte und/oder signierte E-Mails mit anderen Nutzern des BYBN austauschen.

Sofern ein Kommunikationspartner im Internet dem Wurzelzertifikat der Verwaltungs-PKI vertraut, ist ggf. auch ein Austausch verschlüsselter und/oder signierte E-Mails über das Internet möglich.

Wichtig: Sie können eine verschlüsselte E-Mail jedoch nur dann absenden, wenn Ihr Outlook-Client Zugriff auf ein gültiges Verschlüsselungszertifikat eines jeden Empfängers der E-Mail (egal ob An:, Cc: oder Bcc:) hat. Umgekehrt können Absender Ihnen nur dann eine verschlüsselte E-Mail senden, wenn sie Zugriff auf Ihr Verschlüsselungszertifikat haben. Aus diesem Grund wurde die Verbindung zum Verzeichnisdienst des BYBN eingerichtet (vgl. Kapitel 3.2), über den die Zertifikate der Bayern-PKI für Nutzer im BYBN zugänglich sind.

Nur signierte, aber nicht verschlüsselte E-Mails können Sie auch absenden, ohne dass Ihnen ein Zertifikat des Empfängers vorliegt – sogar an Empfänger, die über gar kein E-Mail-Zertifikat verfügen.

Hinweis: Outlook fügt signierten E-Mails automatisch sowohl ihr Signaturzertifikat als auch Ihr Verschlüsselungszertifikat bei. Falls Sie oder Ihr Gegenüber nicht auf die Verschlüsselungszertifikate des anderen zugreifen können, kann es helfen, zunächst nur signierte E-Mails auszutauschen; die meisten gängigen E-Mail-Clients sind in der Lage, aus einer signierten E-Mail das Verschlüsselungszertifikat des Absenders zu entnehmen.

4.1 Versand verschlüsselter und/oder signierter E-Mail-Nachrichten

4.1.1 Regelfall

Erstellen Sie wie üblich eine neue E-Mail-Nachricht. Solange Sie diese E-Mail noch nicht gesendet haben, können Sie unter `Optionen` über die beiden Symbole für `Verschlüsseln` und `Signieren` auswählen, ob und wie die E-Mail gesichert werden soll.

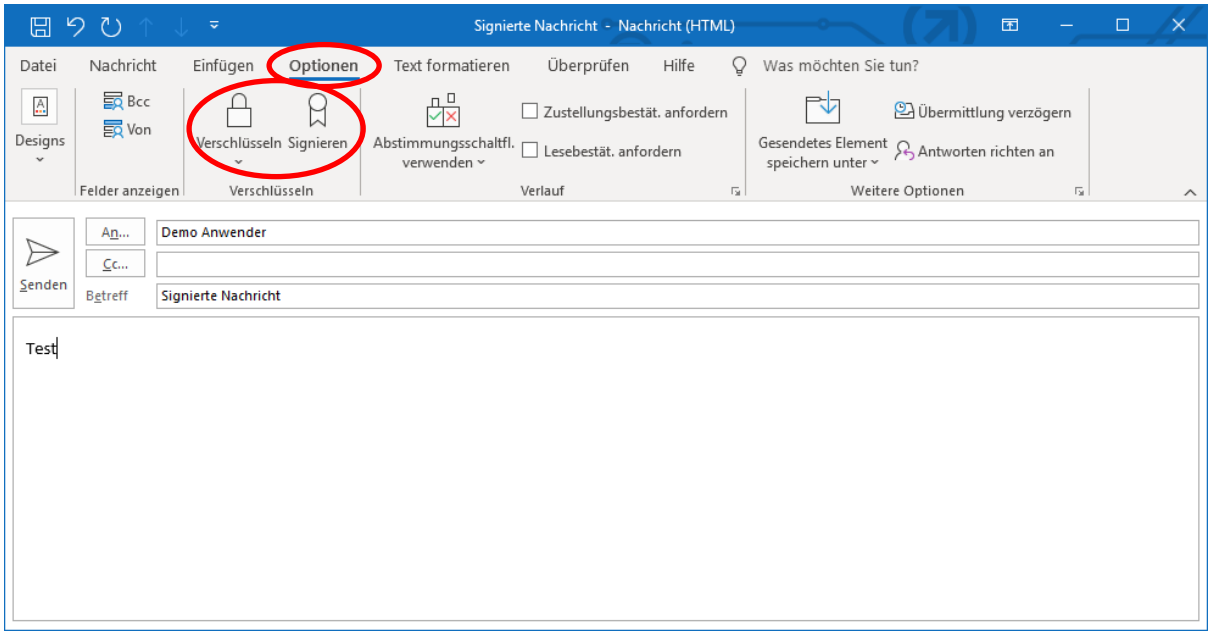


Abbildung 24: Aktivierung der Optionen „Verschlüsseln“ und/oder „Signieren“

Wenn Sie ausgewählt haben, die E-Mail zu signieren, erscheint nach dem Klick auf `Senden` ein Dialog, in dem Sie nach dem Passwort für den privaten Schlüssel gefragt werden. Geben sie hier das Passwort ein, das Sie selbst beim Import der Schlüsseldatei vergeben haben (vgl.Abbildung 7) und bestätigen Sie mit `Zulassen`.

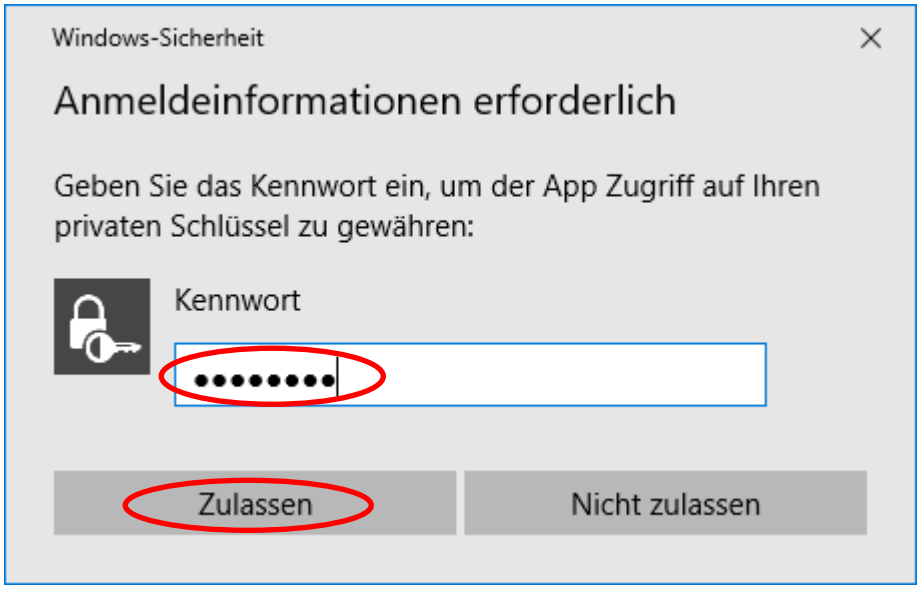


Abbildung 25: Passworteingabe für die Nutzung Ihres privaten Schlüssels beim Versand einer signierten E-Mail

Wichtig: Falls eine solche Passwortabfrage unmotiviert erscheinen sollte, klicken Sie auf `Nicht zulassen`. In diesem Fall könnte eine Schadsoftware im Hintergrund versuchen, Ihren Schlüssel zu missbrauchen. Wenden Sie sich diesbezüglich bitte an Ihren lokalen Administrator.

Beim Senden einer nur verschlüsselten, aber nicht signierten E-Mail erscheint keine Passwort-Abfrage.

Das Senden einer verschlüsselten E-Mail wird fehlschlagen, falls nicht von allen Empfängern ein Verschlüsselungszertifikat vorliegt. Klicken Sie in diesem Fall auf `Abbrechen`.

Hinweis: Versuchen sie die Empfänger der E-Mail noch einmal über das Adressbuch einzugeben, damit auch ihre Zertifikate – sofern vorhanden – von dort bezogen werden. Ggf. bitten Sie Ihr Gegenüber, Ihnen ihr bzw. sein Verschlüsselungszertifikat zuzusenden.

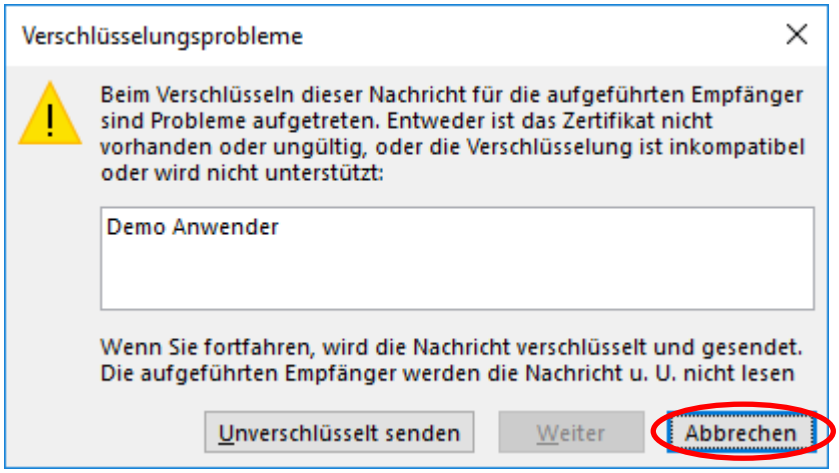


Abbildung 26: Fehlermeldung, falls nicht für alle Empfänger Verschlüsselungszertifikate vorliegen

Hinweis: E-Mails, die Sie verschlüsselt senden, werden auch für sie als Absender verschlüsselt und so im Ausgangsportfach (`Gesendete Elemente` bzw. `Sent`) abgelegt.

Beim Lesen selbst gesendeter verschlüsselter E-Mails gilt sinngemäß das gleiche wie unten für den Empfang von verschlüsselten E-Mails beschrieben.

4.1.2 Versand über eine Funktionsadresse

Die Auswahl einer Funktionsadresse, unter der die Nachricht versendet werden soll, erfolgt unabhängig von Verschlüsselung und Signatur wie bei unverschlüsselten Nachrichten.

Zur Nutzung von Verschlüsselung und Signatur über eine Funktionsadresse müssen Sie auch Zertifikate für dieses Funktionsadresse von der Bayern-PKI beziehen und wie in Kapitel 2 beschrieben in Ihren Windows-Zertifikats- und Schlüsselspeicher importieren.

Outlook wählt dann automatisch anhand des ausgewählten Absenders zwischen den persönlichen Zertifikaten und denen der Funktionsadresse aus und verwendet diejenigen, in denen die passende E-Mail-Adresse enthalten ist.

E-Mails, die Sie über eine Funktionsadresse verschlüsselt absenden, werden dementsprechend mit dem Verschlüsselungszertifikat und Schlüssel der Funktionsadresse verschlüsselt in Ihrem eigenen Postausgang abgelegt.

4.1.3 Besonderheiten bei Antworten, Weiterleitungen und Verteilerlisten

Bei der **Antwort** auf eine empfangene E-Mail wird deren Verschlüsselungseinstellung übernommen, d. h bei der Antwort auf eine verschlüsselte und signierte E-Mail sind die Optionen `Verschlüsseln` und `Signieren` bereits aktiviert; ggf. müssen Sie sie deaktivieren.

Des Weiteren sind bei der Antwort auf eine E-Mail die Empfängerfelder bereits vorbelegt. Falls Outlook beim Senden der E-Mail nicht alle Verschlüsselungszertifikate findet (vgl. Abbildung 26), sollten Sie ggf. die vorbelegten Empfänger löschen und über das Adressbuch wieder neu hinzufügen, damit Outlook darüber die Verschlüsselungszertifikate empfangen kann.

Bei **Weiterleitungen** gilt das gleiche wie bei Antworten. Auch hier werden die Optionen `Verschlüsseln` und `Signieren` bereits entsprechend der weitergeleiteten E-Mail aktiviert.

Der Versand von verschlüsselten und/oder signierten Nachrichten an persönliche **Verteilerlisten** ist möglich, wenn deren Mitgliedern bei der Zusammenstellung der Verteilerliste im persönlichen Adressbuch ein Zertifikat zugeordnet war.

4.2 Empfang verschlüsselter und/oder signierter E-Mail-Nachrichten

In der Postfach-Ansicht werden empfangene, verschlüsselte bzw. signierte E-Mails mit entsprechenden Symbolen markiert.

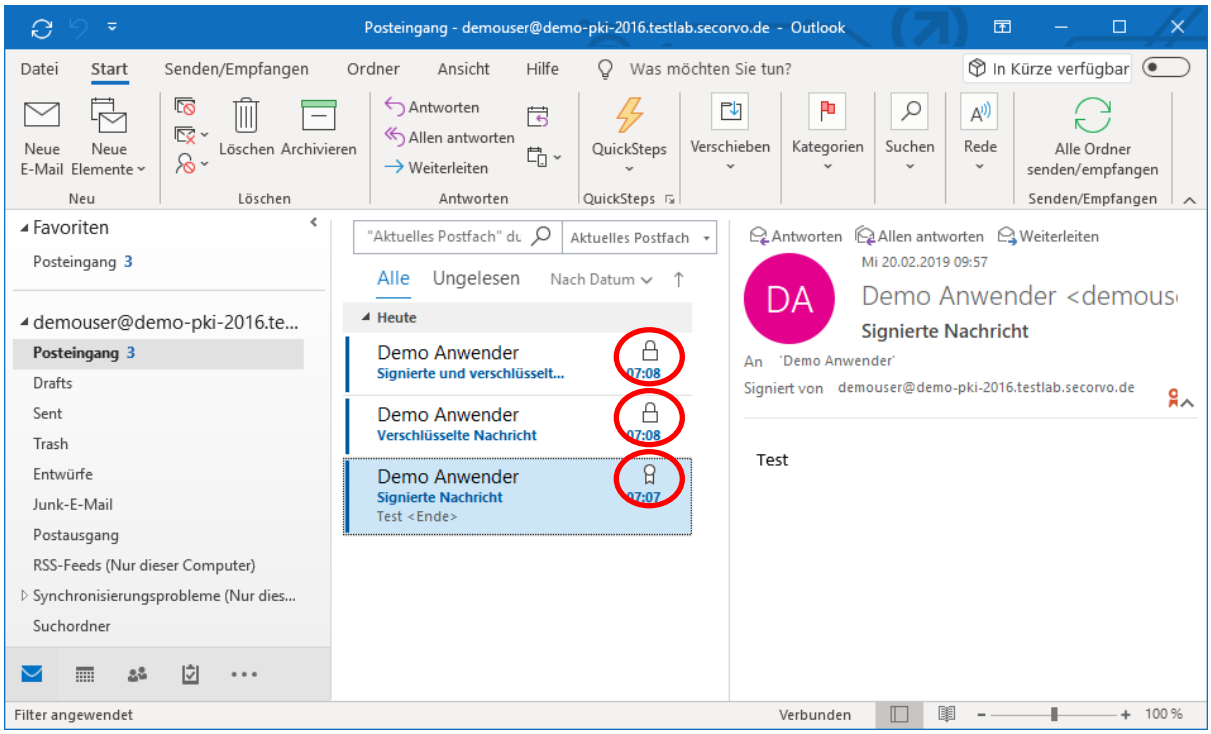


Abbildung 27: Symbole zur Anzeige verschlüsselter bzw. signierte E-Mails in der Postfachansicht

Sobald Sie eine verschlüsselte (oder verschlüsselte und signierte) E-Mail auswählen, erscheint ein Dialog, in dem Sie nach dem Passwort für den privaten Schlüssel zur Entschlüsselung gefragt werden. Geben Sie hier das Passwort ein, das Sie selbst beim Import der Schlüsseldatei vergeben haben (vgl. Abbildung 7) und bestätigen Sie mit `Zulassen`.

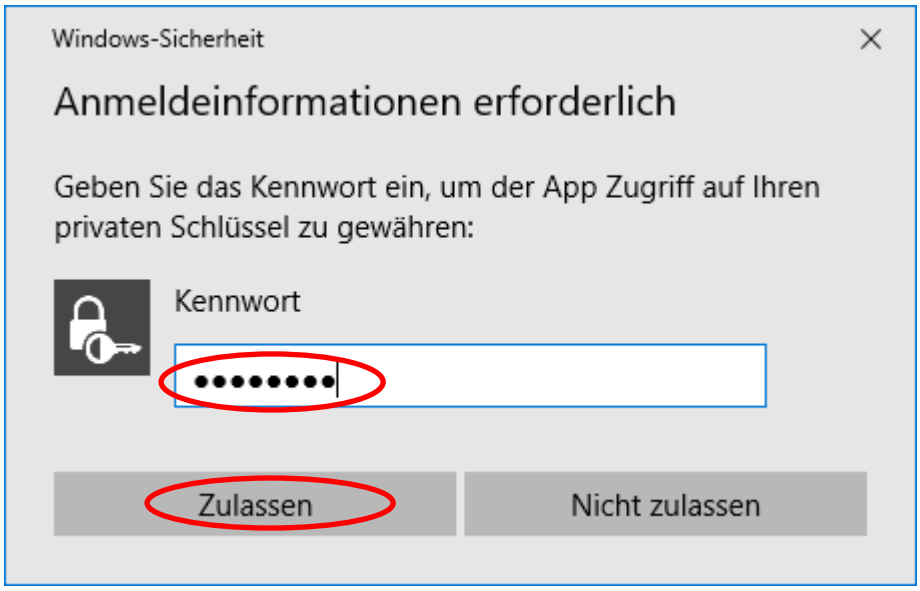


Abbildung 28: Passworteingabe für die Nutzung Ihres privaten Schlüssels zum Lesen einer verschlüsselten E-Mail

Wichtig: Falls eine solche Passwortabfrage unmotiviert erscheinen sollte, klicken Sie auf `Nicht zulassen`. In diesem Fall könnte eine Schadsoftware im Hintergrund versuchen,

Ihren Schlüssel zu missbrauchen. Wenden Sie sich diesbezüglich bitte an Ihren lokalen Administrator.

Falls eine empfangene E-Mail mit einem älteren – bei archivierten Nachrichten evtl. auch bereits abgelaufenen – Verschlüsselungszertifikat oder dem Verschlüsselungszertifikat einer Funktionsadresse verschlüsselt wurde, ordnet Outlook automatisch den richtigen Schlüssel zu und entschlüsselt die Nachricht damit, solange sich der entsprechende private Schlüssel in Ihrem Windows-Schlüsselspeicher befindet.

Beim Empfang einer unverschlüsselten, aber signierten Nachricht wird kein Passwort für die Nutzung eines privaten Schlüssels benötigt.

Bei einer geöffneten, signierten und/oder verschlüsselten E-Mail wird der Status durch eines bzw. zwei Symbole am rechten Rand der Kopf-Information angezeigt. Durch einen Klick auf diese Symbole können Sie sich genauere Informationen zu der bei dieser E-Mail angebrachten Signatur bzw. Verschlüsselung anzeigen lassen.

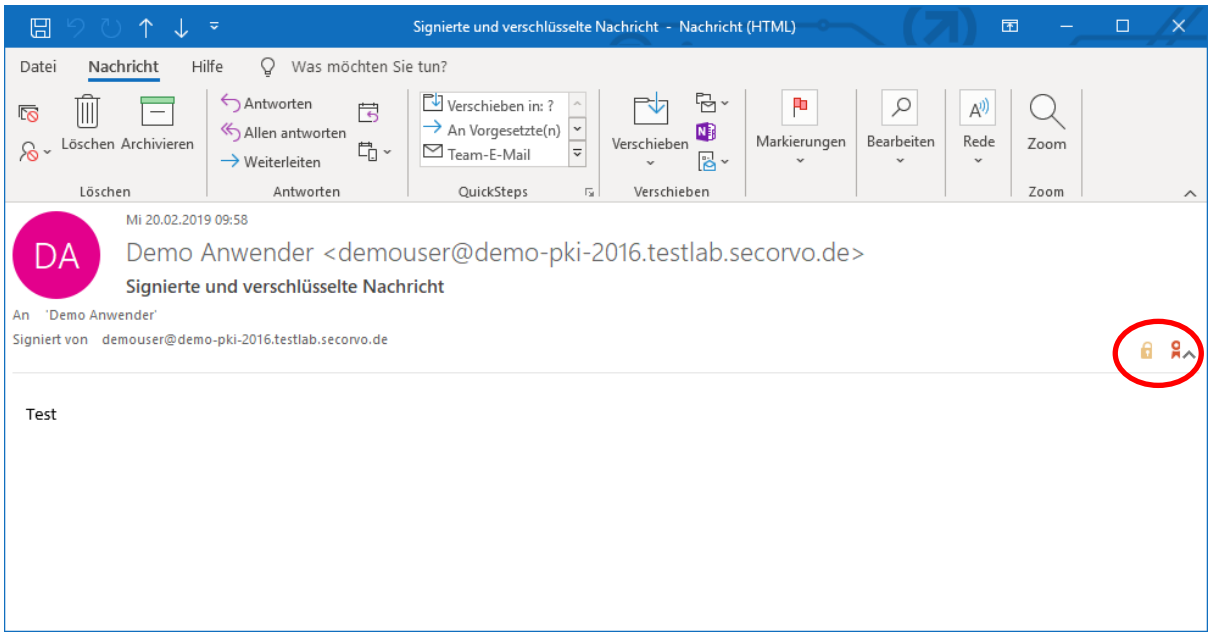


Abbildung 29: Symbole zur Anzeige verschlüsselter bzw. signierte E-Mails in der geöffneten E-Mail

5 Hinweise für den Administrator

5.1 Vorkonfiguration von Outlook 2019

Durch Setzen des Registry-Wertes (DWORD)

`HKEY_CURRENT_USER\Software\Microsoft\Office\16.0\Outlook\Preferences\SecurityAlwaysShowButtons`

auf den Wert (DWORD) `1` wird das Verhalten von Outlook so geändert, dass eine Einstellung von Outlook 20199 (Schritt 3 oben) durch den Endanwender in den meisten Fällen nicht mehr notwendig ist.

Nach Setzen dieser Konfigurationsoption blendet Outlook beim Erstellen einer neuen Nachricht die Schaltknöpfe für die Optionen für „Verschlüsseln“ und „Signieren“ immer ein, sobald im Zertifikatsspeicher des angemeldeten Benutzers gültige, für S/MIME einsetzbare Zertifikate gefunden werden.

Die entsprechende Registry-Einstellung kann bspw. über ein Group Policy vorgenommen werden. Alternativ kann eine `.reg` Datei mit dem folgenden Inhalt erstellt und in die Registry der jeweiligen Systeme importiert werden.

```
Windows Registry Editor Version 5.00

[HKEY_CURRENT_USER\Software\Microsoft\Office\16.0\Outlook\Preferences]
"SecurityAlwaysShowButtons"=dword:00000001
```

5.2 Vorgabe der Schutzstufe für private Schlüssel

Durch Setzen des Registry-Wertes (DWORD)

`HKEY_LOCAL_MACHINE\Software\Policies\Microsoft\Cryptography\ForceKeyProtection`

auf einen der Werte (DWORD) `0`, `1` oder `2` kann vorgegeben werden, unter welchen Schutzstufen für den privaten Schlüssel (siehe Kapitel 2.1) der Anwender beim Import oder der Neuanlage auswählen darf

- Bei Wert `0` kann der Anwender unter den Schutzstufen **einfach**, **mittel** oder **hoch** auswählen.
- Bei Wert `1` kann der Anwender unter den Schutzstufen **mittel** oder **hoch** auswählen.
- Bei Wert `2` muss der Anwender die Schutzstufe **hoch** verwenden.

Alternativ kann diese Einstellung über die lokale Sicherheitsrichtlinie oder die Group Policy für Computer mittels der Sicherheitsoption „`Systemkryptografie: Starken Schlüsselschutz für auf dem Computer gespeicherte Benutzerschlüssel erzwingen`“ konfiguriert werden, die – entsprechend der Registry-Werte `0`, `1` oder `2` – auf einen der drei folgenden Werte eingestellt werden kann:

- `Keine Benutzereingabe erforderlich, wenn neue Schlüssel gespeichert und verwendet werden`
- `Benutzer wird zur Eingabe aufgefordert, wenn der Schlüssel zum ersten Mal verwendet wird`
- `Bei jeder Verwendung eines Schlüssels Kennwort eingeben`

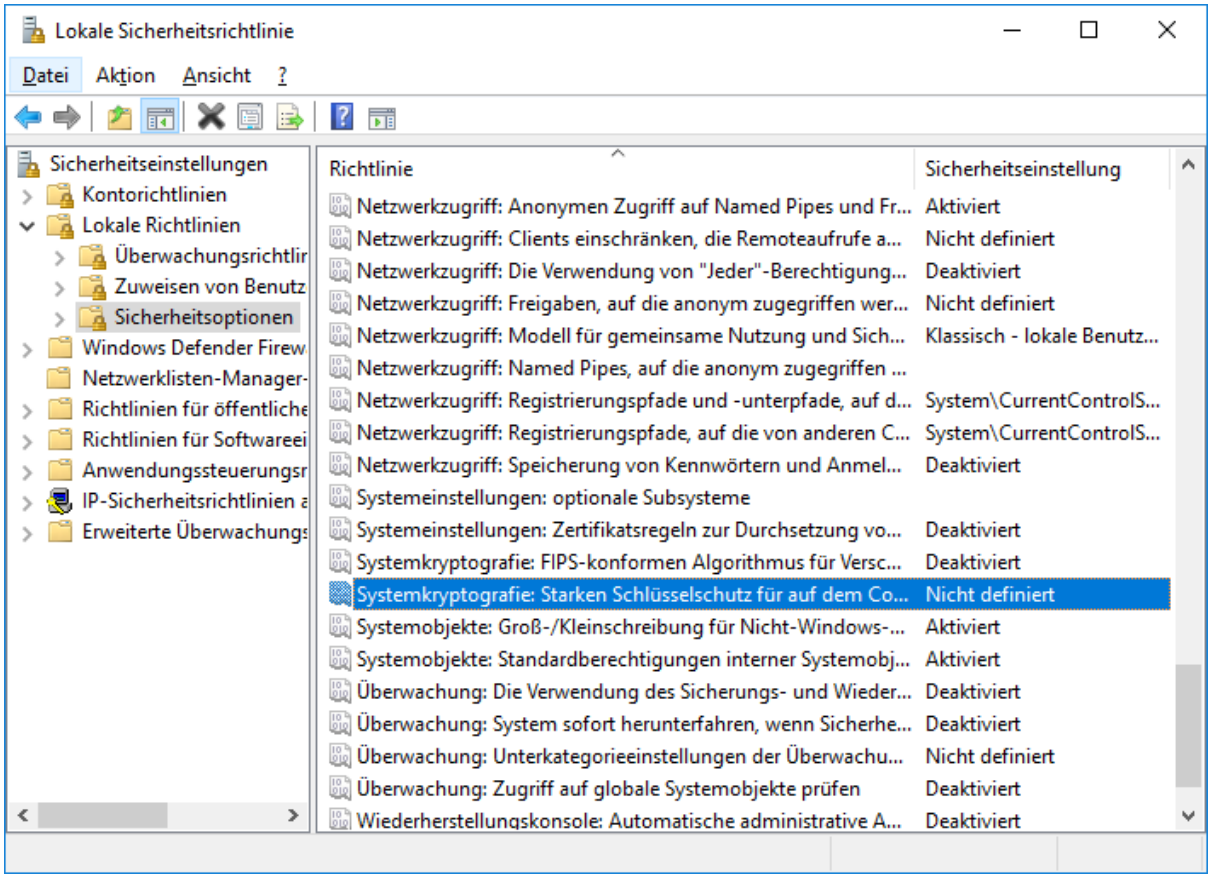


Abbildung 30:Policy-Einstellung zur Vorgabe der Schutzstufe für private Schlüssel

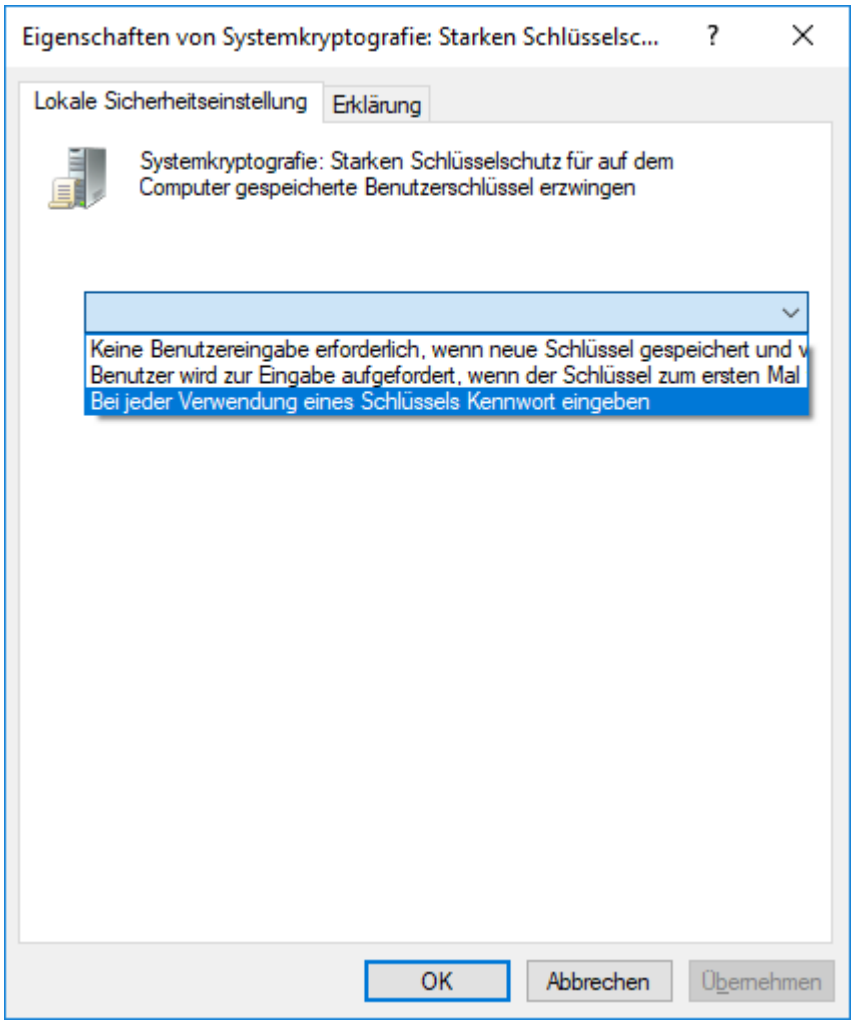


Abbildung 31:Einstellbare Werte zur Vorgabe der Schutzstufe für private Schlüssel

Hinweis: Diese Einstellung – egal, ob über Registry oder Group Policy – wirkt sich nicht nur auf die Schlüssel zu den Zertifikaten der Bayern-PKI aus, sondern auf alle privaten Schlüssel, die von irgendeinem Benutzer auf dem betreffenden System generiert oder importiert werden. Vor einer Verschärfung der Einstellung sollte daher geprüft werden, ob sich dadurch nicht Probleme für andere Benutzer oder andere Anwendungen ergeben.

Beispielsweise kann u. U. bei einer Verbindung mit einem WLAN-Netzwerk oder mit einem WebDAV-Server[1] kein Prompt-Fenster auf dem Desktop des Anwenders angezeigt werden. Daher können Zertifikate, deren private Schlüssel mit Stufe **mittel** oder **hoch** geschützt sind, nicht zur Anmeldung in diesen Anwendungen verwendet werden.

[1] Siehe https://support.microsoft.com/fr-fr/help/2692537/windows-7-the-pin-dialog-box-does-not-appear-when-certificate-security

Kontaktinformationen PKI-Support

Bei Fragen und Problemen rund um die Verwaltung und Nutzung der Zertifikate der Bayern-PKI steht Ihnen der PKI Support des IT-Dienstleistungszentrums im Landesamt für Digitalisierung, Breitband und Vermessung gerne zur Verfügung.

Telefonnummer: **089 / 2119-4924**

E-Mail Adresse: pki-support@ldbv.bayern.de