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 2024 unter Windows 11

Überblick 3

1 Empfang der Zertifikate per E-Mail 3

2 Import der Zertifikate und Schlüssel in Windows 11 3

2.1 Vorbemerkung zu den Optionen beim Schlüsselimport 3

2.2 Import der Schlüsseldateien 4

3 Einstellung von Outlook 2024 12

3.1 Einstellungen für die Nutzung der Zertifikate 12

3.2 Einrichten der LDAP-Verbindung zum Verzeichnisdienst des BYBN 18

4 Nutzung sicherer E-Mails bei der täglichen Arbeit 27

4.1 Versand verschlüsselter und/oder signierter E-Mail-Nachrichten 27

4.1.1 Regelfall 27

4.1.2 Versand über eine Funktionsadresse 29

4.1.3 Besonderheiten bei Antworten, Weiterleitungen und Verteilerlisten 29

4.2 Empfang verschlüsselter und/oder signierter E-Mail-Nachrichten 30

Kontaktinformationen PKI-Support 31

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 2024 unter Windows 11 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 11
3. Einstellung von Outlook 2024
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. Auf Nachfrage können Informationen für Administratoren gesondert geliefert werden.

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 bzw. zum digitalen Signieren von Nachrichten (zusammen mit den zugehörigen Zertifikaten) enthält und per Transport-PIN geschützt ist.
Diese Transport-PIN für Ihre beiden `.p12`-Schlüsseldateien können Sie nach Ihrer Anmeldung im Zertifikatsverwaltungssystem PRIME sowie nach 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 11

2.1 Vorbemerkung zu den Optionen beim Schlüsselimport

Beim Import eines privaten Schlüssels erlaubt Windows Ihnen die Wahl zwischen drei Sicherheitsstufen, die bestimmen 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 öffnen 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.

Unter Umständen hat auch Ihr Administrator bereits eingeschränkt, welche dieser Schutzstufen Sie beim Import der Schlüsseldatei auswählen können.

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 dieser 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 exportieren. Das ist vergleichbar mit derjenigen, in der sie Zertifikat und Schlüssel von der Bayern-PKI erhalten haben.
- 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 vorherigen 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`.

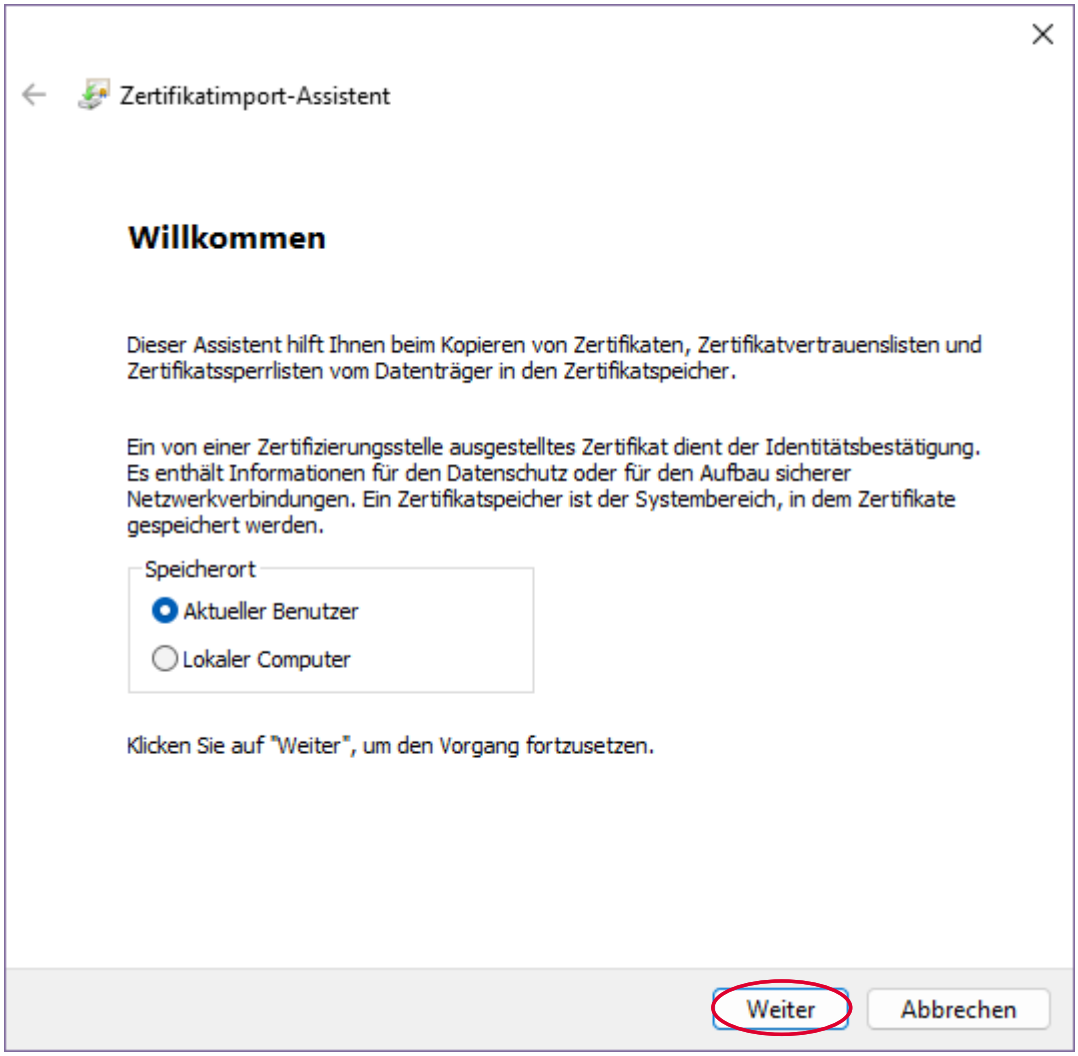


Abbildung 1: Startseite des Zertifikatimport-Assistenten

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.

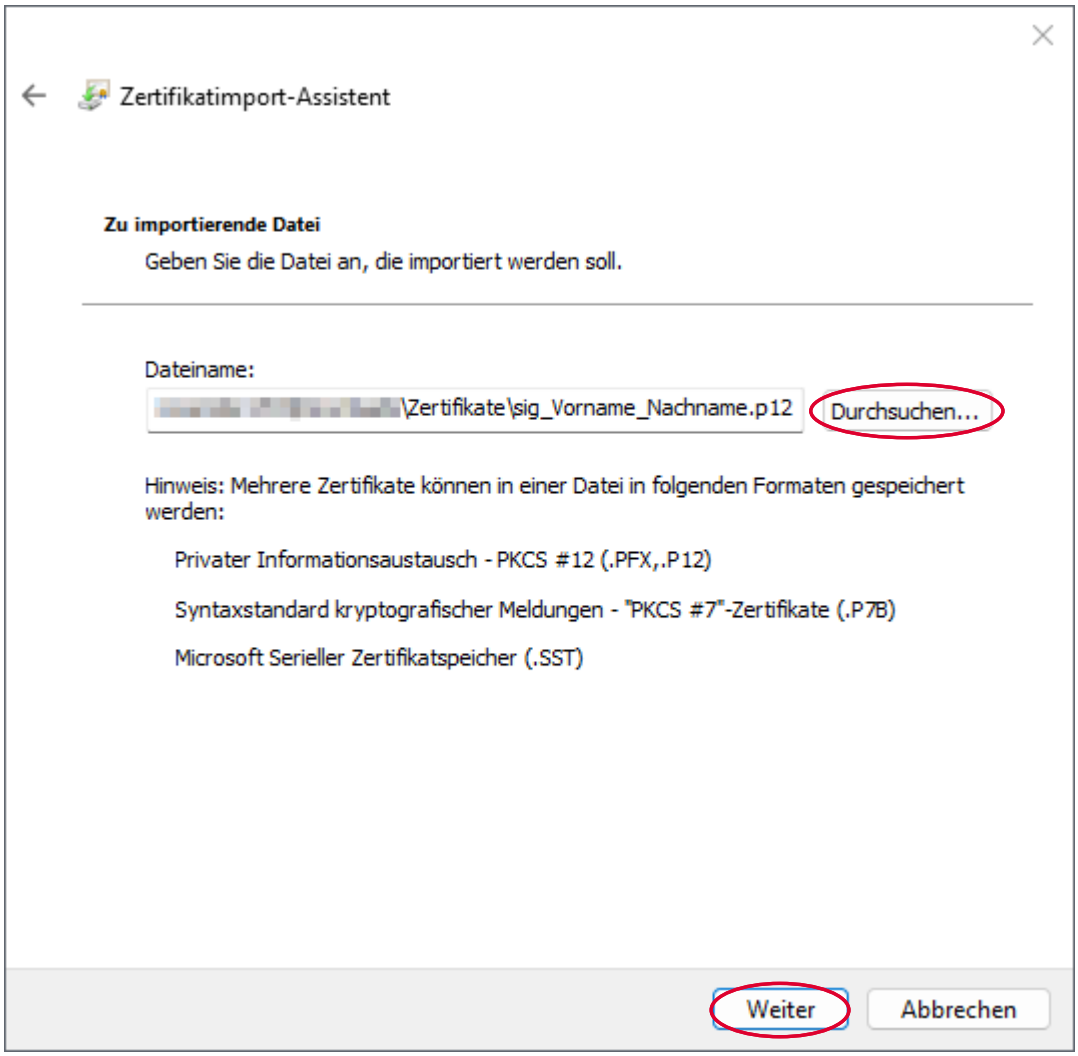


Abbildung 2: Vorausgewählte Schlüsseldatei

Nun geben Sie in das `Kennwort`-Feld 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`.

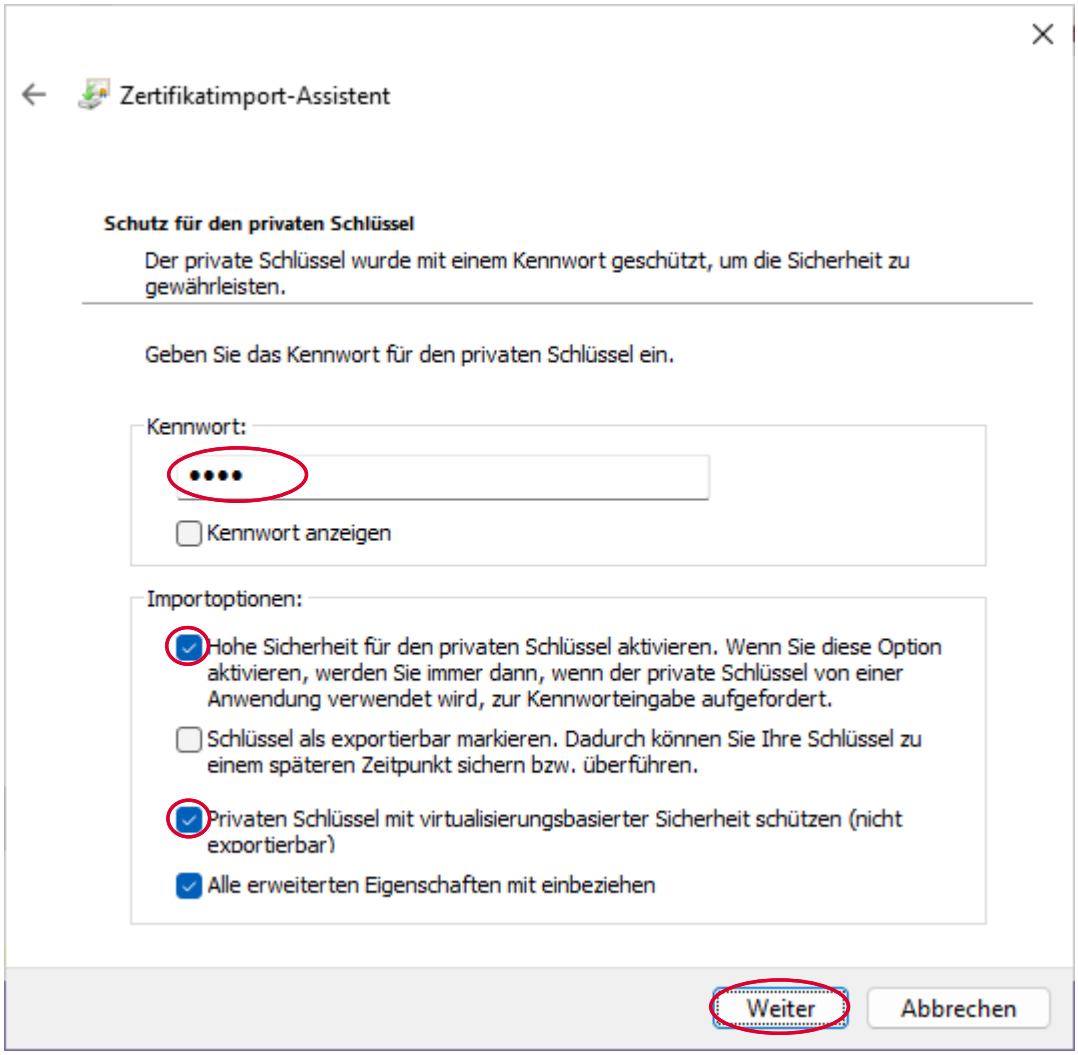


Abbildung 3: Eingabe der Transport-PIN und Auswahl der Schutzstufe

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

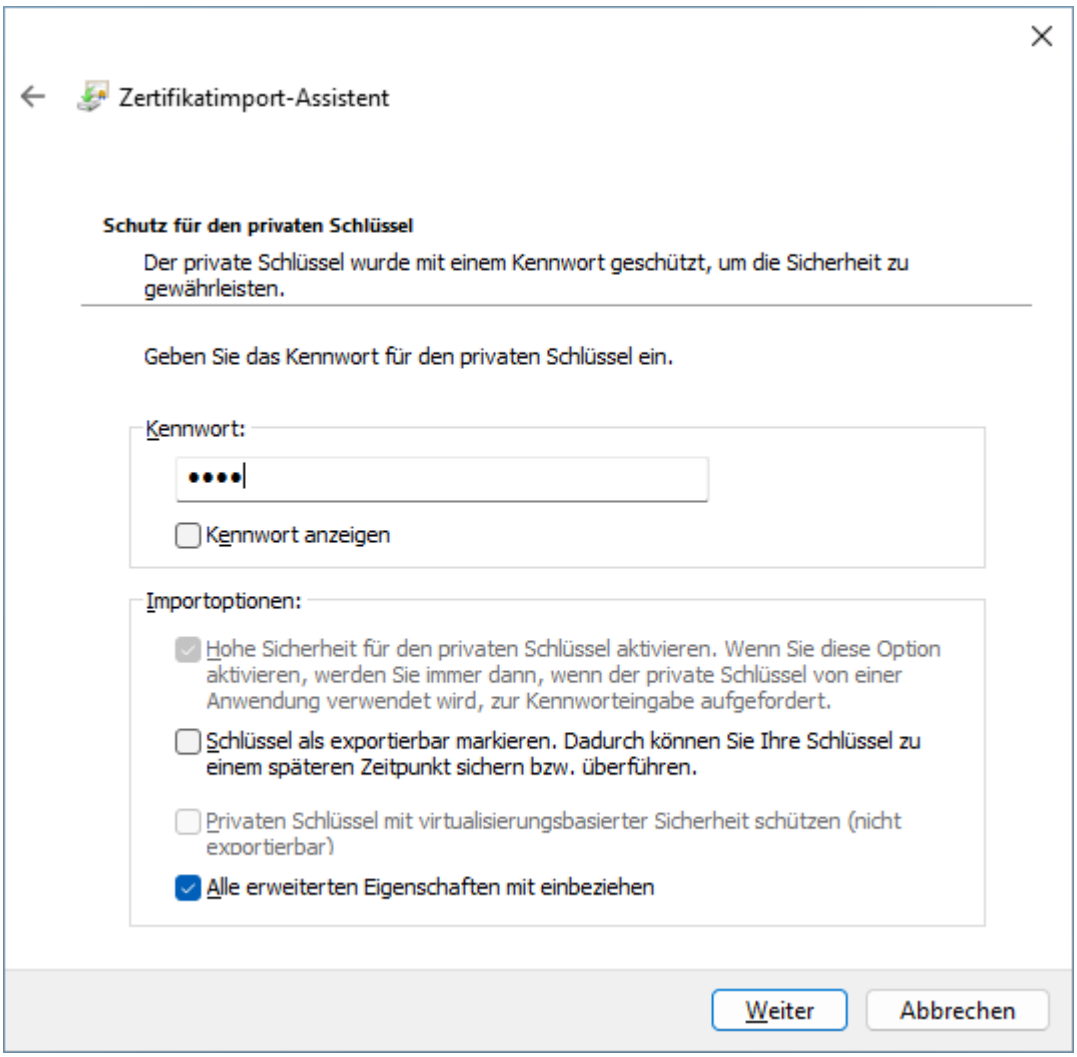


Abbildung 4: Bei Einschränkung der zulässigen Schutzstufe durch den Administrator

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

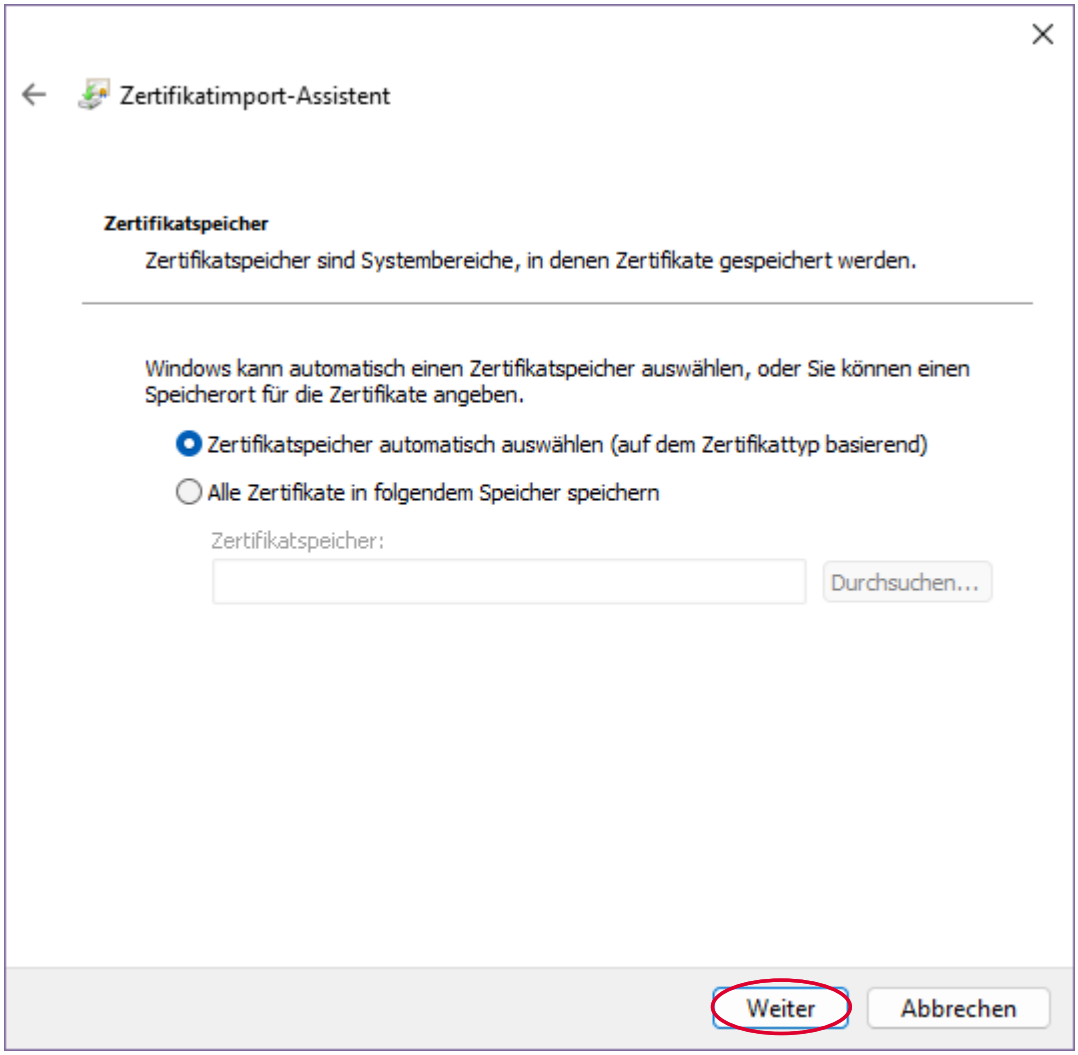


Abbildung 5: Automatische Auswahl des Zertifikatsspeichers

Klicken Sie bei der Zusammenfassung auf `Fertig stellen`.

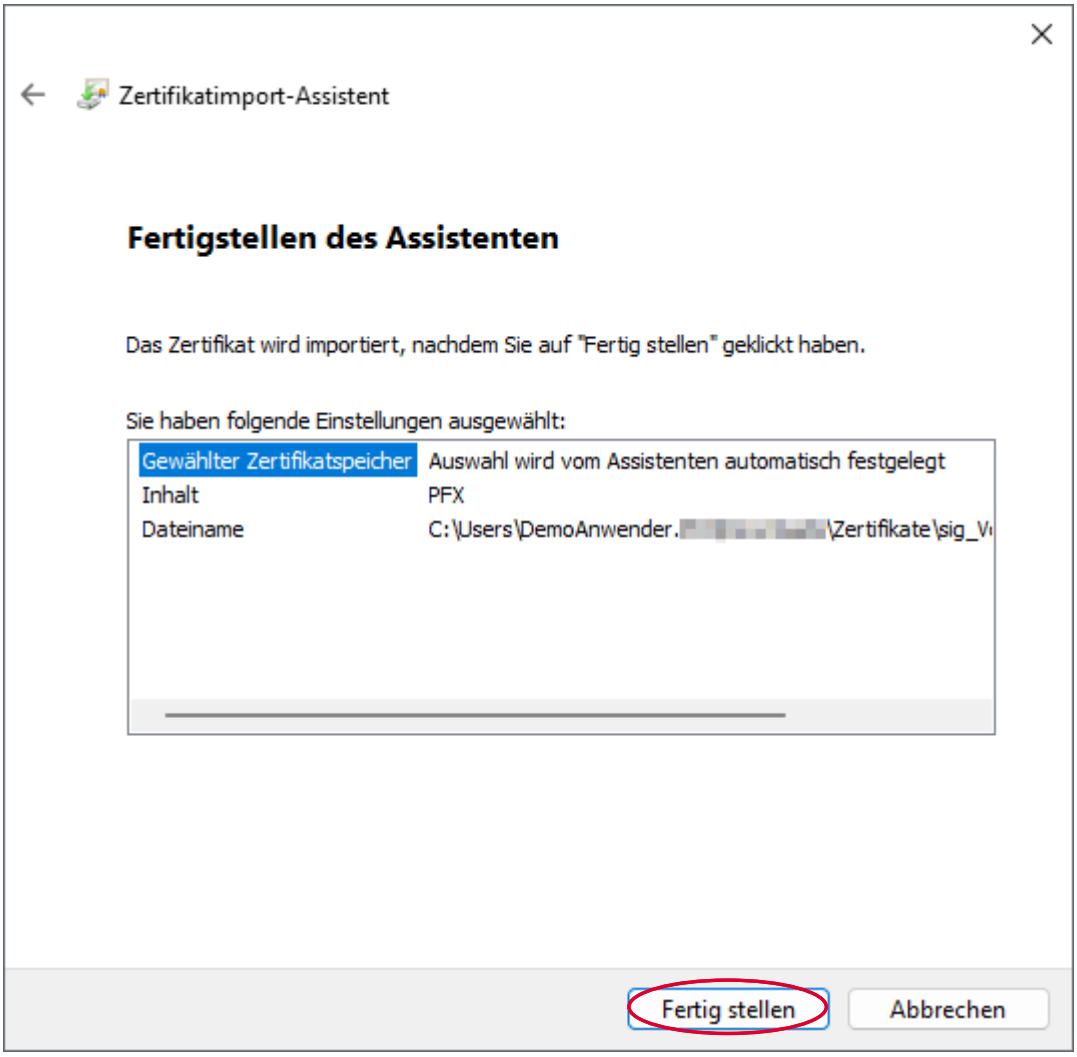


Abbildung 6: Zusammenfassung der gewählten Optionen

Im nächsten Schritt des Assistenten vergeben Sie das Passwort zum Schutz Ihres privaten Schlüssels. Stellen Sie sicher, dass das Häkchen „Kennwort mit diesem Schlüssel anfordern“ gesetzt ist. Dies sorgt auch für die Verwendung der Schutzstufe **hoch**. Geben Sie zweimal das von Ihnen gewählte Passwort ein. Klicken Sie zum Abschluss auf `OK`.

Wichtig: Dieses Passwort sollte der Passwort-Richtlinie Ihrer Organisation entsprechen. Insbesondere sollte es mindestens Groß- und Kleinbuchstaben, Sonderzeichen, und Ziffern enthalten, sowie mindestens zwölf Zeichen lang sein.

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

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

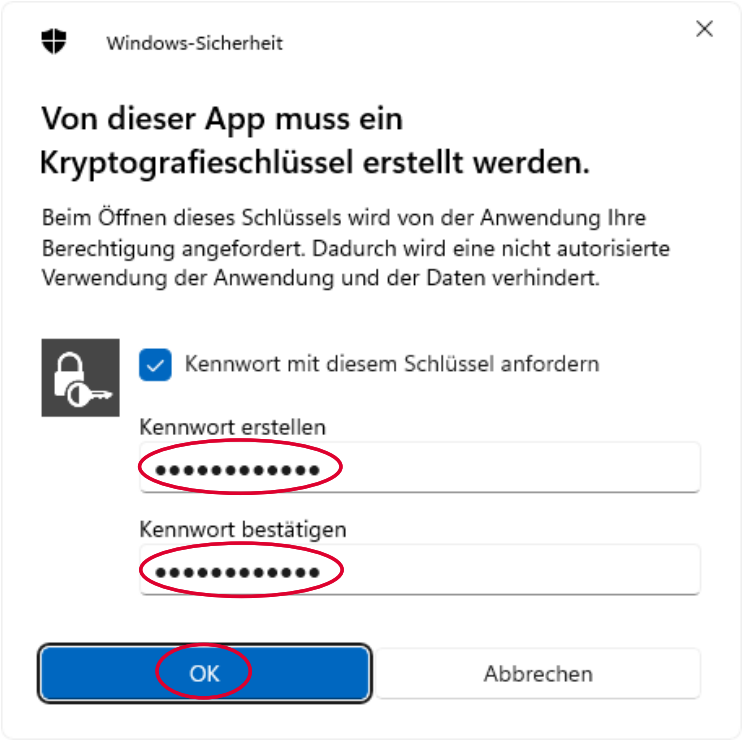


Abbildung 7: Festlegen des Passworts für die Nutzung des importierten Schlüssels

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.

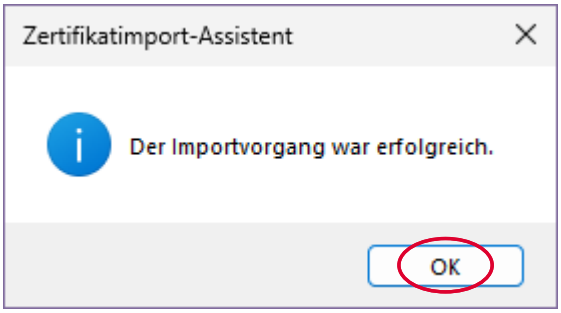


Abbildung 8: Abschluss des Zertifikatimport-Assistenten

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 2024

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.

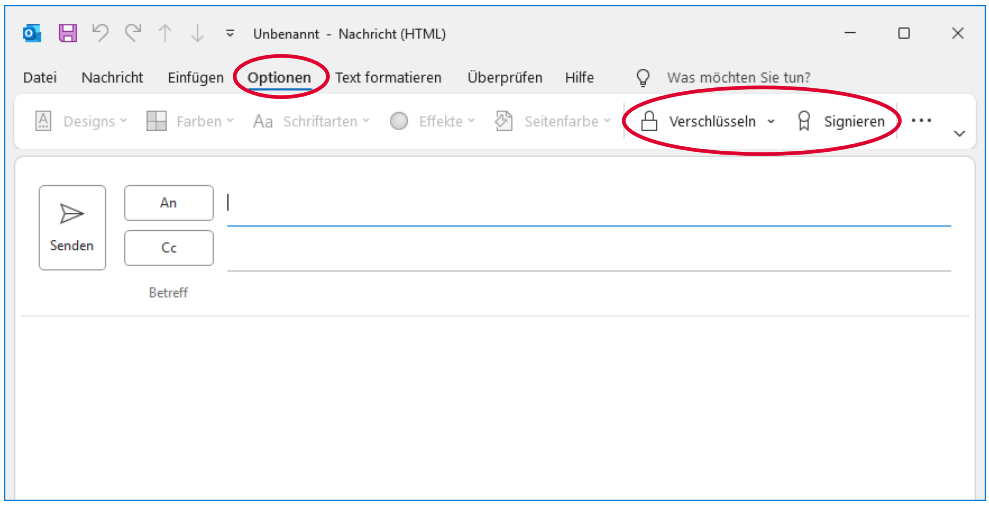


Abbildung 9: Angezeigte Optionen „Verschlüsseln“ und „Signieren“ für eine neue E-Mail bei passender Voreinstellung von Outlook durch den Administrator

Falls der Reiter „Optionen“ nicht angezeigt wird, ist ihr Fenster zum Nachrichten verfassen in das Hauptfenster eingebettet. Es liefert dann nur eine eingeschränkte Anzahl an Reitern. In diesem Fall klicken Sie zunächst auf „Ausklappen“ im oberen rechten Rand der Nachricht, siehe Abb. 9b.

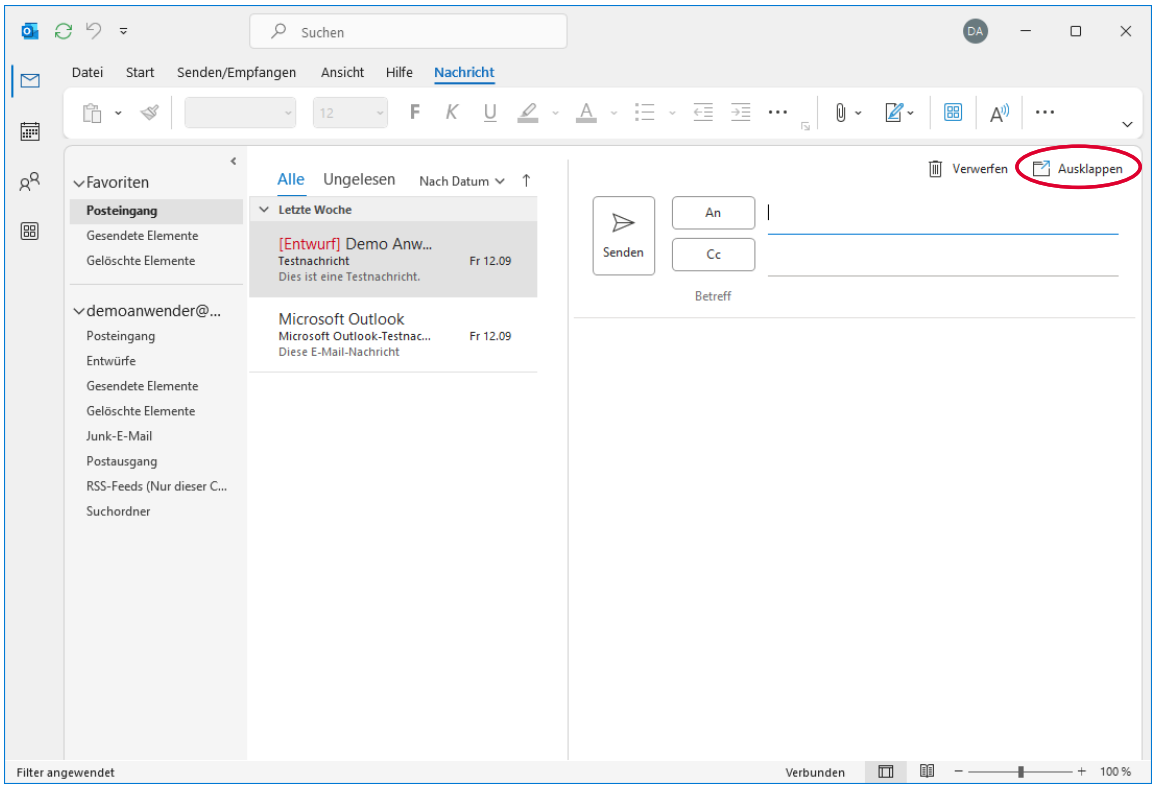
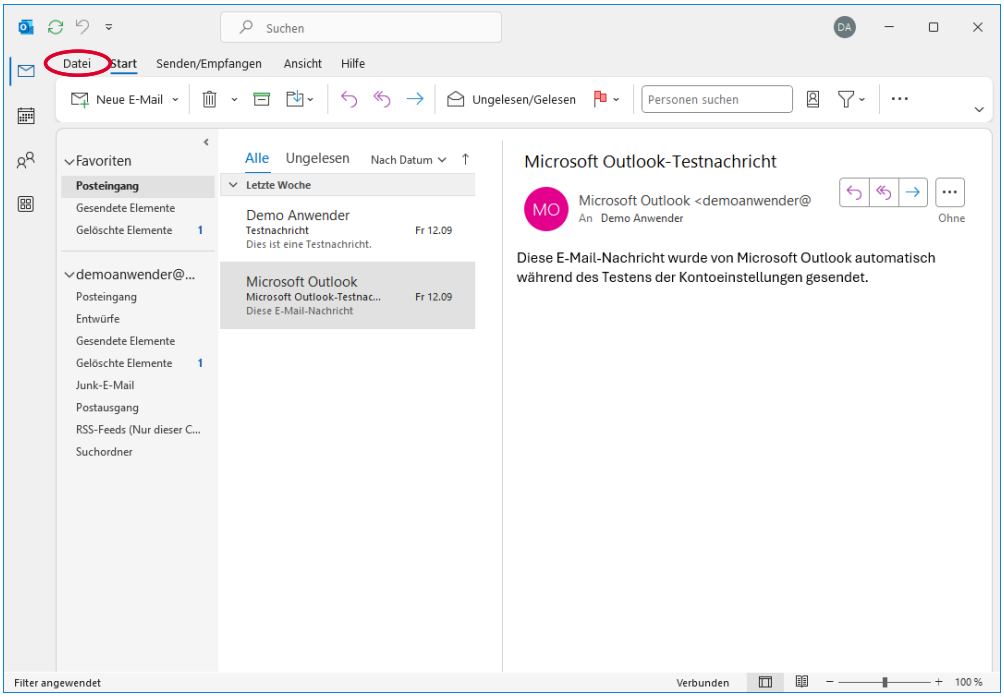


Abbildung 10b: Erstellen einer Nachricht im eingebetteten Fenster mit reduzierten Reiter-Optionen

Falls im Reiter Optionen die beiden Symbole von Abb. 9 nicht angezeigt werden, führen Sie die Schritte der nachfolgenden Anleitung durch. Klicken Sie im Hauptfenster von Outlook auf `Datei` und dann auf `Optionen`.



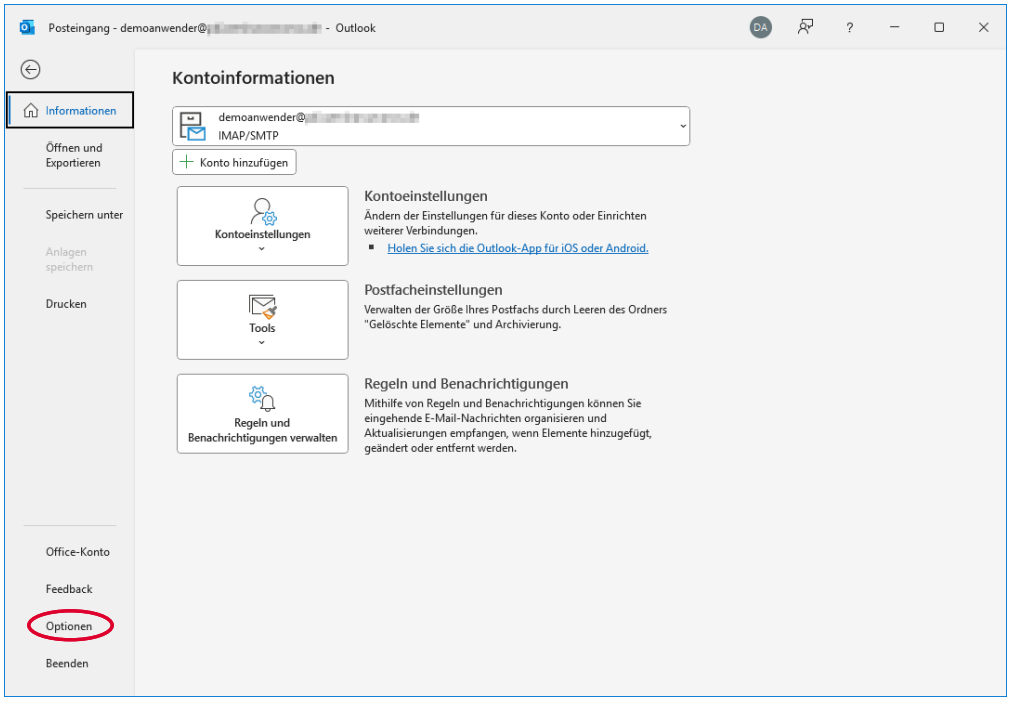


Abbildung 11: Aufruf der Outlook-Optionen

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

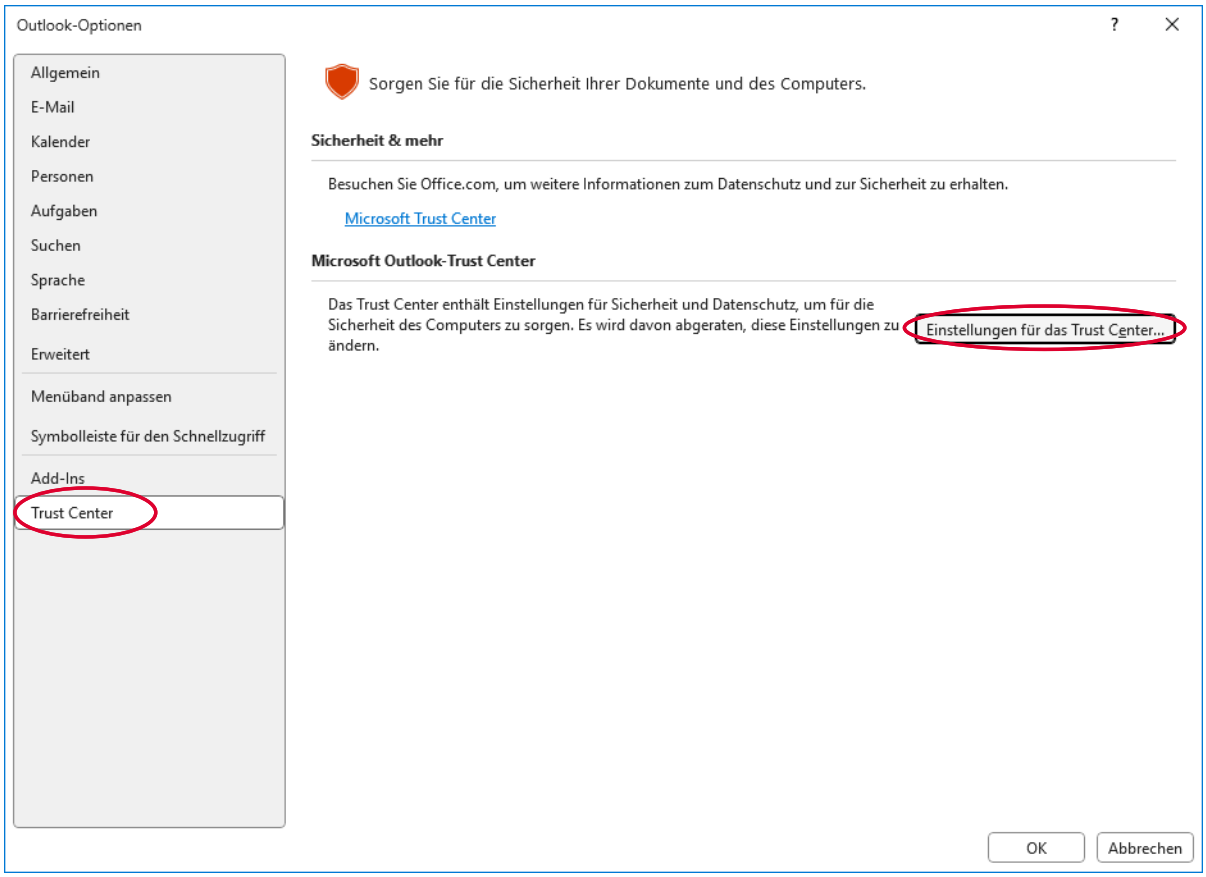


Abbildung 12: Aufruf der Trust Center-Einstellungen

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

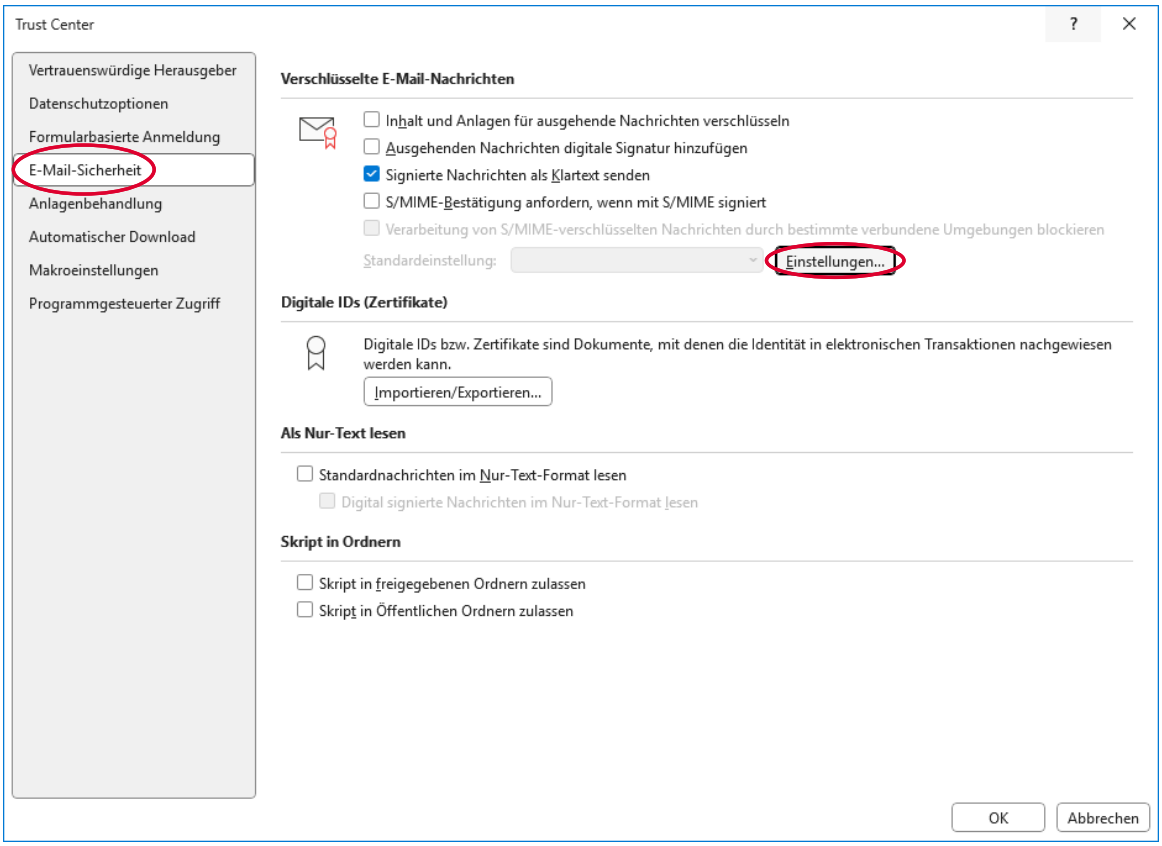


Abbildung 13: Aufruf der Einstellungen für die E-Mail-Verschlüsselung

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 Verfahren `SHA256` 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 einen Klick auf OK. Wenn Sie in der Liste Ihr Zertifikat nicht finden können, wiederholen Sie bitte den Zertifikatsimport wie in Kapitel 2.2 beschrieben. Sollte der Fehler danach immer noch auftauchen, wenden Sie sich bitte an den PKI-Support der Bayern-PKI. Die Kontaktinformationen dazu finden Sie am Ende dieses Handbuchs.

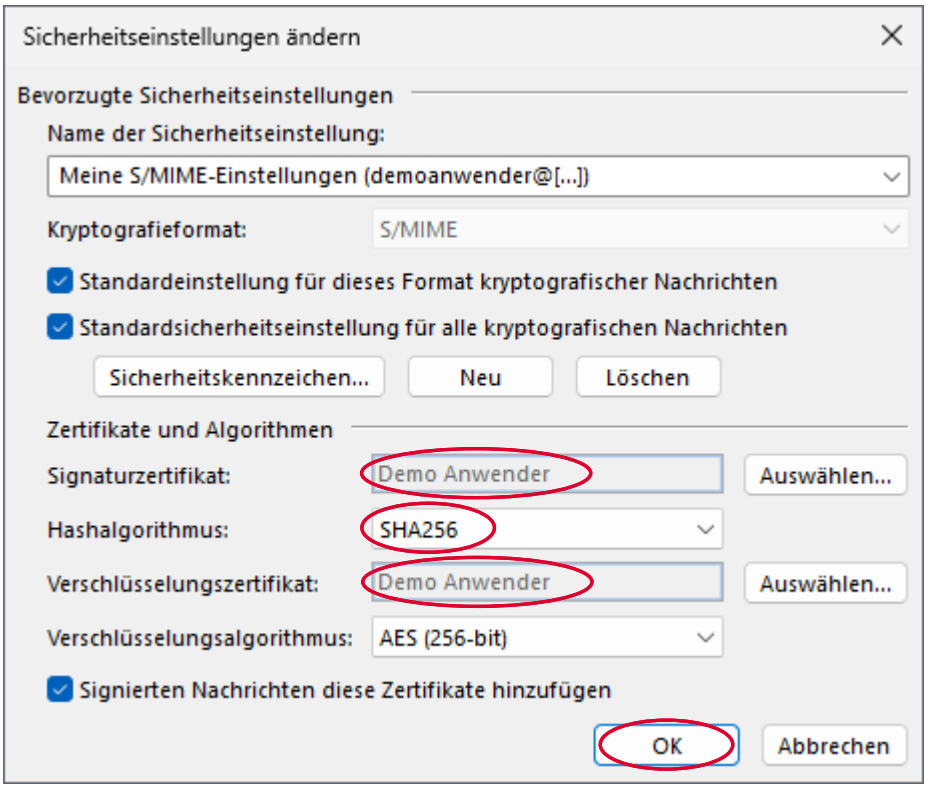


Abbildung 14: Prüfen der vorausgewählten Zertifikate und Einstellung des Hashalgorithmus

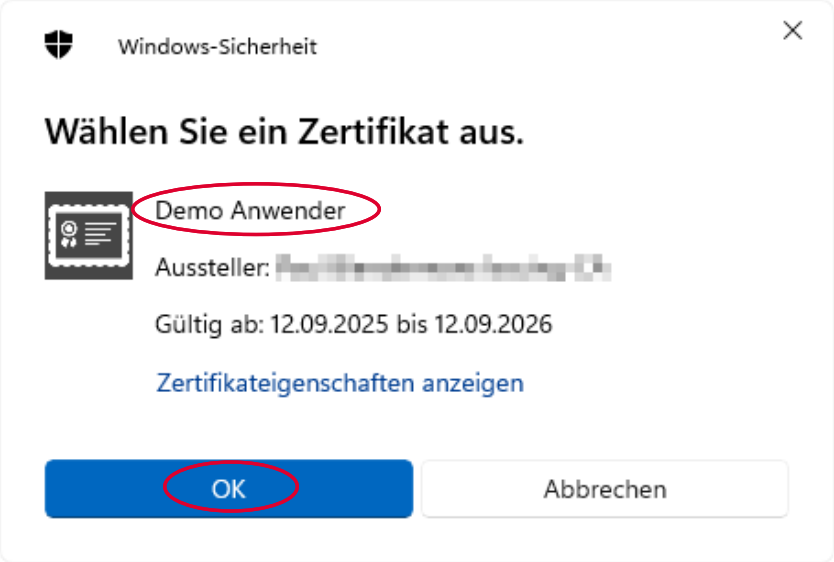


Abbildung 15: Explizite Auswahl eines Zertifikats (nur im Bedarfsfall)

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.

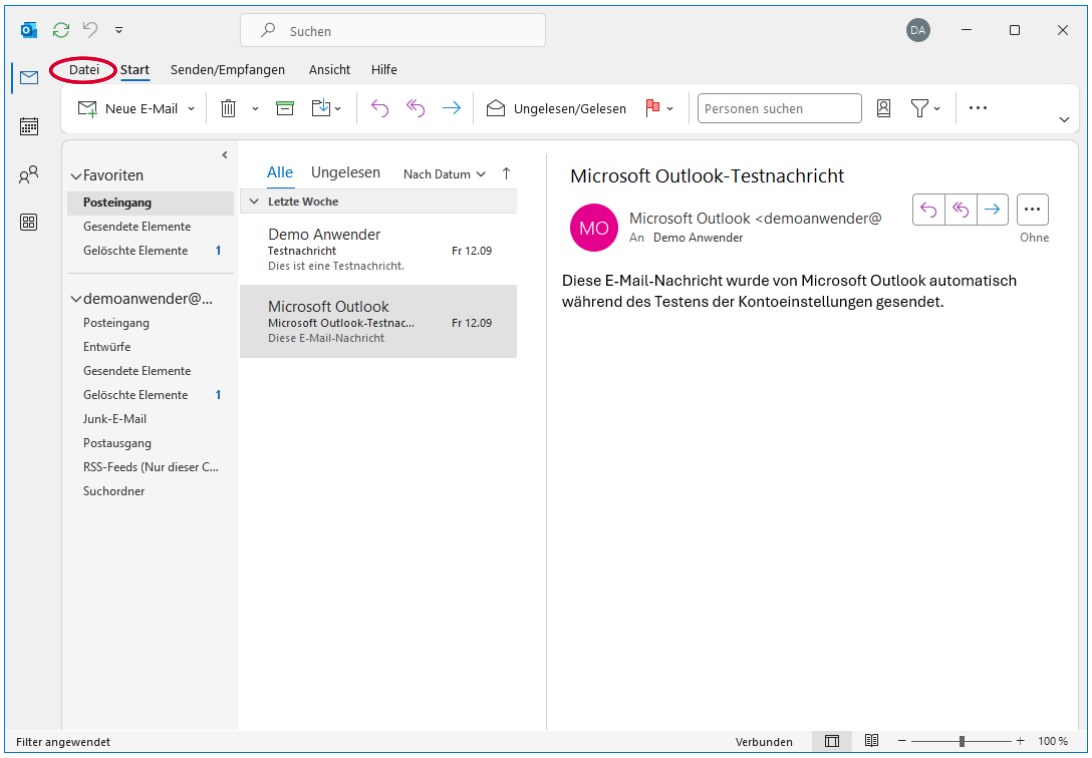
Sofern der Zertifikatsinhaber einer externen Veröffentlichung zugestimmt hat, werden die E-Mail-Zertifikate zusätzlich in einem per Internet zugänglichen externen LDAP-Verzeichnisdienst veröffentlicht.

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. 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. lediglich zeitweise 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`….



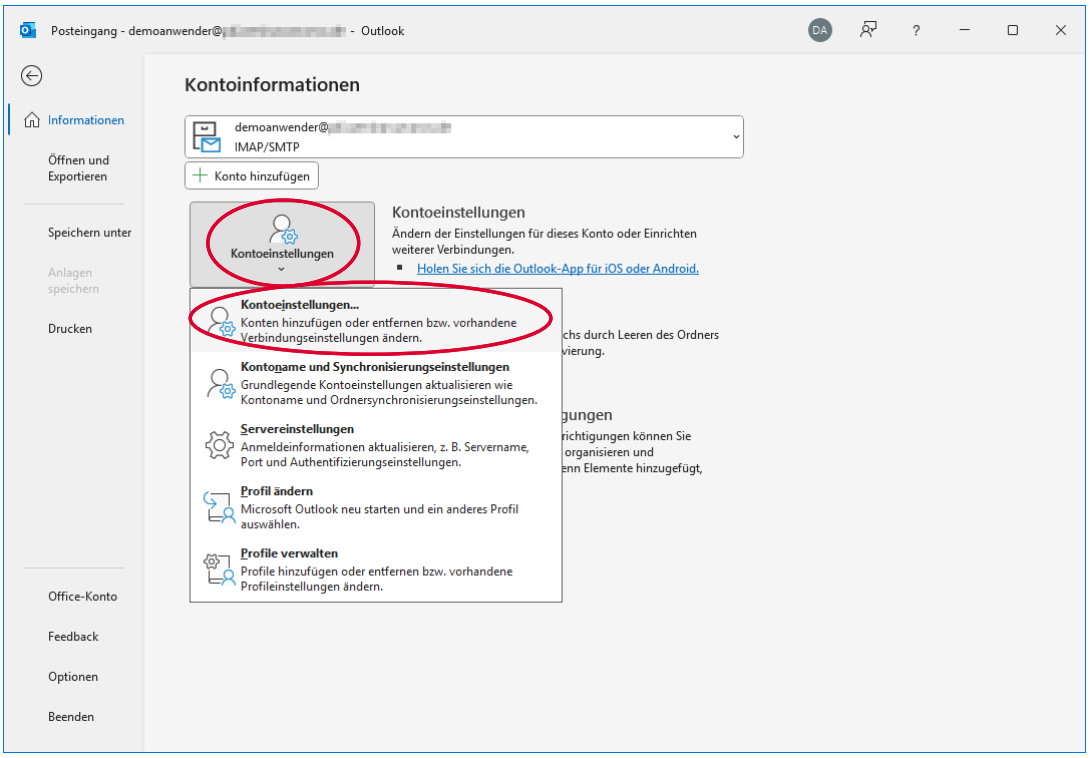


Abbildung 16: Aufruf der Kontoeinstellungen in Outlook

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

Hinweis: Möglicherweise hat Ihr Administrator bereits die LDAP-Verbindung zum 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 26), dann können Sie die restlichen Schritte in diesem Kapitel überspringen.

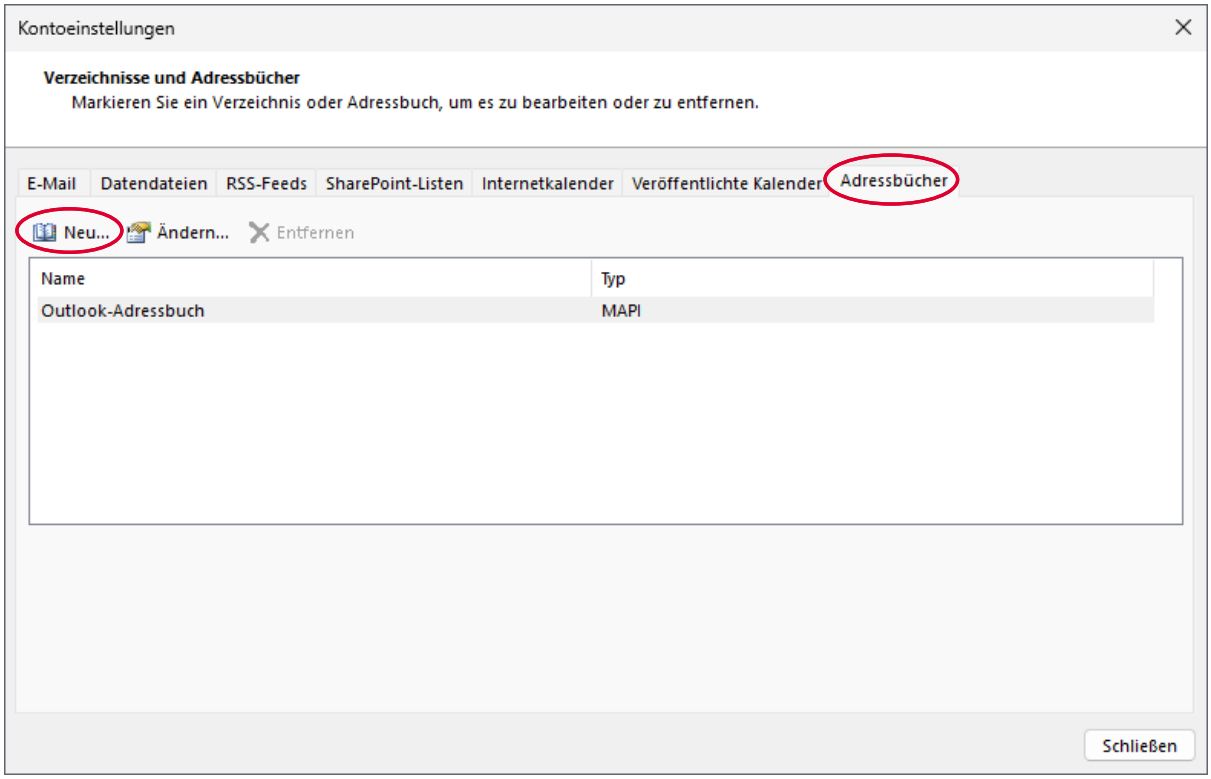


Abbildung 17: Hinzufügen einer Verbindung zum LDAP-Server als Outlook-Adressbuch

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

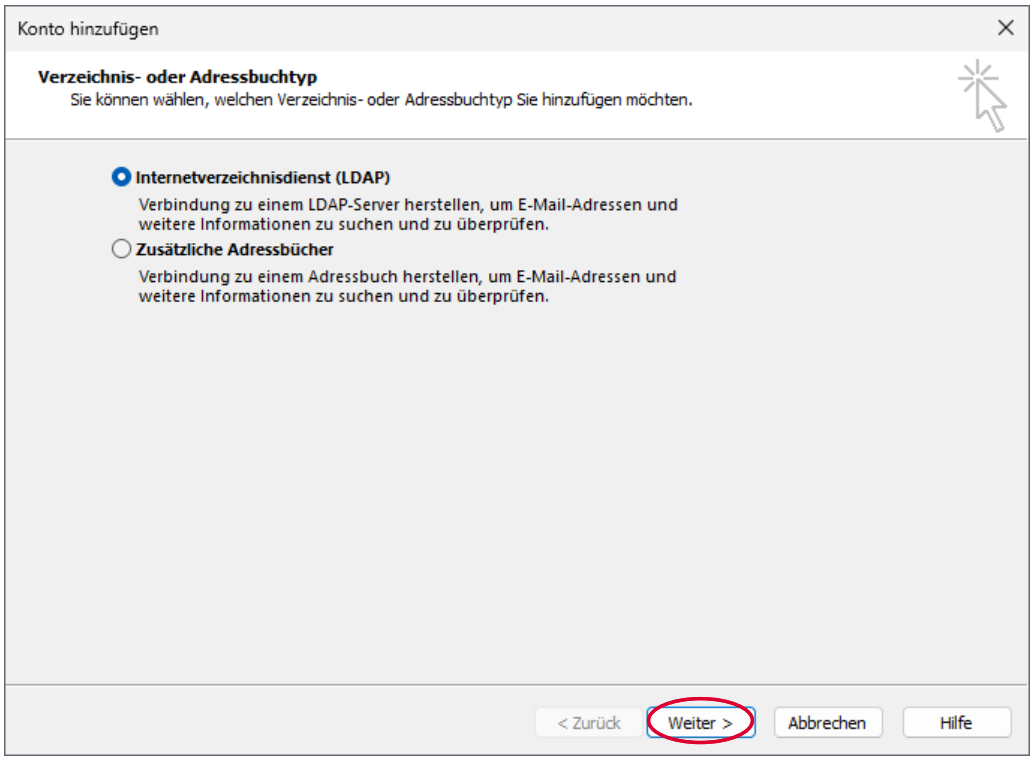


Abbildung 18: Auswahl von LDAP als Schnittstelle zum Verzeichnisdienst

Geben Sie im Feld `Servername` die Adresse `directory.bybn.de`, bzw. für den externen Verzeichnisdienst die Adresse `directory.bayern.de` ein. Die Option `Server erfordert Anmeldung` bleibt deaktiviert. Klicken Sie dann auf `Weitere Einstellungen…`.

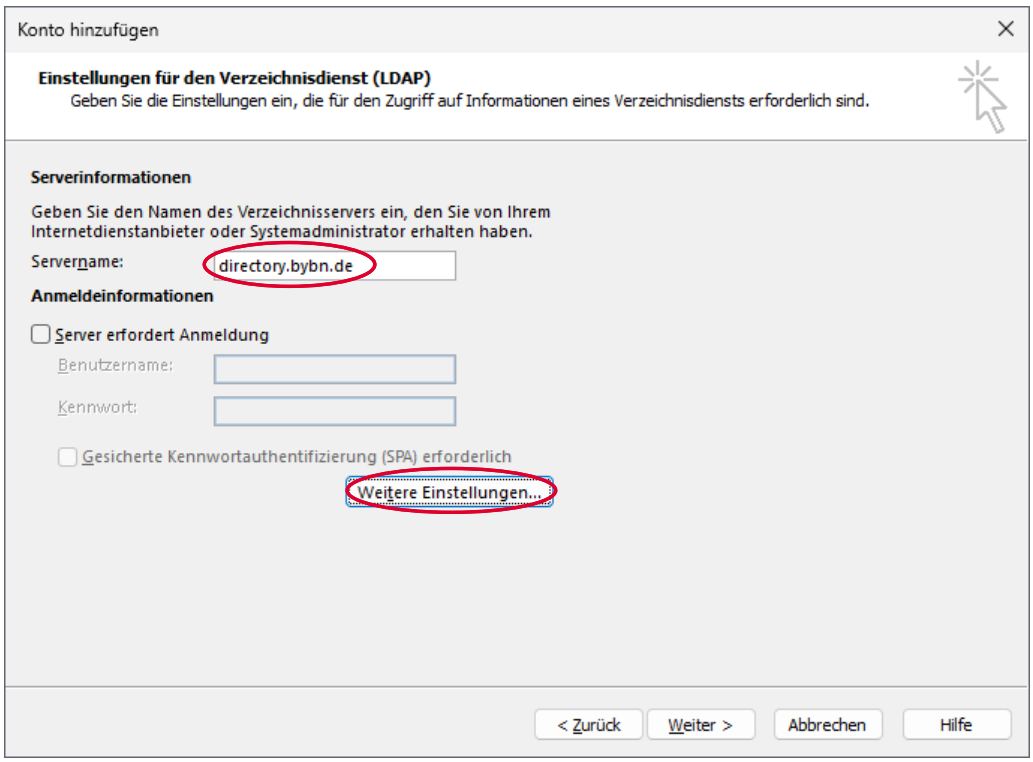


Abbildung 19: Einstellen des Servernamens

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 mit `OK`.

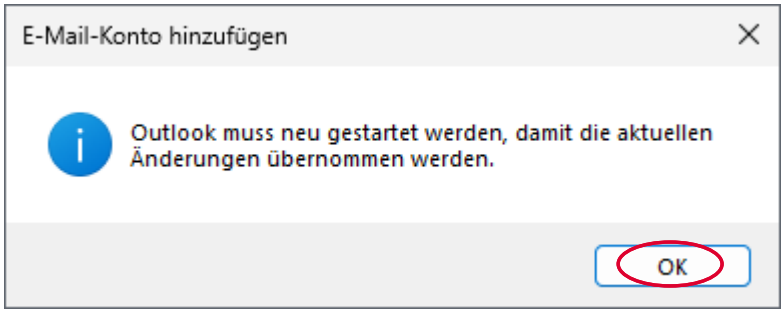


Abbildung 20: Hinweis auf den erforderlichen Neustart von Outlook

Für einen Abruf des Verzeichnisdienstes gibt es zwei Optionen mit unterschiedlicher Sicherheit, vergleichbar mit einem Abruf einer Internetseite über a) HTTPS oder b) HTTP. Es ist aus Sicherheitsgesichtspunkten gut, im Reiter `Verbindung` die Option „Secure Sockets Layer verwenden“ zu aktivieren (vergleichbar mit HTTPS), und bei Anschluss die Portnummer „636“ einzutragen, siehe Abb. 20a. (Die Änderung der Portnummer passiert automatisch, wenn Sie später das Fenster mit OK schließen.)

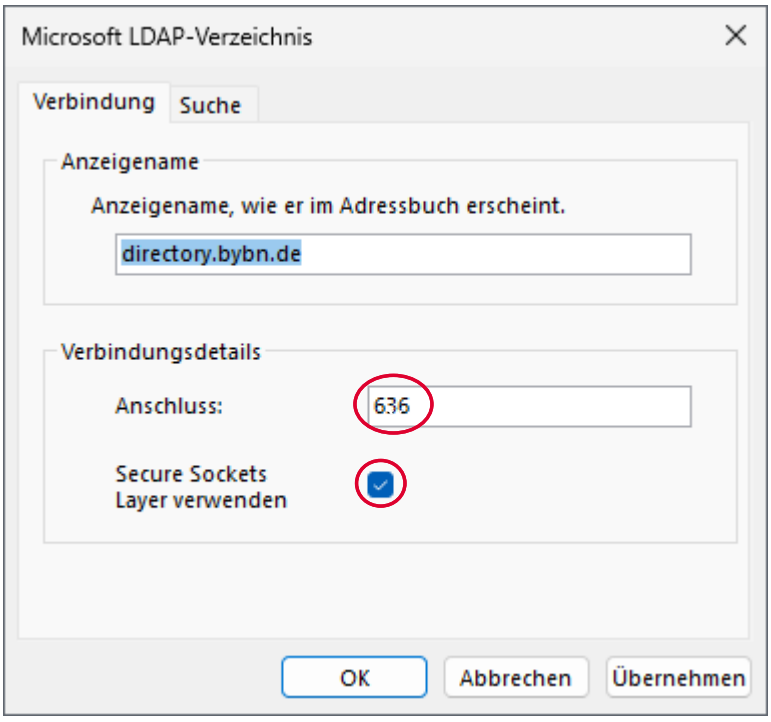


Abbildung 21a: Aktivieren der sicheren Verbindung zum LDAP-Dienst

Da die Unterstützung noch nicht in allen Systemen vollständig ist, kann es jedoch zu Problemen beim Abruf des Verzeichnis-Diensts kommen. In diesem Fall schalten Sie die Option wieder ab – diese Option ist vergleichbar mit einem Website-Abruf über HTTP. Tragen Sie dann bei Anschluss die Portnummer auf „389“ ein, siehe Abb. 20b.

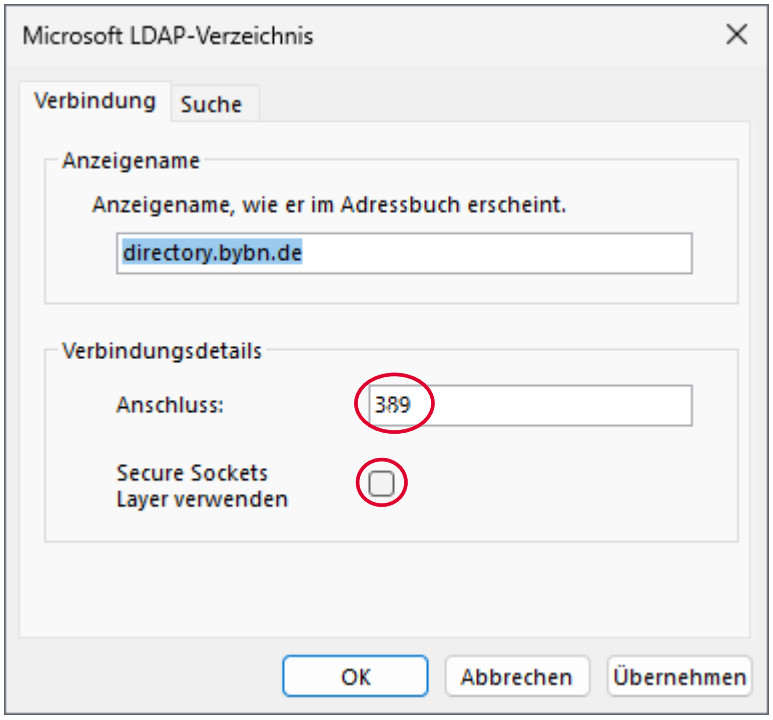


Abbildung 22b: Aktivieren der gewöhnlichen Verbindung zum LDAP-Dienst

In diesen weiteren Einstellungen klicken Sie nun auf den Reiter `Suche`. Wählen Sie als `Suchbasis` den Eintrag `Benutzerdefiniert` aus und geben Sie als Wert für diese

`OU=pki-teilnehmer,DC=pki,DC=bybn,DC=de`

ein, bzw. für den externen Dienst den Wert

`OU=pki-teilnehmer,DC=pki,DC=bayern,DC=de`.

Schließen Sie das Einstellungsfenster mit `OK`.

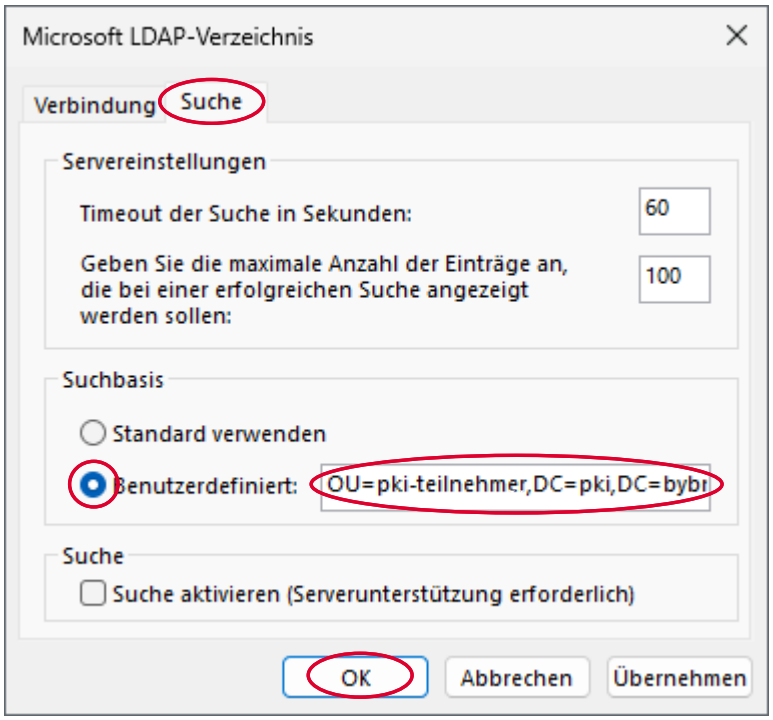


Abbildung 23c: Einstellung der Suchbasis

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

Hinweis: Nach dem Klick auf `Weiter >` wird u. U. die 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.

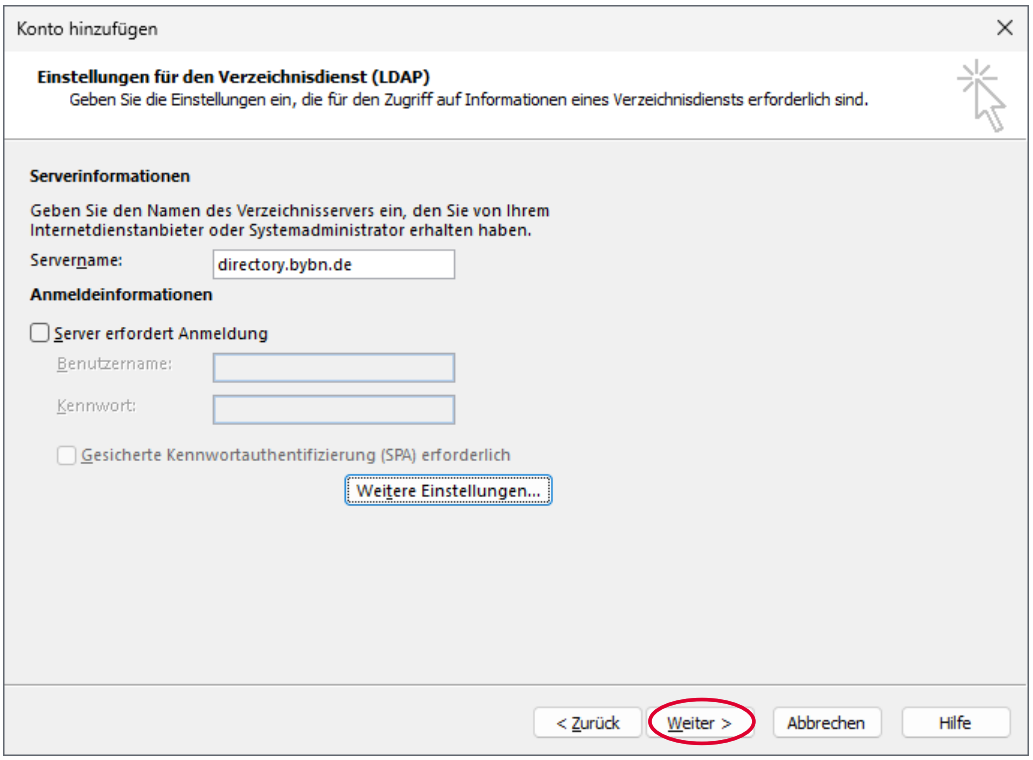


Abbildung 24: Fortsetzen des Assistenten zum Hinzufügen eines Adressbuchs

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`.

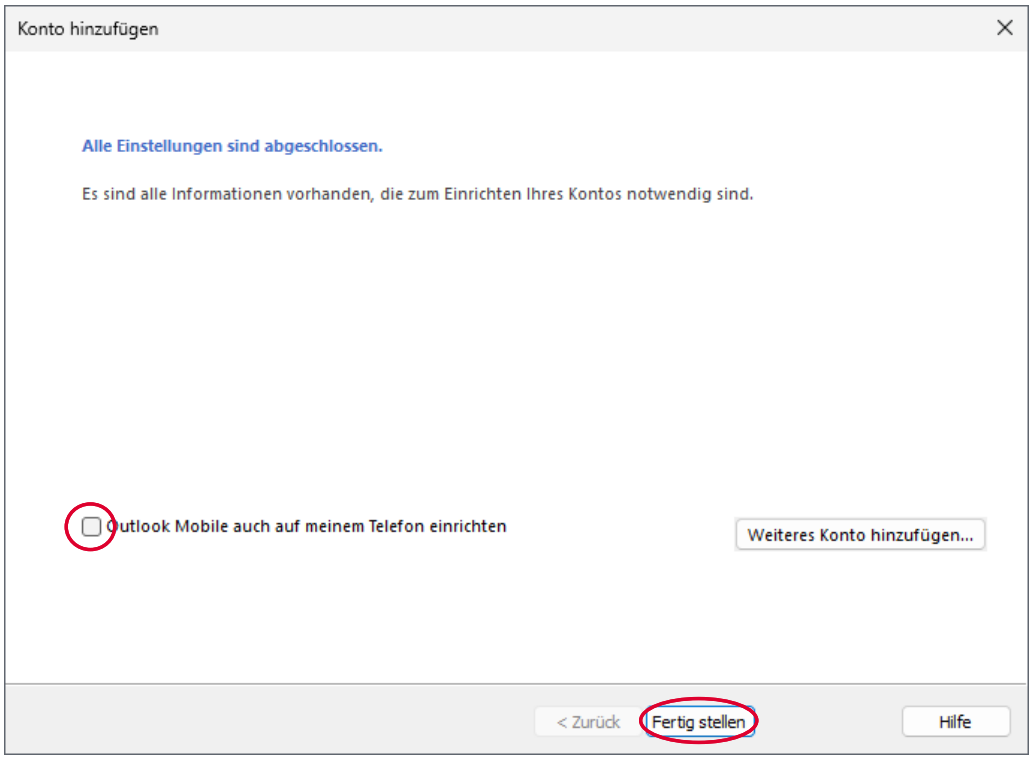


Abbildung 25: Rückmeldung des Assistenten zum Hinzufügen eines Adressbuchs

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

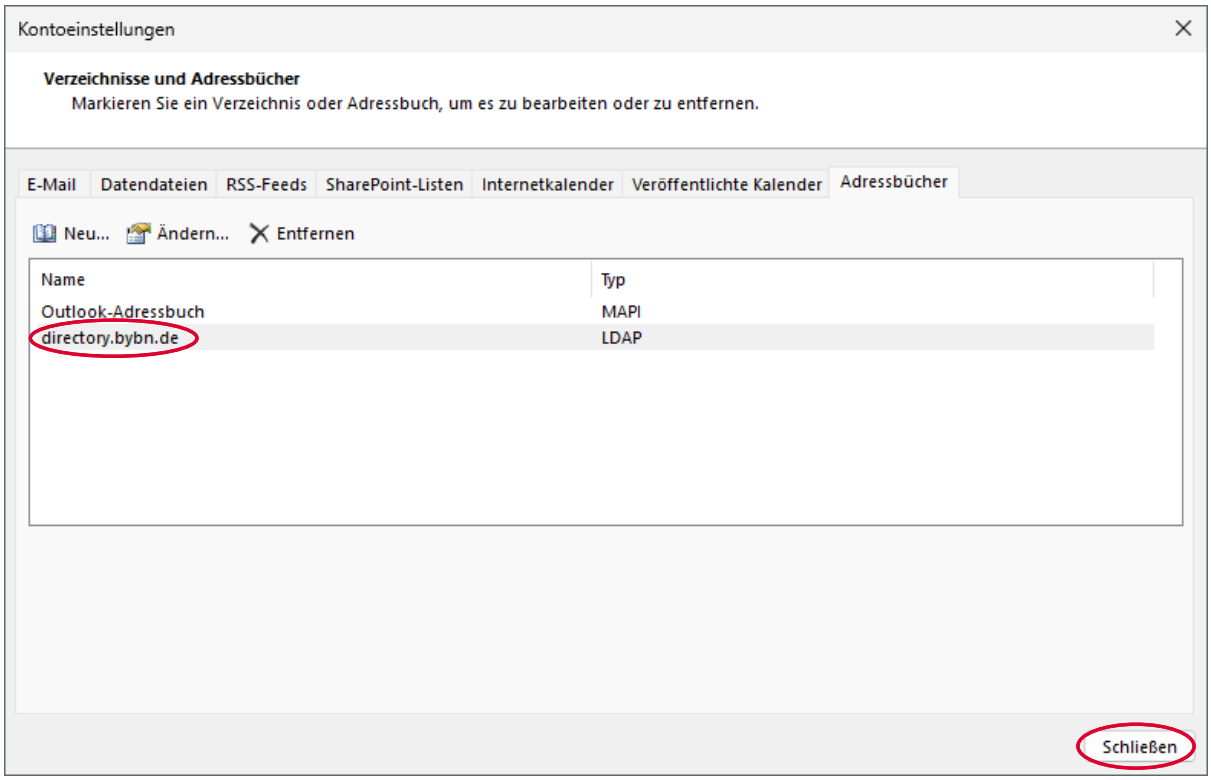


Abbildung 26: Neue LDAP-Verbindung in der Liste der Adressbücher

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 Bayern-PKI vertraut, ist auch ein Austausch verschlüsselter und/oder signierter 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 für jeden Empfänger der E-Mail (egal ob im An-, Cc- oder Bcc-Feld) hat. Umgekehrt können Absender Ihnen nur dann eine verschlüsselte E-Mail senden, wenn diese 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. Falls der Reiter „Optionen“ nicht verfügbar ist, verfahren Sie wie bei Abb. 9b.

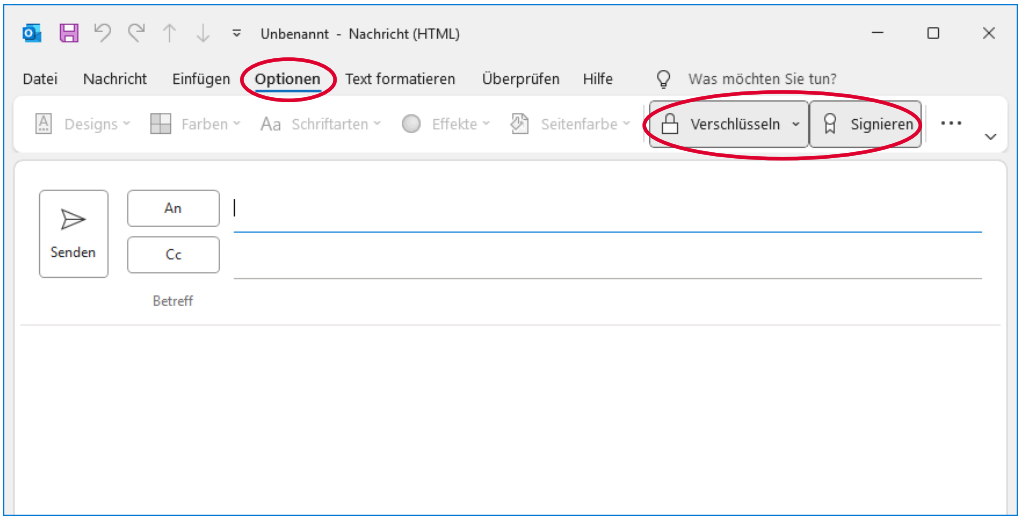


Abbildung 27: Aktivierung der Optionen „Verschlüsseln“ und/oder „Signieren“

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`.

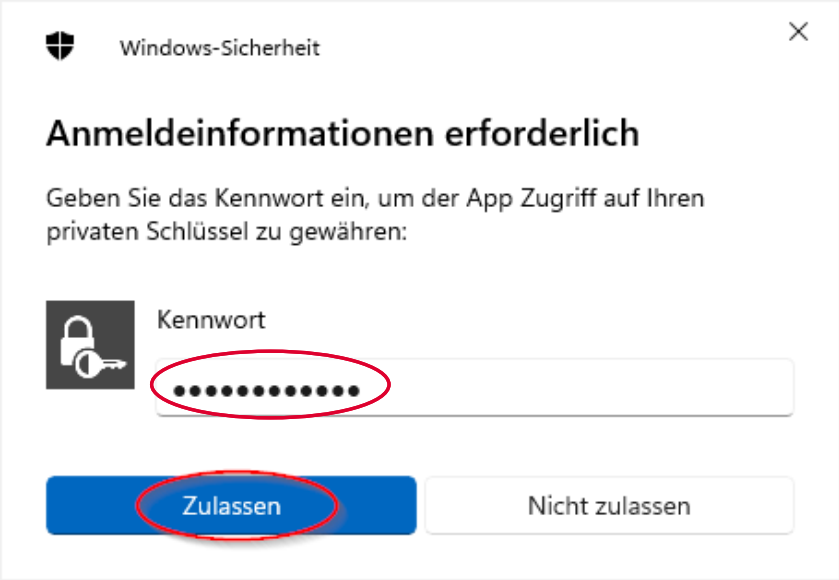


Abbildung 28: Passworteingabe für die Nutzung Ihres privaten Schlüssels beim Versand einer signierten E-Mail

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 in diesem Fall 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.

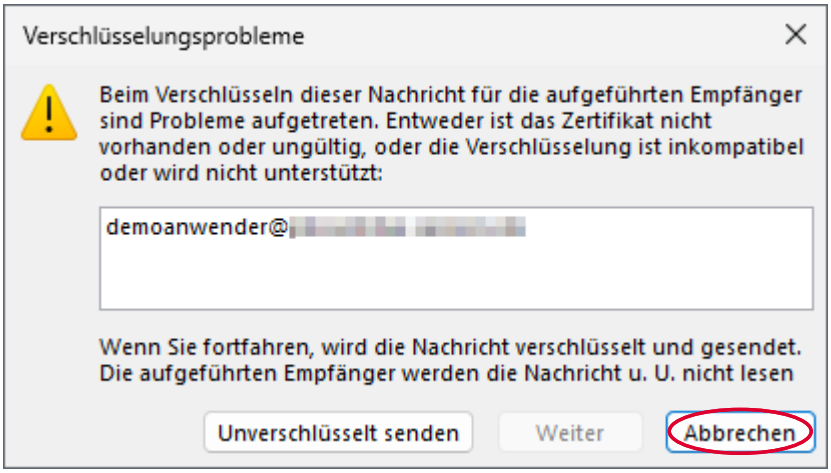


Abbildung 29: Fehlermeldung, falls nicht für alle Empfänger Verschlüsselungszertifikate vorliegen

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

abgelegt. Beim Lesen selbst gesendeter verschlüsselter E-Mails gilt daher 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 diese Funktionsadresse von der Bayern-PKI beziehen und wie in Kapitel 2 beschrieben in Ihren Windows-Zertifikats- und Schlüsselspeicher importieren.

Outlook wählt dann automatisch an Hand 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; falls Sie die Antwort nicht verschlüsseln oder signieren möchten, müssen Sie diese Einstellungen im Reiter Optionen 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 29), 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 allen 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.

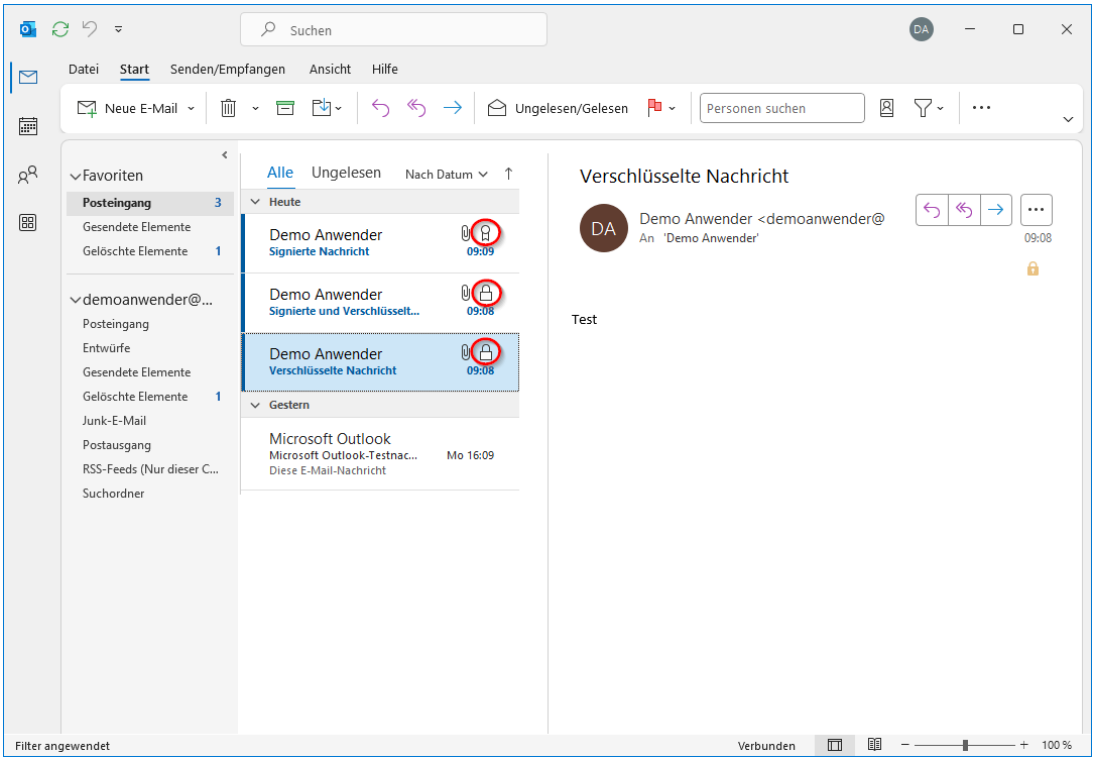


Abbildung 30: Symbole zur Anzeige verschlüsselter bzw. signierter E-Mails in der Postfachansicht. Das Siegel-Symbol zeigt eine vorhandene, gültige E-Mail-Signatur (einer ansonsten unverschlüsselten Nachricht), das Schloss-Symbol eine verschlüsselte Nachricht

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`.

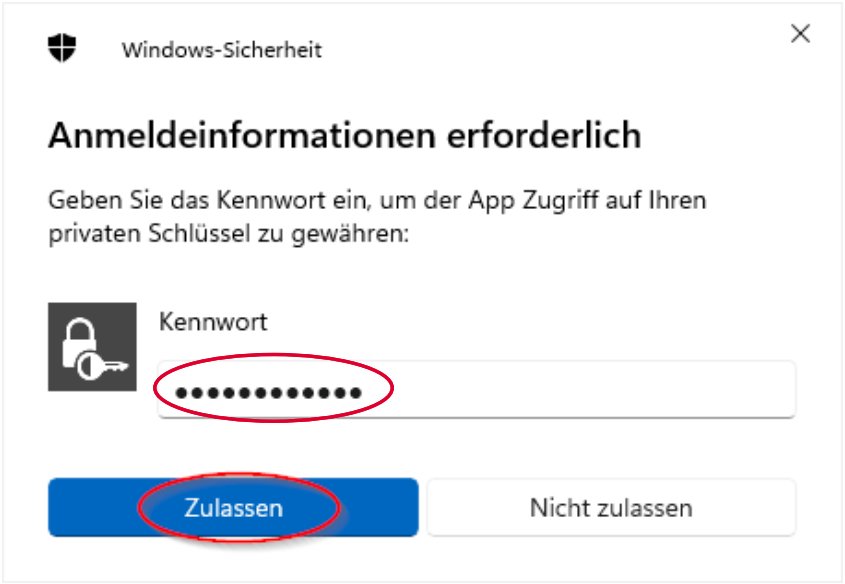


Abbildung 31: Passworteingabe für die Nutzung Ihres privaten Schlüssels zum Lesen einer verschlüsselten E-Mail

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 32: Symbole zur Anzeige verschlüsselter bzw. signierter E-Mails in der geöffneten E-Mail

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: trustcenter@ldbv.bayern.de