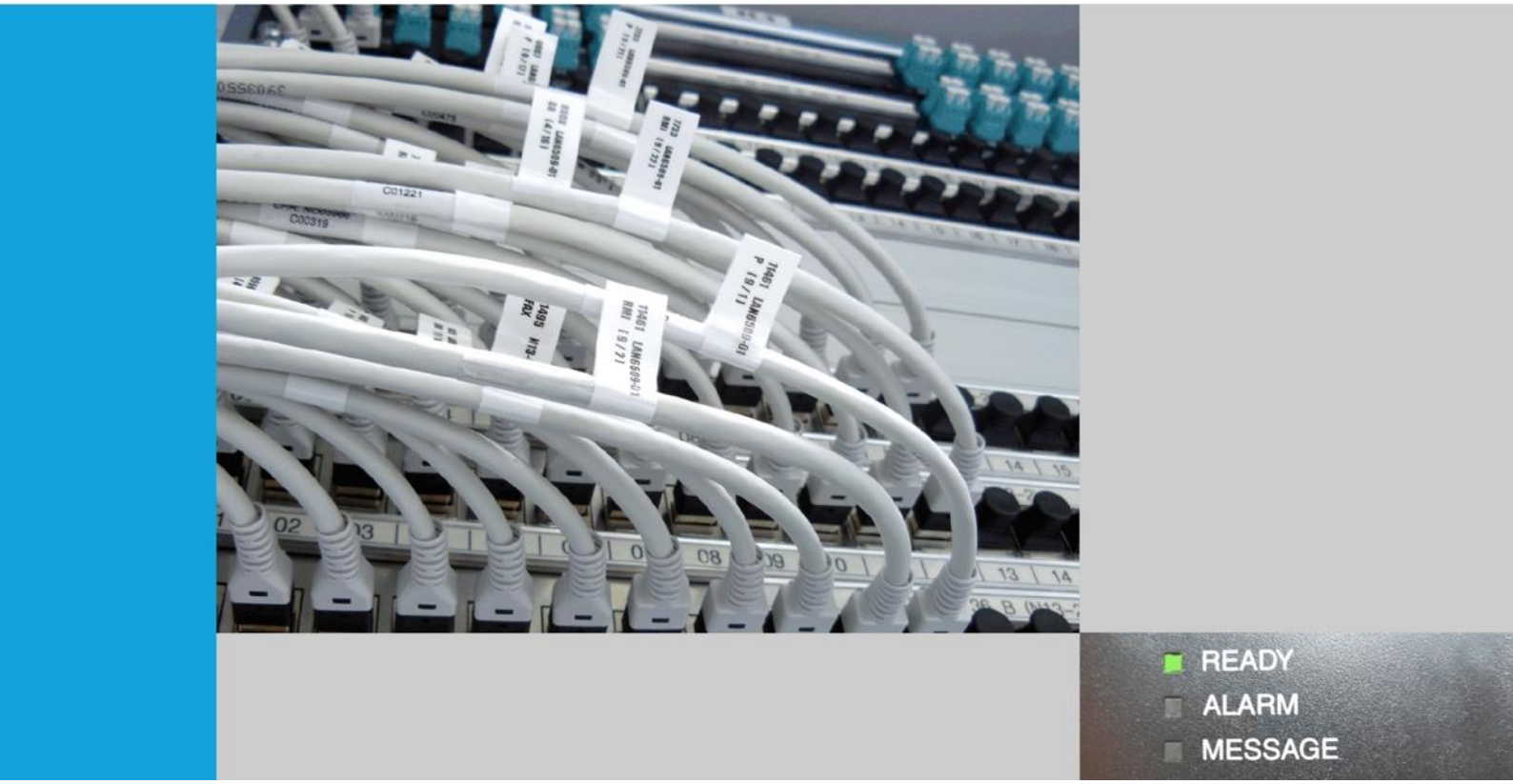
Landesamt für Digitalisierung,
Breitband und Vermessung

IT-Dienstleistungszentrum des Freistaats Bayern



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

Outlook 2016/2019 unter macOS

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 2016/2019 unter macOS 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 macOS
3. Einstellung von Outlook 2016 bzw. 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. unter Dokumente, 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 macOS

2.1 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 neuen Schlüsselbund 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`.

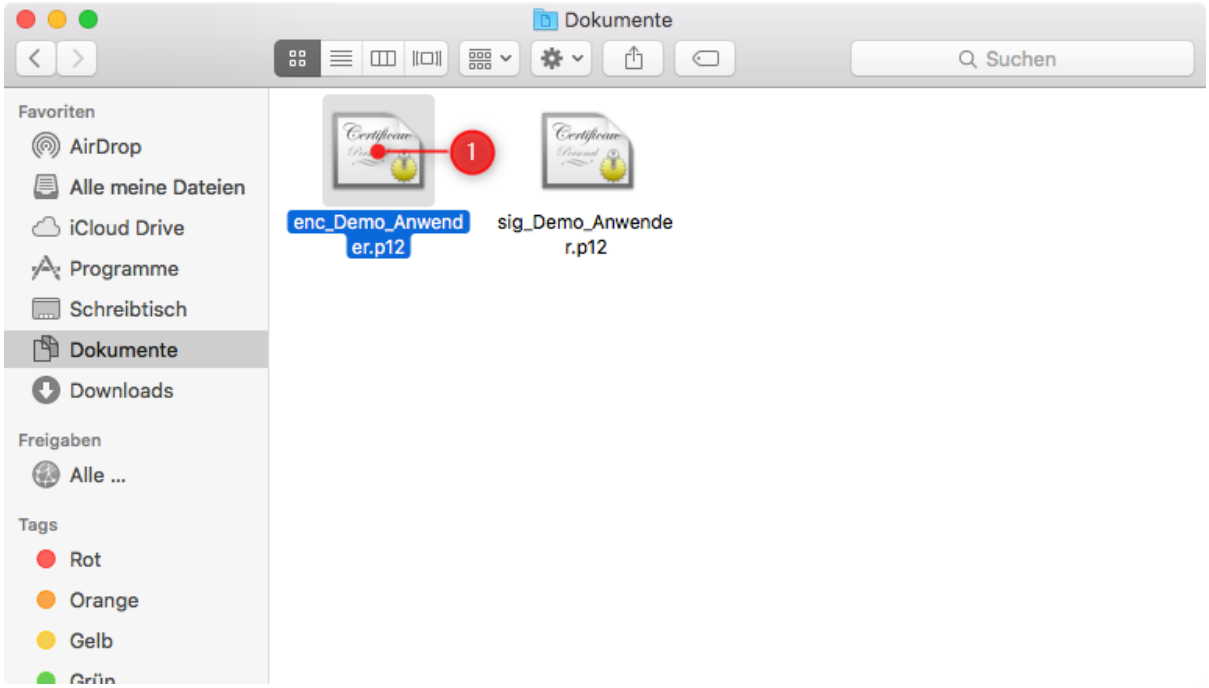


Abbildung 1: Zertifikatsdateien im Finder

Stellen Sie sicher, dass Ihr Schlüsselbund `Anmeldung` ausgewählt ist und passen Sie die Auswahl ggf. an. Bestätigen Sie den Dialog mit `Hinzufügen`.

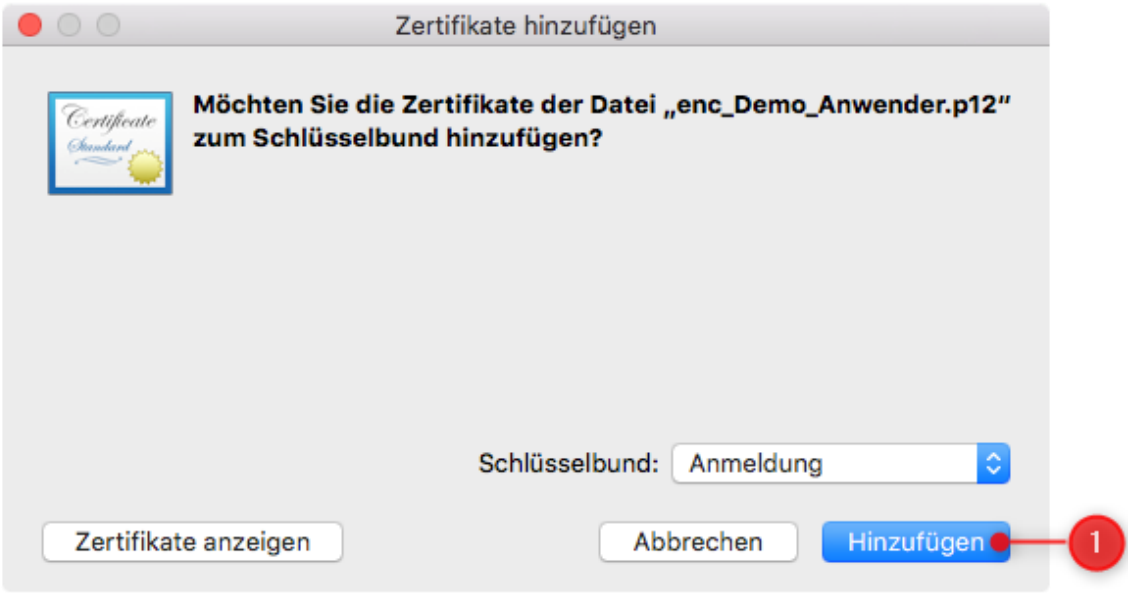


Abbildung 2 Zertifikate zum Schlüsselbund hinzufügen

Nun geben Sie als `Passwort` die Transport-PIN zu Ihrer Schlüsseldatei ein. Klicken Sie dann auf `OK` und führen Sie die gleichen Schritte anschließend mit Ihrer zweiten Schlüsseldatei durch.

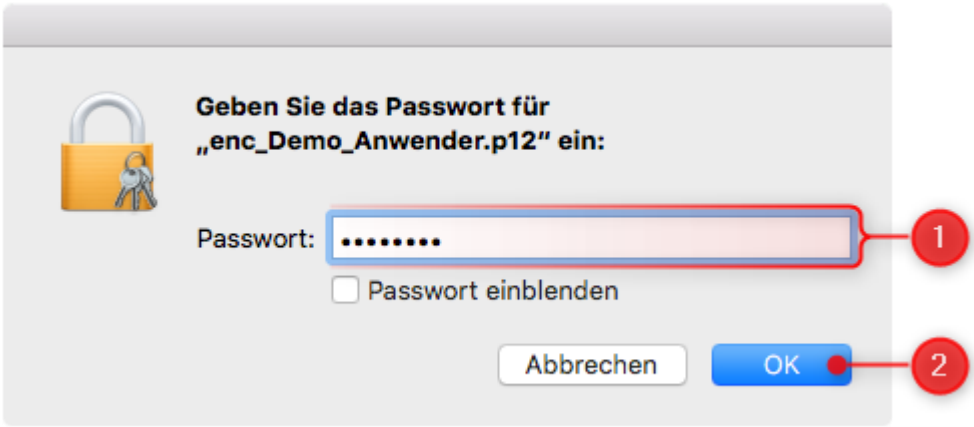


Abbildung 3:Eingabe der Transport-PIN

Nachdem Sie beide Schlüsseldateien importiert haben, müssen Sie ggf. noch die Vertrauenseinstellung für die Zertifizierungsstelle der Bayern-PKI anpassen.

Dazu öffnen Sie die Schlüsselbundverwaltung unter `Programme > Dienstprogramme > Schlüsselbundverwaltung`.

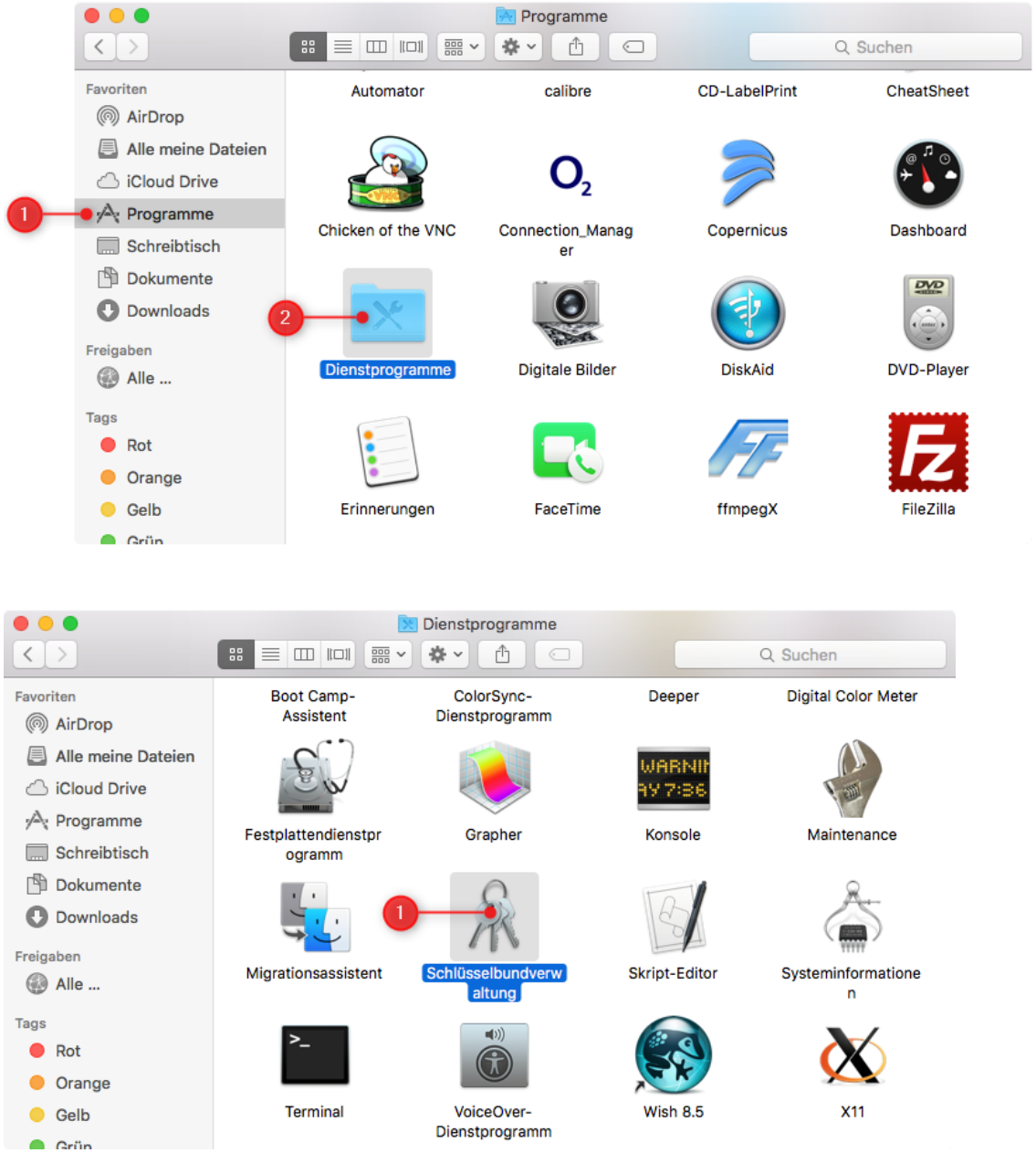


Abbildung 4 Schlüsselbundverwaltung öffnen

Wählen Sie zunächst den Schlüsselbund `Anmeldung` und danach die Kategorie Zertifikate aus. Suchen Sie nun je nach Bedarf nach dem `Zertifikat` mit dem Namen `PCA-1-Verwaltung-15` – ggf. mit Abweichender Jahreszahl am Ende – oder `Bayern-Root-CA-2019` und klicken Sie doppelt auf diesen Eintrag.

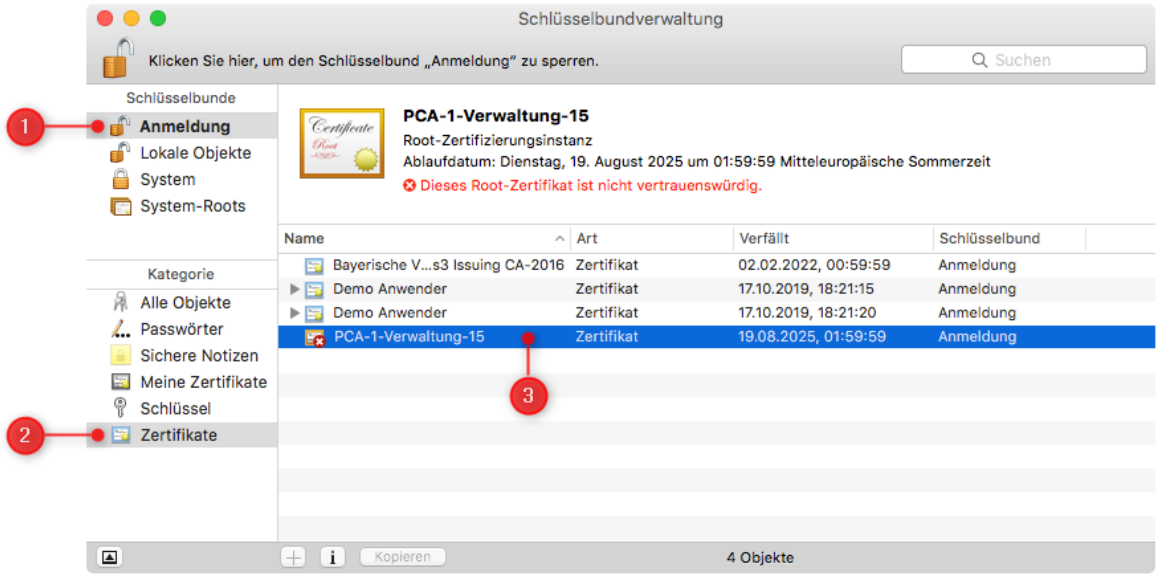


Abbildung 5 Vertrauenseinstellung öffnen

Es öffnet sich ein Fenster mit Informationen über das Zertifikat. Klicken Sie in diesem Fenster auf den Pfeil neben `Vertrauen` um die Vertrauenseinstellungen aufzuklappen.

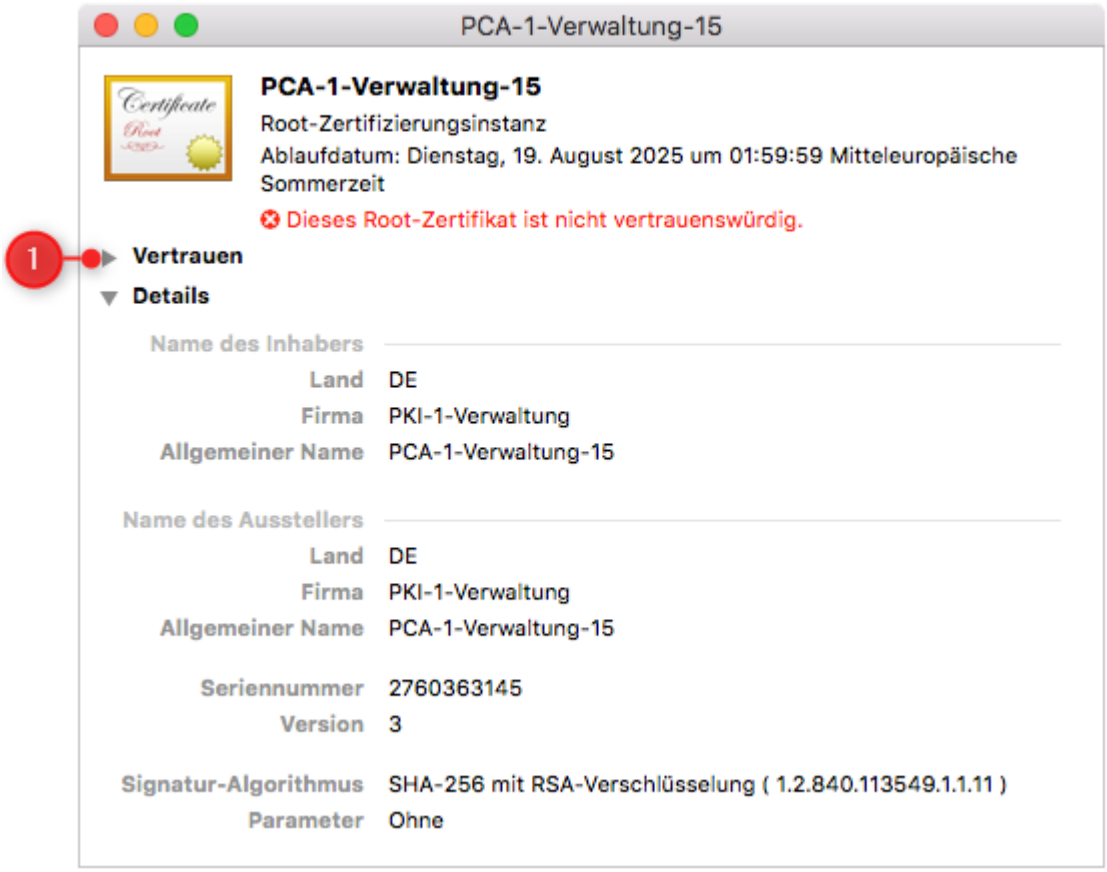


Abbildung 6 Vertrauenseinstellung aufklappen

Wählen Sie bei `S/MIME (Secure Mail)` sowie bei `X.509-Standardrichtlinien` die Option `Immer vertrauen` aus.

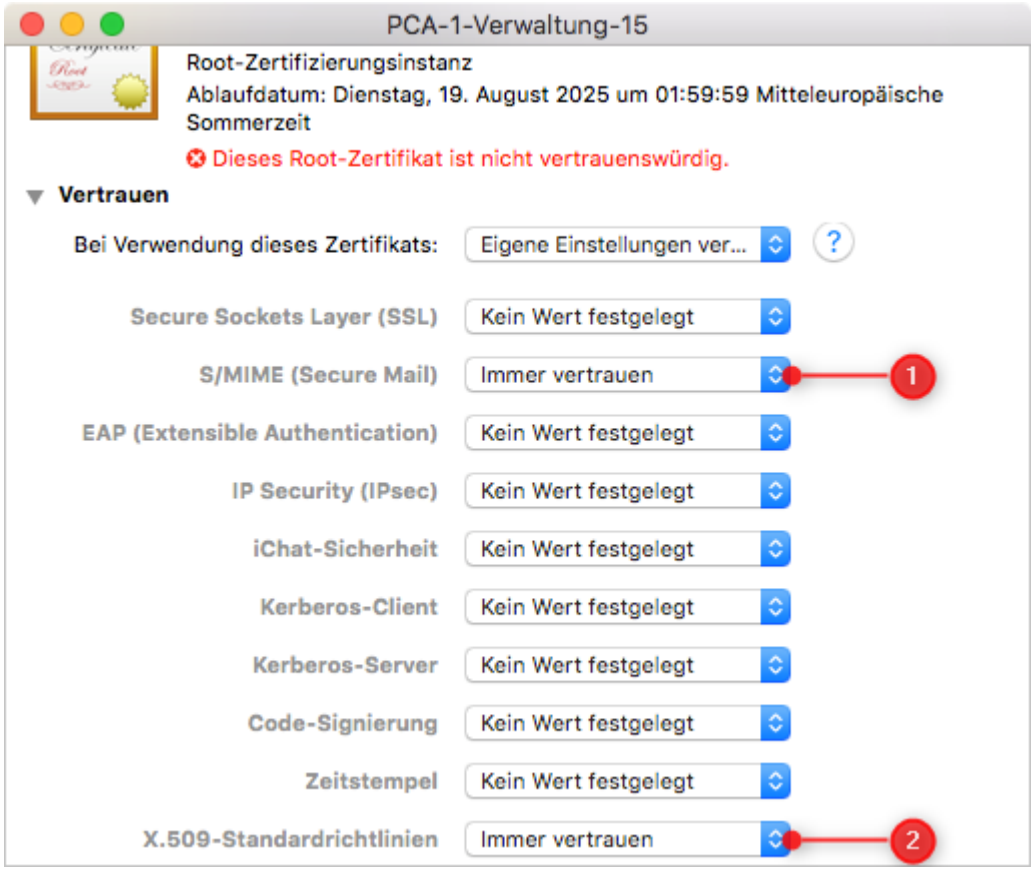
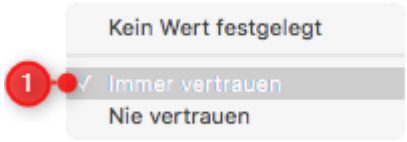


Abbildung 7 Vertrauenseinstellung bearbeiten



Schließen Sie nun das Fenster. Sie werden nun von macOS aufgefordert, Ihr Benutzerpasswort einzugeben, um die Vertrauenseinstellung für dieses Zertifikat anzupassen. Bestätigen Sie den Dialog mit `Einstellungen aktualisieren` und schließen Sie die Schlüsselbundverwaltung.

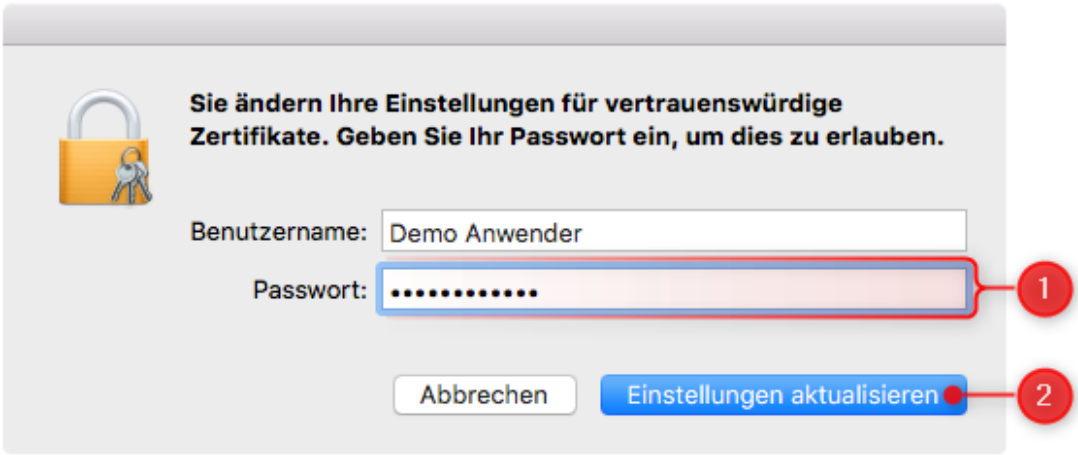


Abbildung 8 Vertrauenseinstellung aktualisieren

Einstellung von Outlook 2016 bzw. 2019

2.2 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 Schlüsselbund importierten Zertifikate der Bayern-PKI dafür nutzt.

Klicken Sie im Hauptfenster von Outlook auf `Extras` und dann auf `Konten`.

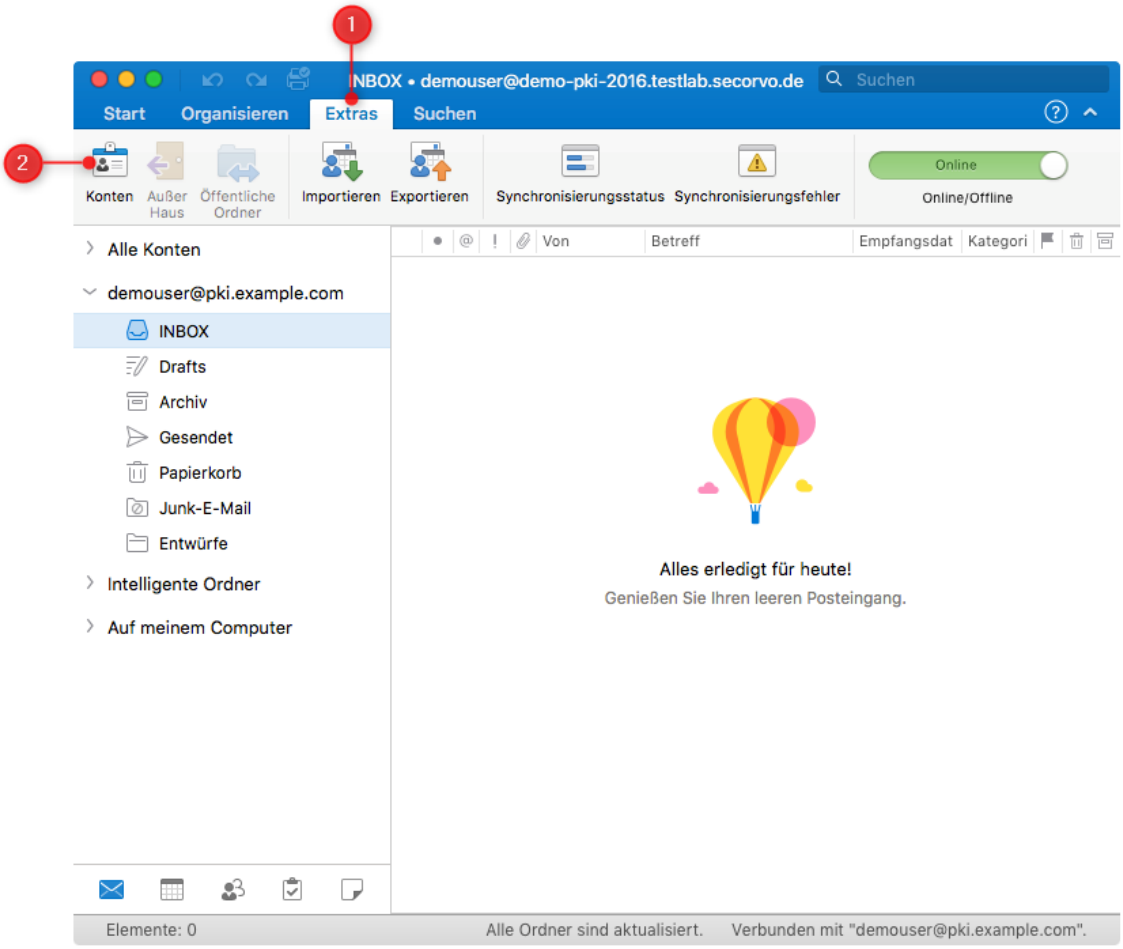


Abbildung 9: Outlook Startseite

Wählen Sie Ihr E-Mail-Konto aus und klicken Sie auf `Erweitert…`.

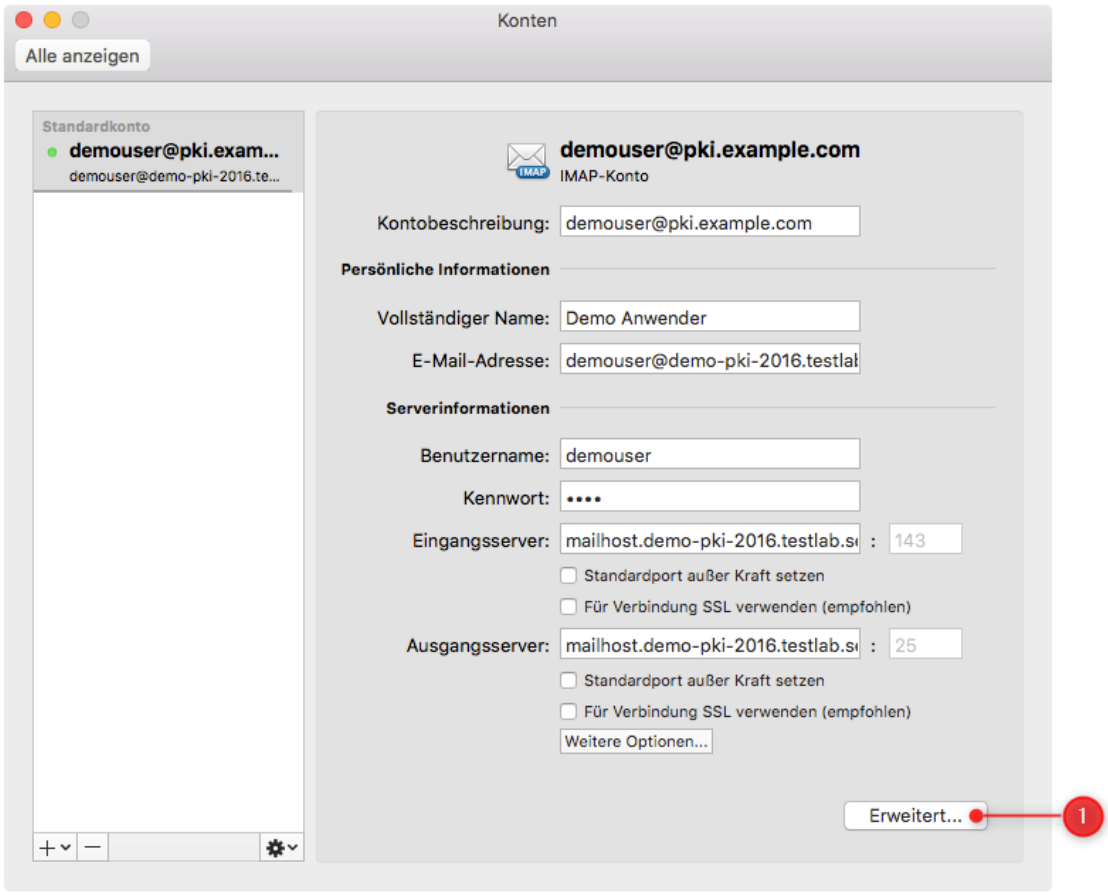


Abbildung 10 E-Mail Konteneinstellungen

Wechseln Sie auf den Reiter `Sicherheit` und wählen Sie unter `Digital signieren` und unter `Verschlüsselung` jeweils bei `Zertifikat` ihr Signatur- bzw. Verschlüsselungszertifikat aus. Dieses sollte mit Ihrem Namen gekennzeichnet sein.

Hinweis: Sollte in dem Einblendmenü (Pop-up-Menü) zur Zertifikatsauswahl mehr als ein Zertifikat unter Ihrem Namen auftauchen, wählen Sie in diesem Menü `Zertifikat auswählen…` und lassen Sie sich weitere Details zu den Zertifikaten anzeigen, um das aktuellste Zertifikat der Bayern-PKI auszuwählen.

Belassen Sie die Einstellungen zum `Signaturalgorithmus` auf `SHA-256` und zum `Verschlüsselungsalgorithmus` auf `AES-256 (sicherer)`.

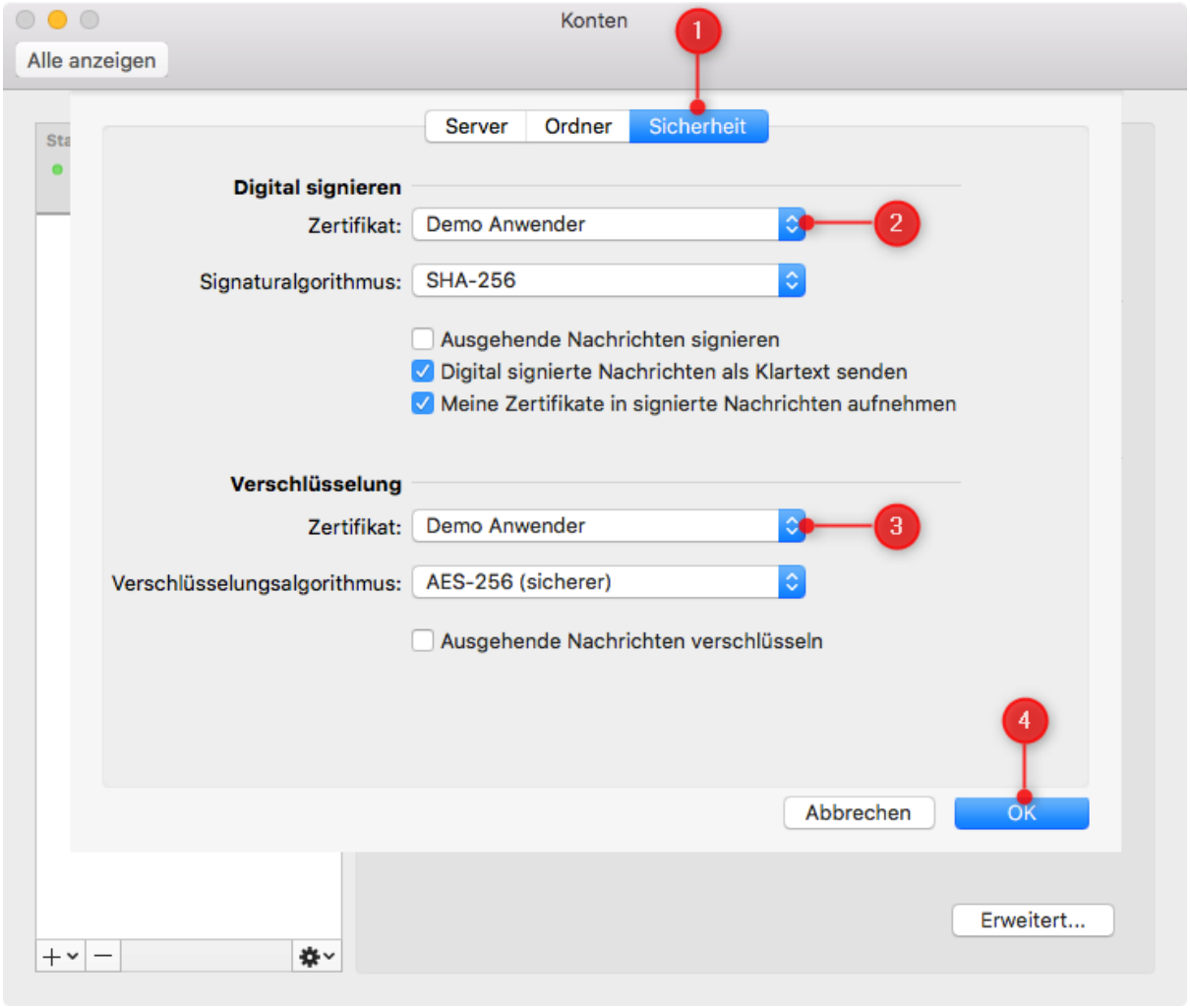


Abbildung 11 Signatur- und Verschlüsselungszertifikat auswählen

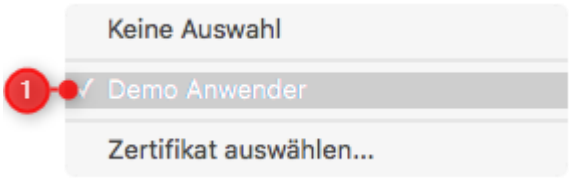


Abbildung 12 Einblendmenü zur Zertifikatsauswahl

2.3 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.

Öffnen Sie den Konten-Dialog über `Extras > Konten` und klicken Sie auf das + Symbol in der unteren, linken Ecke.

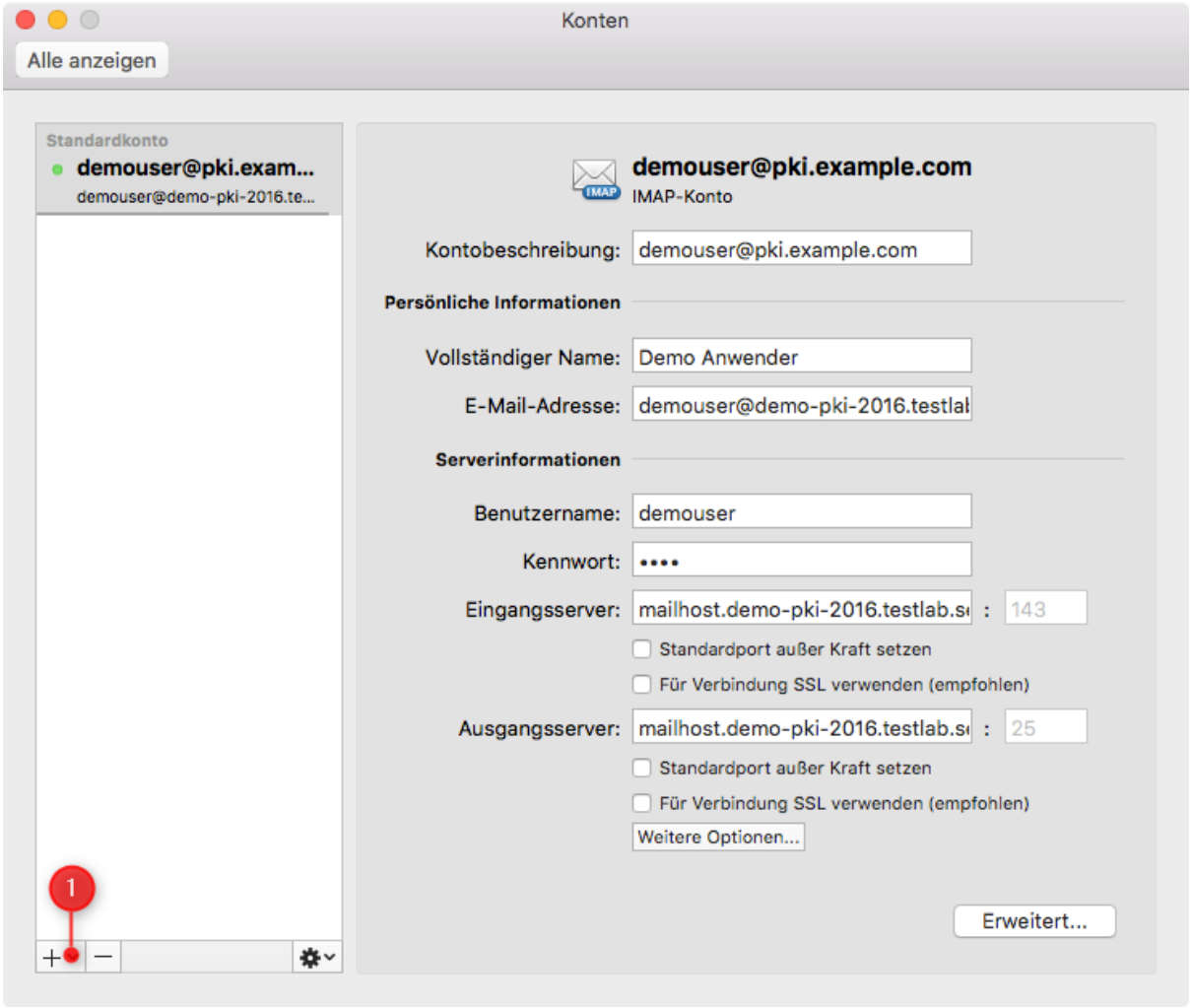


Abbildung 13 Verzeichnisdienst hinzufügen

Wählen Sie in dem dann erscheinenden Einblendmenü (Pop-up-Menü) die Auswahloption `Verzeichnisdienst…` aus.

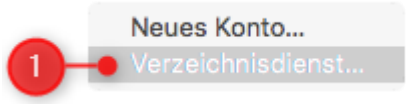


Abbildung 14 Einblendmenü zum Hinzufügen eines neuen Kontos

Geben Sie dann bei `LDAP-Server`
`directory.bybn.de`
bzw. für den externen Verzeichnisdienst `directory.bayern.de`
ein. Die Option `Standardport außer Kraft setzen` bleibt deaktiviert und die Option `Für Verbindung SSL verwenden (empfohlen)` bleibt aktiviert. Klicken Sie dann auf `Konto hinzufügen`.

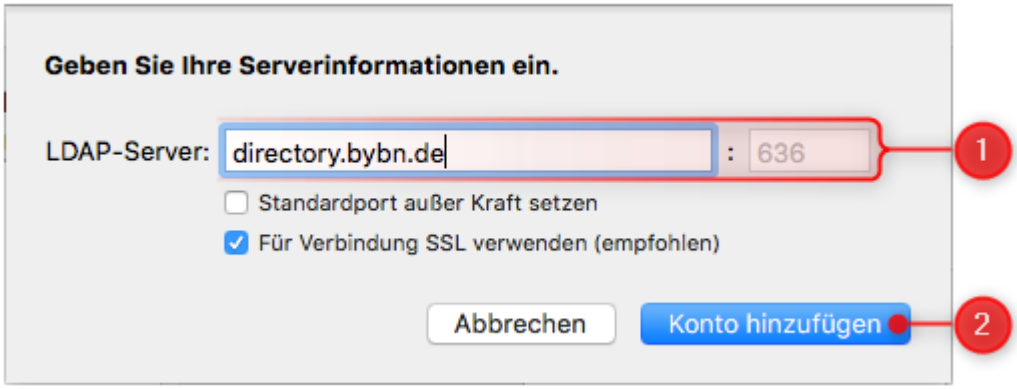


Abbildung 15 LDAP-Serveradresse eingeben

Im Konten-Dialog erscheint ein neuer Eintrag für den soeben angelegten Verzeichnisdienst. Wählen Sie diesen aus – sofern nicht bereits ausgewählt – und klicken Sie auf `Erweitert…`.

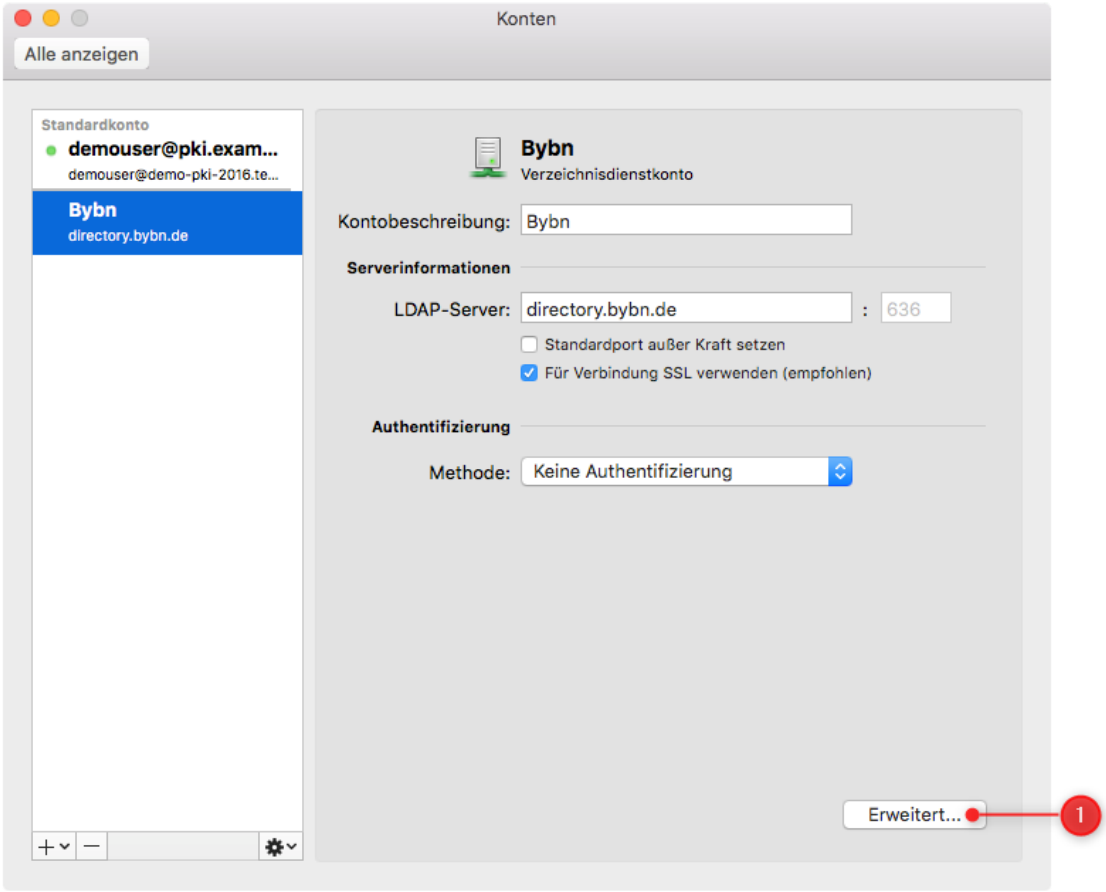


Abbildung 16 Erweiterte Einstellungen des Verzeichnisdienst-Kontos öffnen

Geben Sie als Wert für die Suchbasis

```
ou=pki-teilnehmer,dc=pki,dc=bayern,dc=de
```

ein. Schließen Sie das Einstellungsfenster mit `OK`.

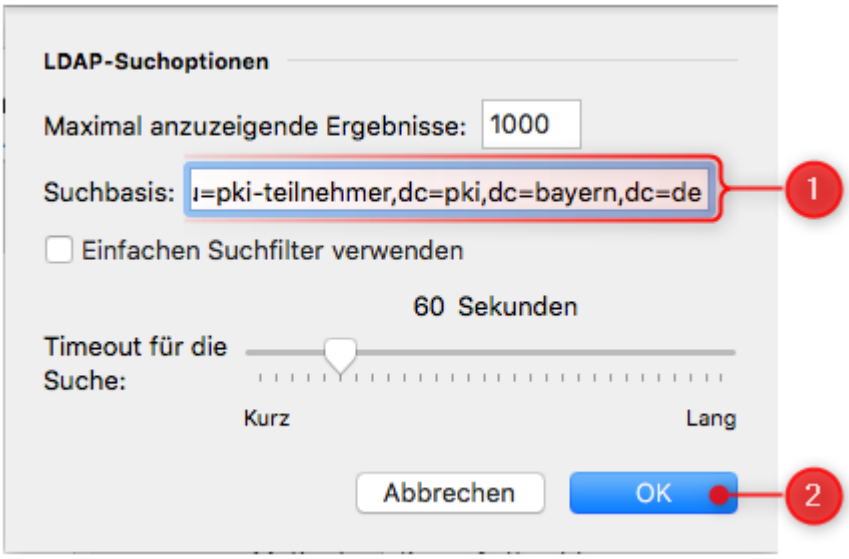


Abbildung 17 LDAP-Suchbasis angeben

Schließen Sie abschließend den Konten-Dialog und beenden Sie Outlook.

3 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 2.3), 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.

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

3.1.1 Regelfall

Erstellen Sie wie üblich eine neue E-Mail-Nachricht. Solange Sie diese E-Mail noch nicht gesendet haben, können Sie unter `Optionen > Sicherheit` über die beiden Menüpunkte für `Nachricht digital signieren` und `Nachricht verschlüsseln` auswählen, ob und wie die E-Mail gesichert werden soll.

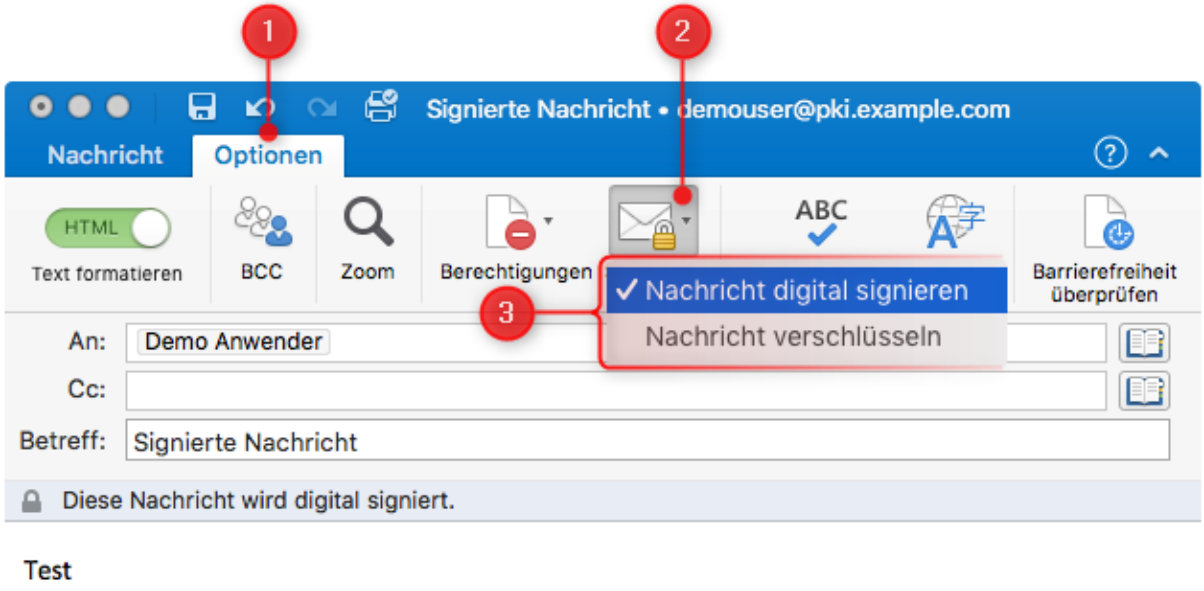


Abbildung 18 Sicherheitsoptionen auswählen

Wenn Sie ausgewählt haben, die E-Mail zu signieren, erscheint nach dem Klick auf `Senden` ein Dialog, in dem Sie nach dem Passwort für Ihren Schlüsselbund gefragt werden. Geben Sie hier ihr Benutzerpasswort ein und bestätigen Sie mit `Erlauben`, um den Schlüsselbund zu entsperren.

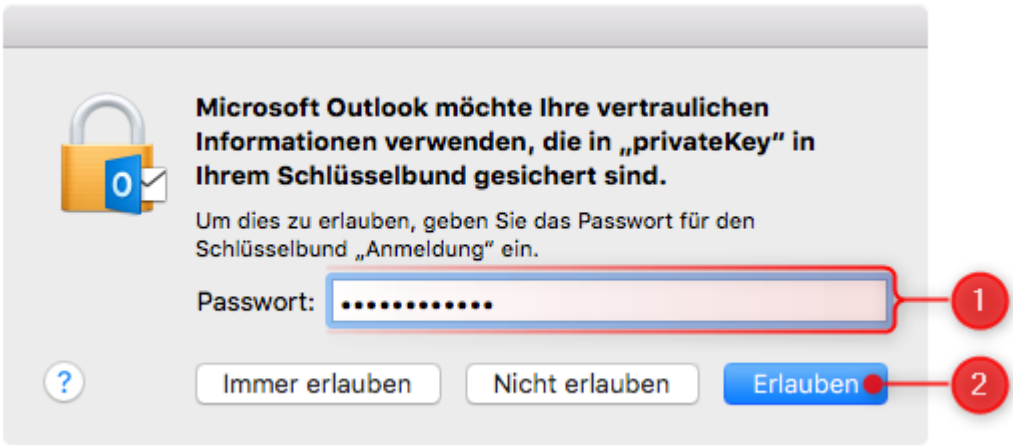


Abbildung 19 Schlüsselbundpasswort eingeben

Wichtig: Falls eine solche Passwortabfrage unmotiviert erscheinen sollte, klicken Sie auf `Nicht erlauben`. 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 mit einer Warnmeldung 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 deren Zertifikate – sofern vorhanden – von dort bezogen werden. Ggf. bitten Sie Ihr Gegenüber, Ihnen ihr bzw. sein Verschlüsselungszertifikat zuzusenden.

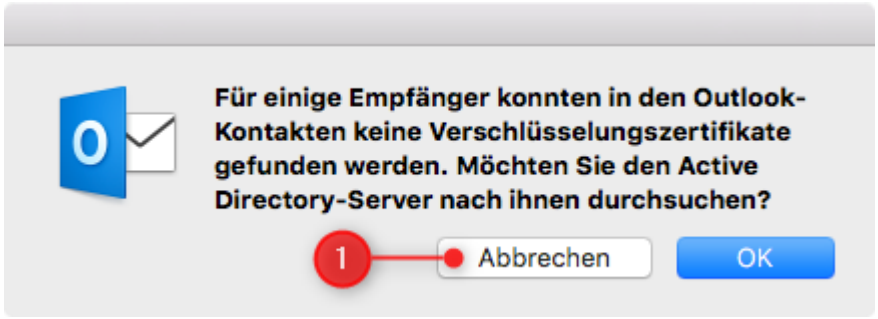


Abbildung 20 Fehlendes Verschlüsselungszertifikat des Empfängers

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

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

Hinweis: Der Versuch eine verschlüsselte E-Mail abzusenden wird zu einer Warnmeldung führen, wenn das eigene Verschlüsselungszertifikat nicht korrekt eingerichtet wurde. Klicken Sie in diesem Fall auf `Abbrechen` und wiederholen Sie den Import Ihres Verschlüsselungszertifikats wie in Kapitel 2.1 beschrieben.

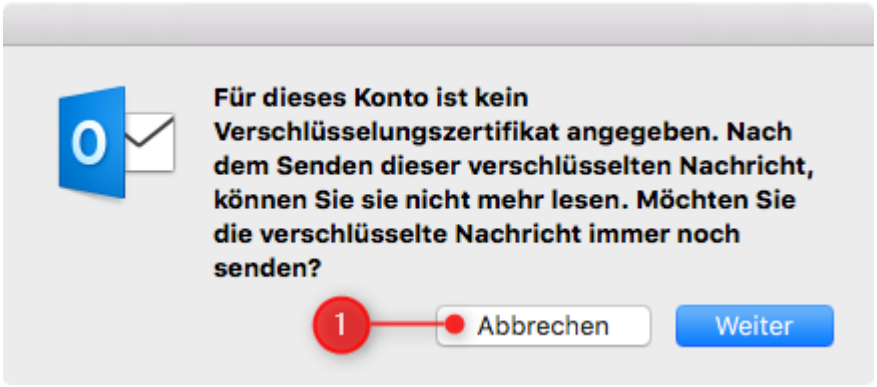


Abbildung 21 Eigenes Verschlüsselungszertifikat nicht korrekt eingerichtet

3.1.2 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 Schlüsselbund 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.

3.1.3 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 20), 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 `Nachricht digital signieren` und `Nachricht verschlüsseln` 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.

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

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

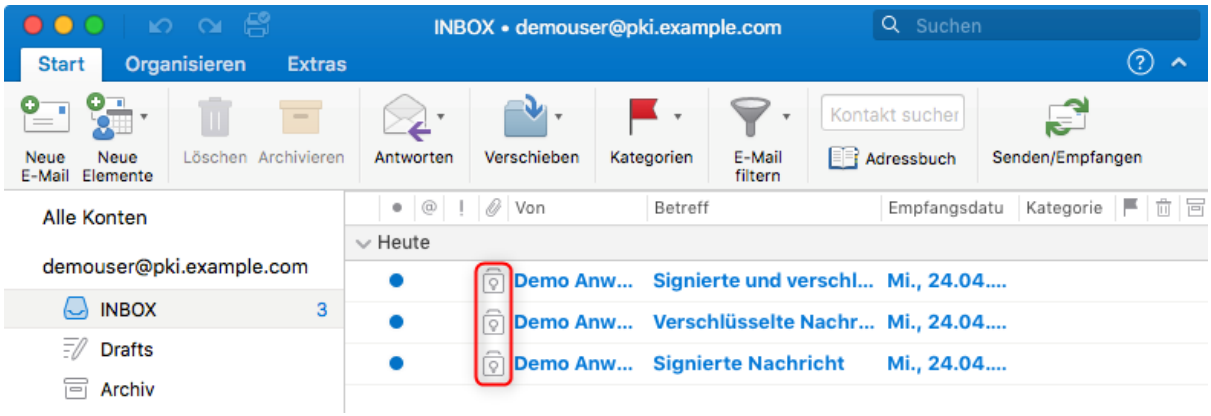


Abbildung 22: Symbole zur Anzeige verschlüsselter bzw. signierter E-Mails in der Postfachansicht

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 Ihr Benutzerpasswort ein und bestätigen Sie mit `Erlauben`.

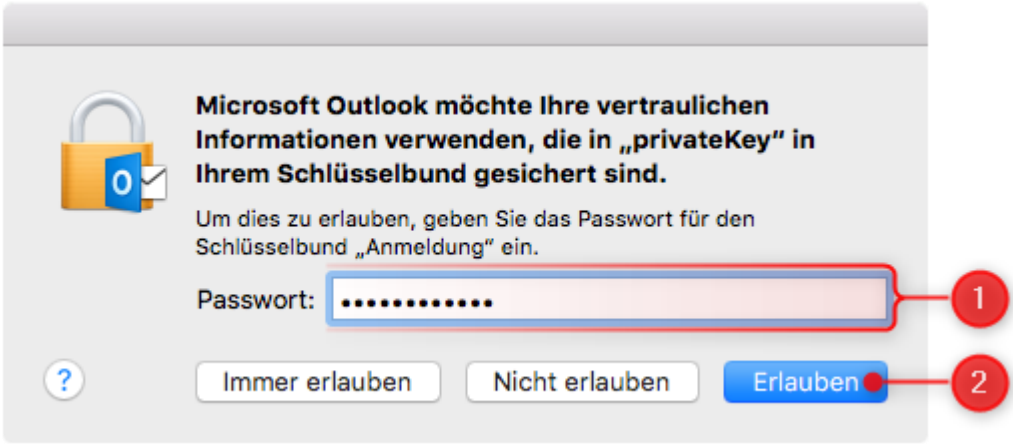


Abbildung 23: Passworteingabe für die Nutzung Ihres privaten Schlüssels zum Lesen einer verschlüsselten E-Mail

Wichtig: Falls eine solche Passwortabfrage unmotiviert erscheinen sollte, klicken Sie auf `Nicht erlauben`. 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 Schlüsselbund 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 eine zusätzliche Zeile in der Kopf-Information angezeigt. Durch einen Klick auf die Schaltfläche `Details` können Sie sich genauere Informationen zu der bei dieser E-Mail angebrachten Signatur bzw. Verschlüsselung anzeigen lassen.

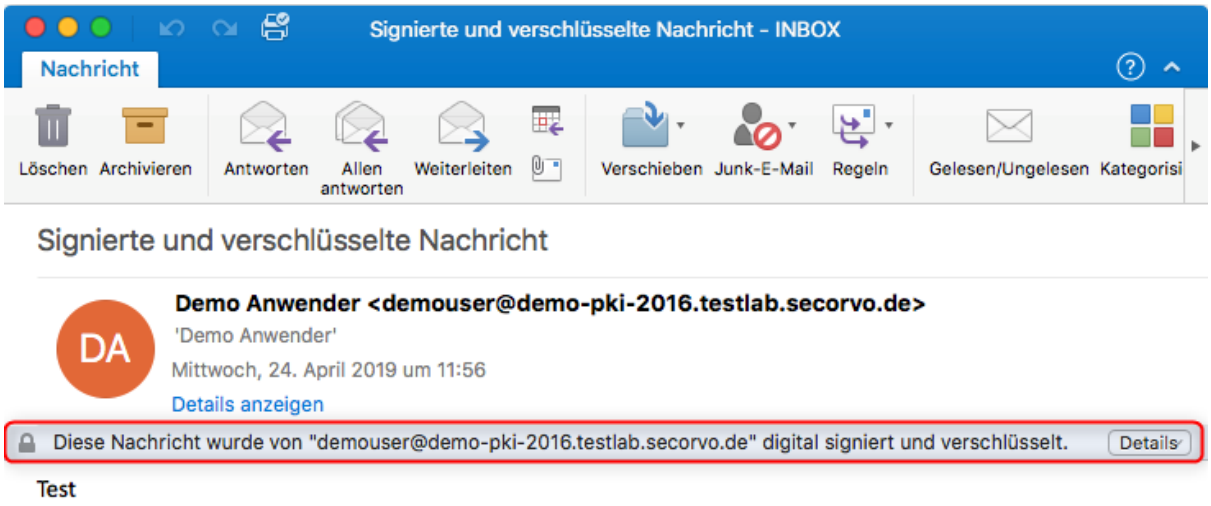


Abbildung 24: Kopf-Information zur Anzeige verschlüsselter bzw. signierter E-Mails in der geöffneten E-Mail

4 Hinweise für den Administrator

4.1 Importieren der Root-CA mit Vertrauenseinstellungen

Über die Kommandozeile lässt sich mit dem Programm `security` ein Zertifikat mit Vertrauenseinstellungen in den Anmeldeschlüsselbund importieren.

```
/usr/bin/security add-trusted-cert -p "smime" -p "basic" -k "login.keychain" /tmp/PCA-1-Verwaltung-15.cer
```

Danach ist das Zertifikat im Anmeldeschlüsselbund importiert und kann für S/MIME verwendet werden. Werden diese Schritte ausgeführt, muss der Anwender die unter 2.1 aufgeführten Schritte zum Ändern der Vertrauenseinstellung nicht mehr durchführen.

4.2 Importieren von CA-Zertifikaten per Geräteprofil

Wenn der Mac mit Hilfe eines Management Systems verwaltet wird, das Geräteprofile (Apple Configuration Profiles) für macOS unterstützt, bspw. dem Apple Profilmanager, können darüber CA-Zertifikate – insbesondere Root-Zertifikate – in den System-Schlüsselbund importiert werden.

Dazu müssen im Geräteprofil eine oder mehrere Certificate Payloads aufgenommen werden. Nähere Informationen hierzu sollten ggf. in der Dokumentation des eingesetzten Management Systems zu finden sein.

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