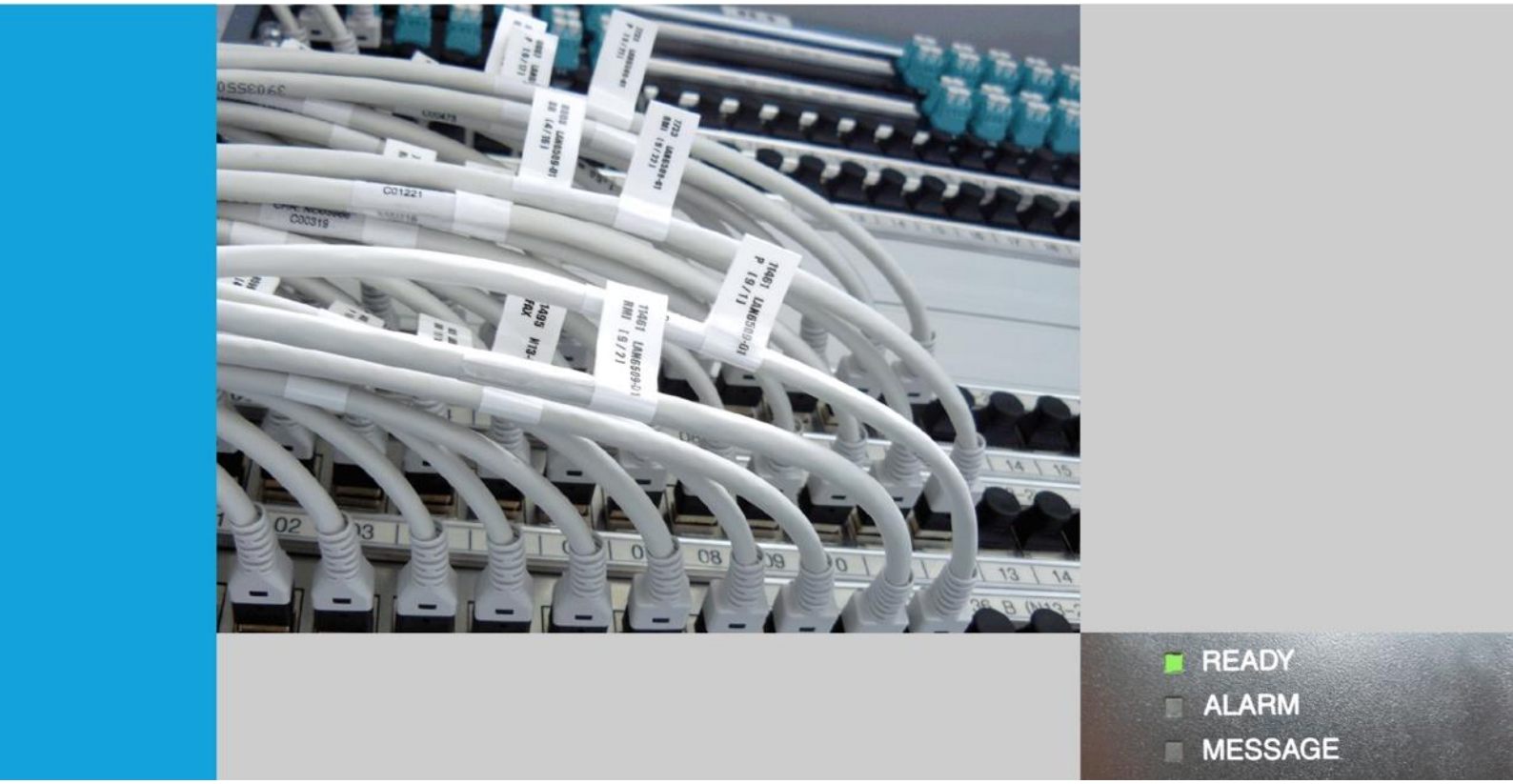
Landesamt für Digitalisierung,
Breitband und Vermessung

IT-Dienstleistungszentrum des Freistaats Bayern



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

Thunderbird 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 Thunderbird unter Windows 10 zu verschlüsseln bzw. entschlüsseln und zu signieren, sind drei Schritte erforderlich, die in den nachfolgenden Kapiteln genauer beschrieben werden:

1. Empfang der Zertifikate per E-Mail
2. Einstellung von Thunderbird
3. Nutzung sicherer E-Mails bei der täglichen Arbeit

Unter Umständen kann Ihr Administrator Ihnen Teile der Einrichtung durch eine passende Vorkonfiguration Ihrer Thunderbird Anwendung abnehmen oder bei Problemen unterstützen. 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 Einstellung von Thunderbird

2.1 Setzen eines Master-Passworts

Damit die Schlüsselinformationen nicht ungeschützt auf Ihrem Rechner gespeichert werden, müssen Sie ein Master-Passwort für Thunderbird vergeben. Bei jedem Start von Thunderbird werden Sie dann aufgefordert, dieses Master-Passwort einmal einzugeben um die von Thunderbird gespeicherten Passwörter und Schlüsselinformationen zu entschlüsseln.

Hinweis: Möglicherweise haben Sie bereits ein Master-Passwort eingestellt. Dies ist der Fall, wenn Sie beim Start von Thunderbird immer ein Passwort eingeben müssen (vgl. Abbildung 1). In diesem Fall können Sie direkt mit dem Schritt 2.2 Import der Schlüsseldateien fortfahren.

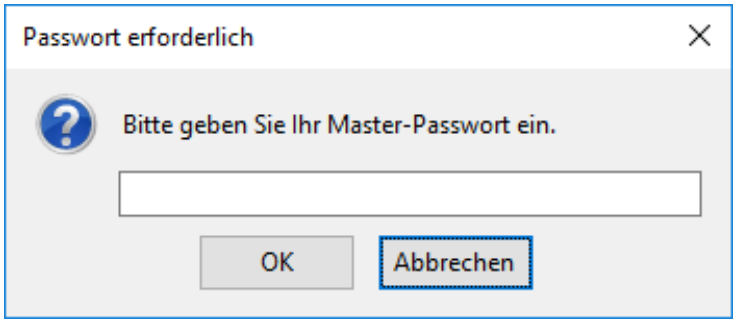


Abbildung 1 Abfrage des Master-Passworts beim Start von Thunderbird

Um ein Master-Passwort festzulegen, klicken Sie zunächst auf den `Menüknopf` und wählen Sie `Einstellungen`.

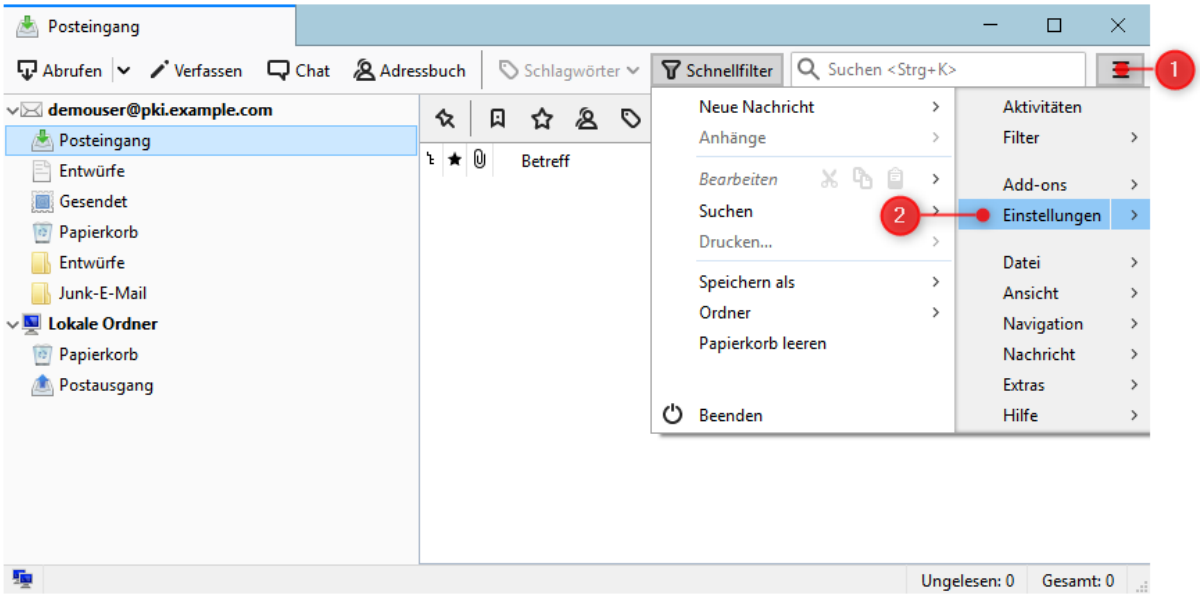


Abbildung 2 Einstellungen in Thunderbird öffnen

Klicken Sie auf `Sicherheit`, wählen Sie dann den Reiter `Passwörter` aus und setzen Sie das Häkchen bei `Master-Passwort verwenden`.

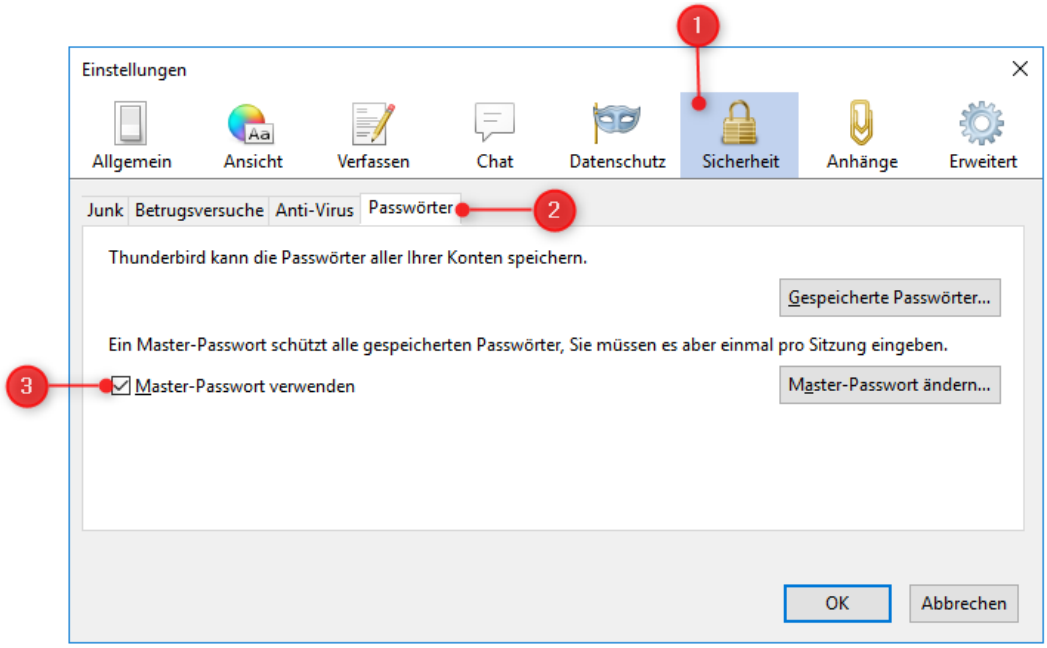


Abbildung 3 Einstellungs-Fenster von Thunderbird

Nun können Sie Ihr neues Master-Passwort festlegen. Achten Sie darauf, dass Ihr neues Master-Passwort ausreichend komplex ist. Sie werden bei jedem zukünftigen Start von Thunderbird dazu aufgefordert, dieses Passwort einzugeben. Nachdem Sie ihr neues Passwort zweimal eingegeben haben, klicken Sie auf `OK`.

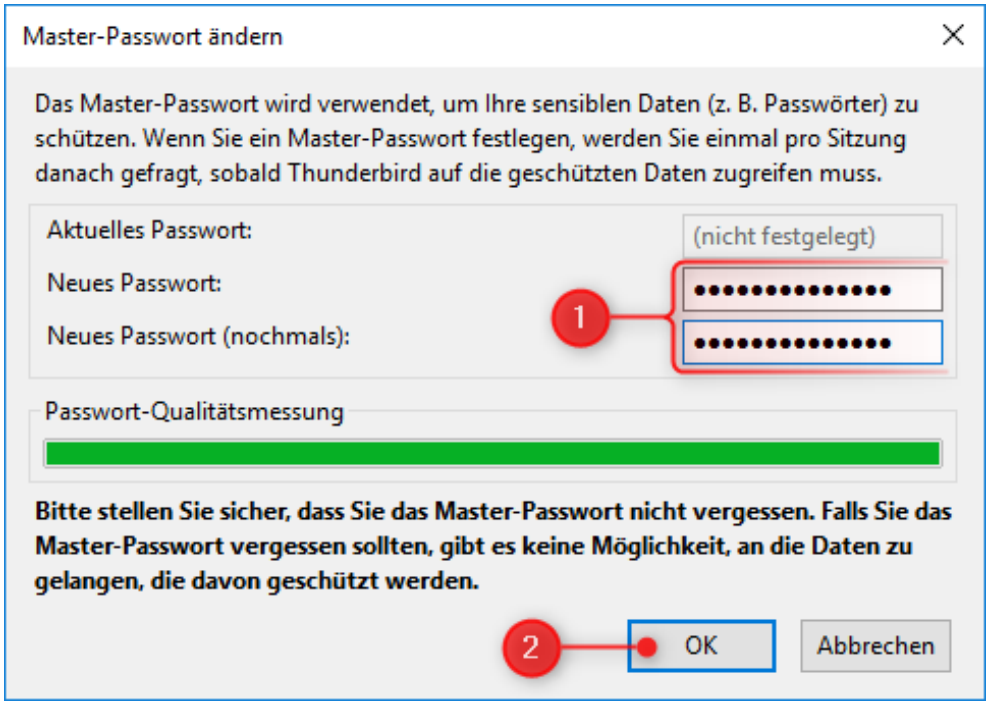


Abbildung 4 Dialog zum Ändern/Erstellen eines Master-Passworts

Wichtig: Wie in diesem Dialog angezeigt, gibt es keine Möglichkeit mehr, auf die gespeicherten Passwörter und Schlüssel zuzugreifen, falls Sie das Master-Passwort vergessen haben.
Ihr Administrator kann Sie dabei unterstützen, ein vergessenes Master-Passwort

zurückzusetzen. Dabei werden jedoch alle gespeicherten Passwörter und Ihre Schlüssel gelöscht. Ihre Zertifikate der Bayern-PKI sind zwar danach noch vorhanden, können aber mangels der zugehörigen Schlüssel nicht verwendet werden; d. h. Sie müssen anschließend Ihre Schlüsseldateien erneut importierten. Die für das Zurücksetzen des Master-Passworts notwendige Prozedur ist in Kapitel 4.3 beschrieben.

Bestätigen Sie den Bestätigungs-Dialog mit `OK` und schließen Sie danach das Einstellungs-Fenster.

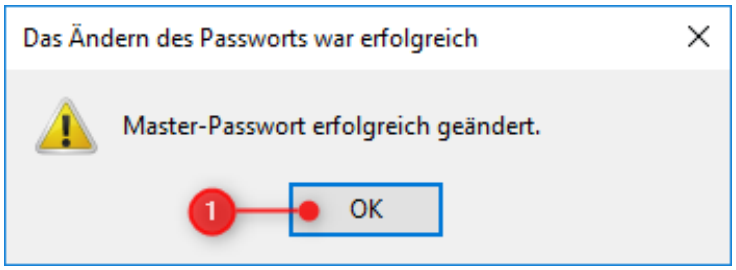


Abbildung 5 Bestätigung zur Änderung/Erstellung eines Master-Passworts

2.2 Import der Schlüsseldateien und Aktivierung der Zertifikate

Nun können Sie Ihre neuen Schlüssel und Zertifikate der Bayern-PKI aus den Schlüsseldateien, die sie zuvor in einem lokalen Ordner abgespeichert haben, in Ihren persönlichen Zertifikatsspeicher in Thunderbird importieren.

Zum Import öffnen Sie Thunderbird und klicken Sie mit der rechten Maustaste auf Ihre E-Mail-Adresse. Wählen Sie den Menüpunkt `Einstellungen` aus.

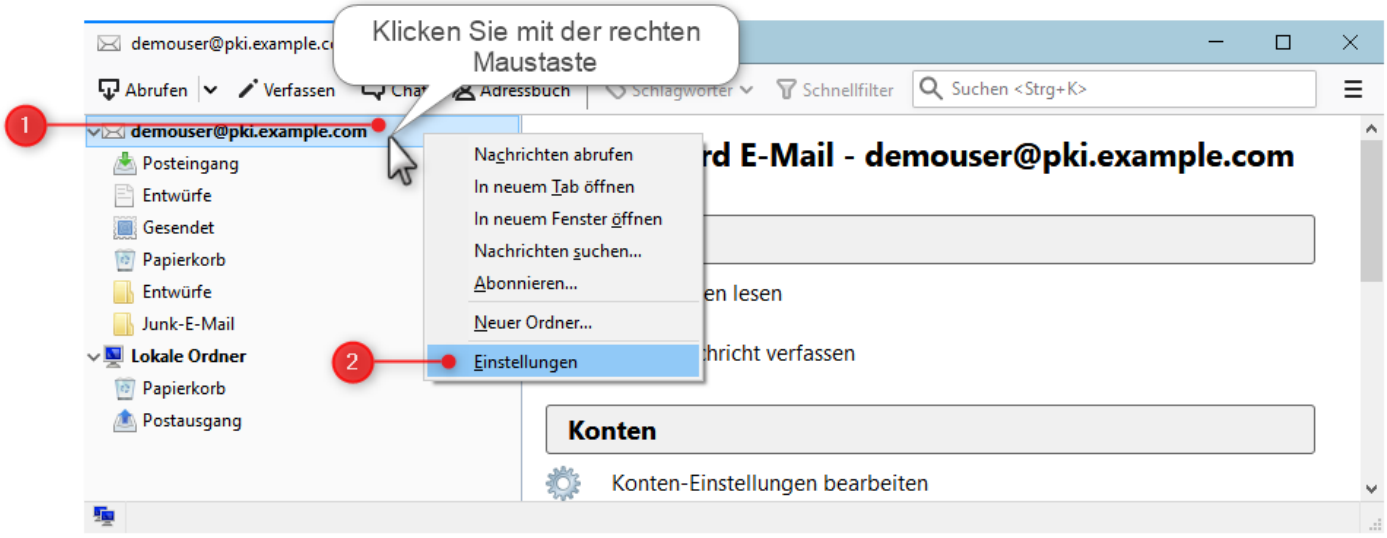


Abbildung 6 Aufruf der Konten-Einstellungen in Thunderbird

Wählen Sie im darauf erscheinenden Dialog im Menü `S/MIME-Sicherheit` aus, klicken Sie danach auf `Zertifikate verwalten…` .

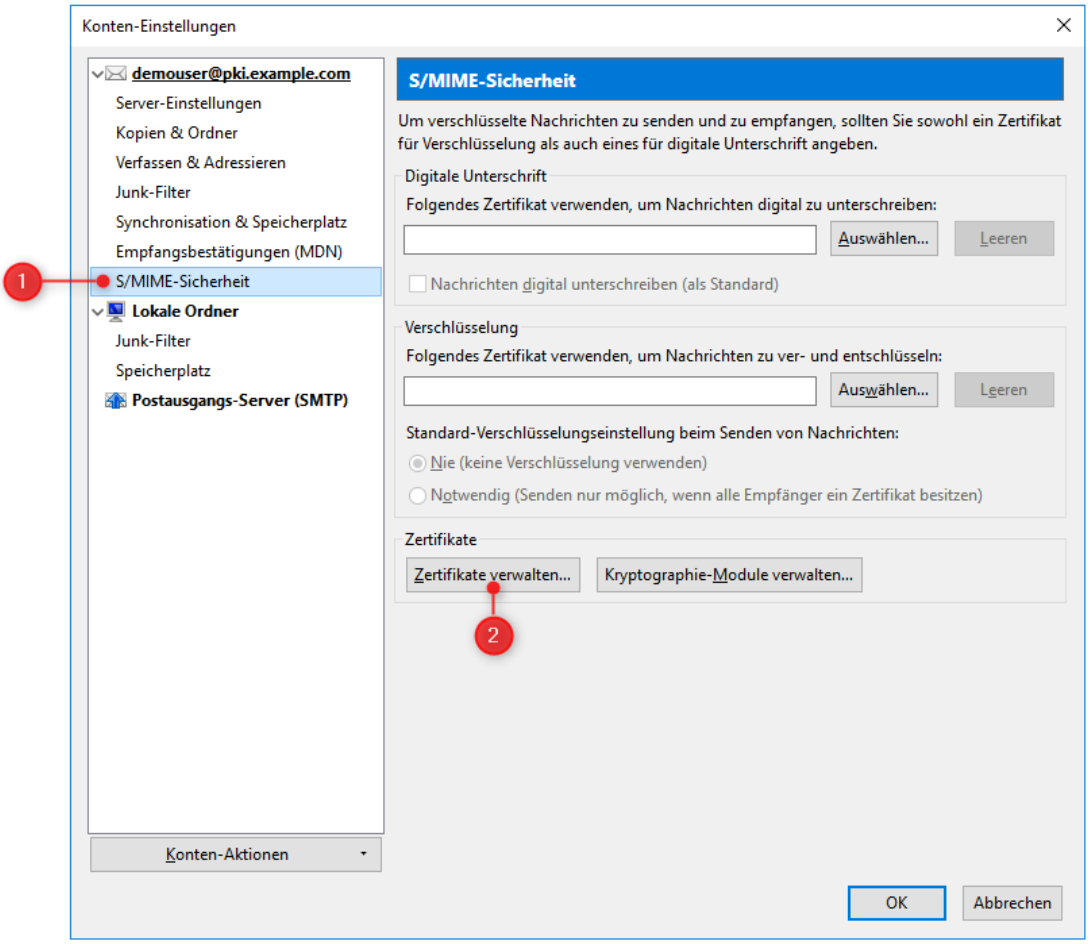


Abbildung 7 Aufruf der Zertifikatsverwaltung

Wählen Sie den Reiter `Ihre Zertifikate` und klicken Sie im darauf erscheinenden Dialog auf `Importieren…`.

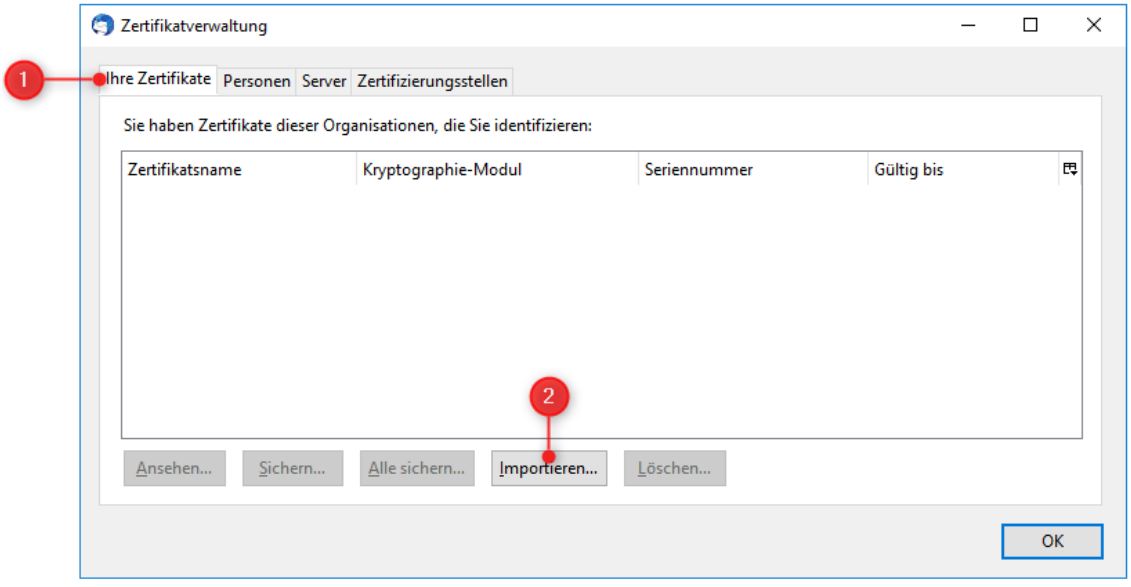


Abbildung 8 Zertifikatsverwaltung von Thunderbird

Navigieren Sie zum Speicherort Ihrer Zertifikate und wählen Sie eines der Zertifikate aus. In diesem Beispiel beginnen wir mit dem Verschlüsselungszertifikat. Ob Sie zuerst das Verschlüsselungszertifikat, oder zuerst das Signaturzertifikat für den Importvorgang wählen ist unerheblich. In diesem Beispiel beginnen wir mit dem Verschlüsselungszertifikat.

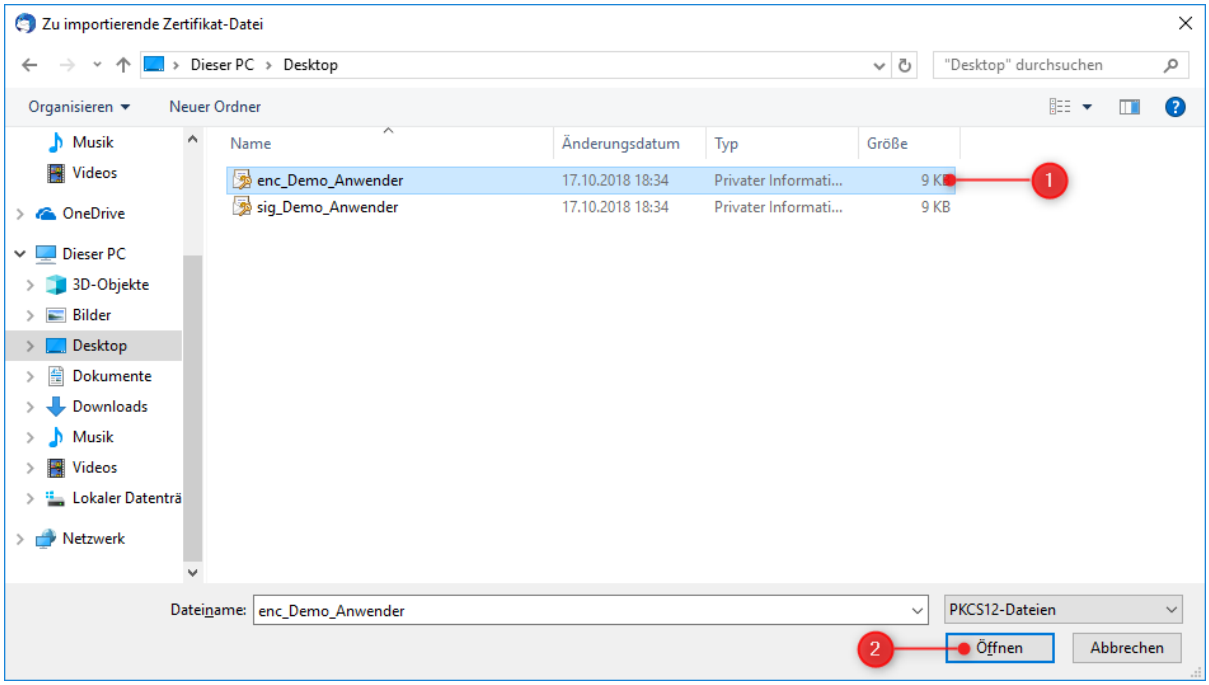


Abbildung 9 Zu importierende Zertifikatsdatei auswählen

Geben Sie im erscheinenden Dialog die Transport-PIN für das Zertifikat ein und bestätigen Sie diese mit `OK`.

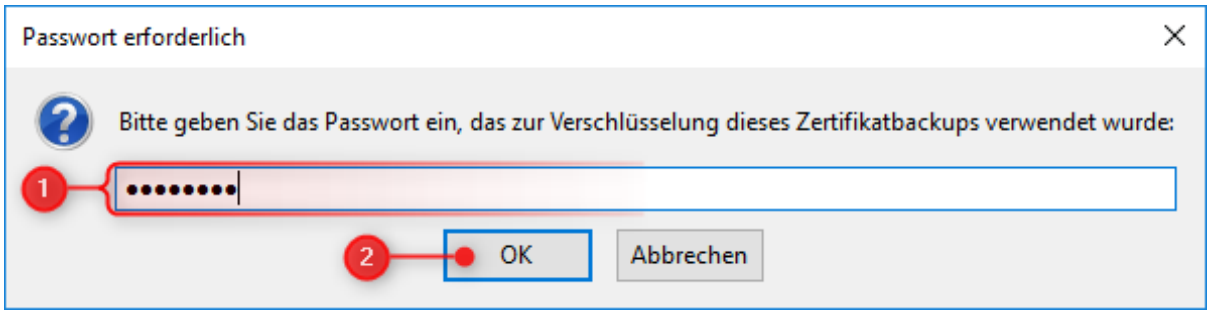


Abbildung 10 Abfrage der Transport-PIN

Wiederholen Sie den Vorgang für das andere Zertifikat, so dass Sie letztendlich beide Zertifikate importiert haben. Klicken Sie dazu erneut auf `Importieren...`.

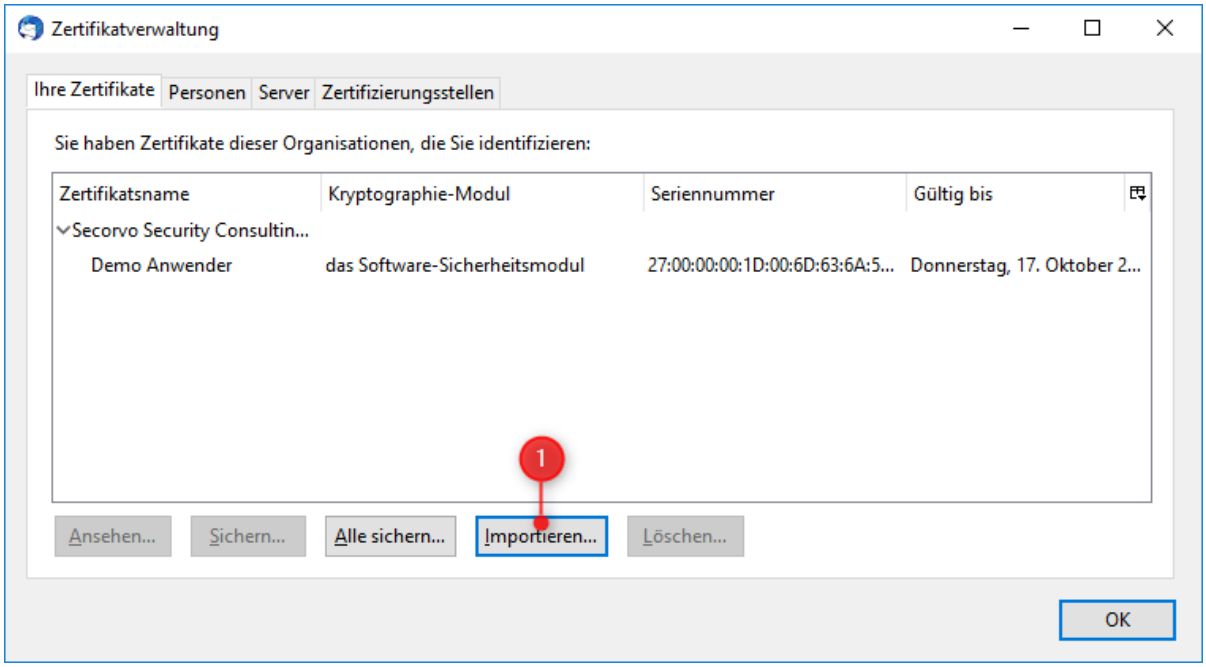


Abbildung 11 Importieren einer weiteren Zertifikatsdatei

Navigieren Sie erneut zum Speicherort Ihrer Zertifikate und wählen Sie nun das andere Zertfikat aus. Klicken Sie danach auf `Öffnen`.

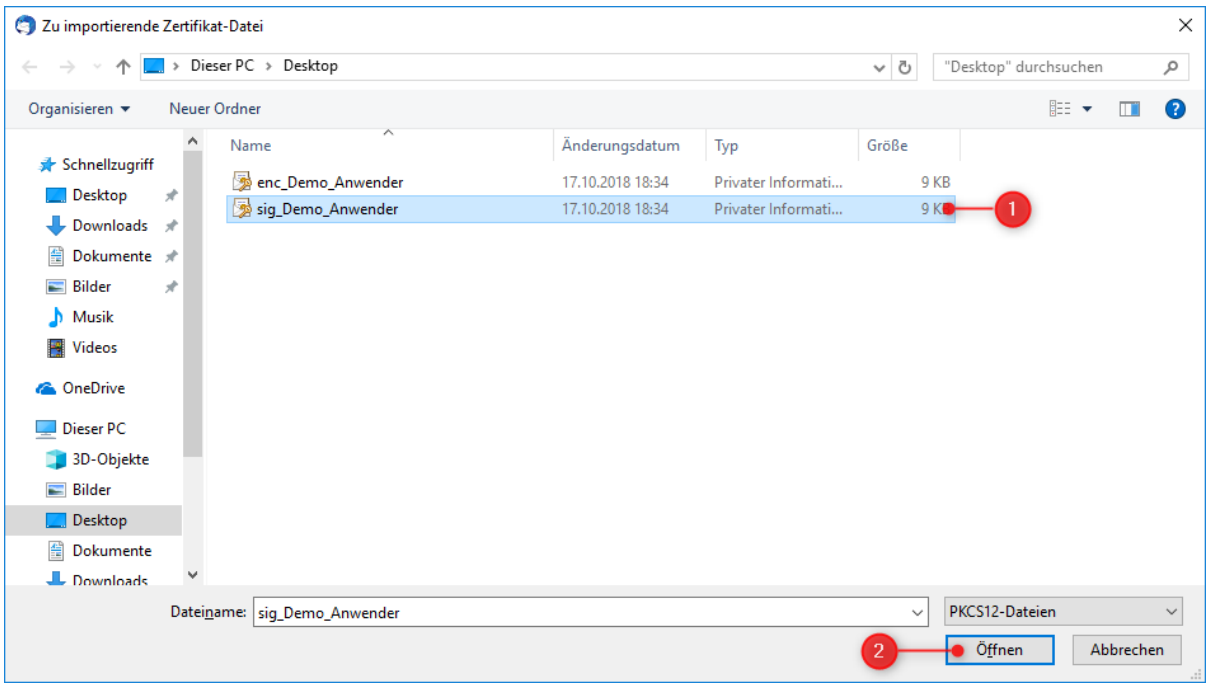


Abbildung 12 Zu importierende Zertifikatsdatei auswählen

Geben Sie im erscheinenden Dialog die Transport-PIN für das Zertifikat ein und bestätigen Sie diese mit `OK`.

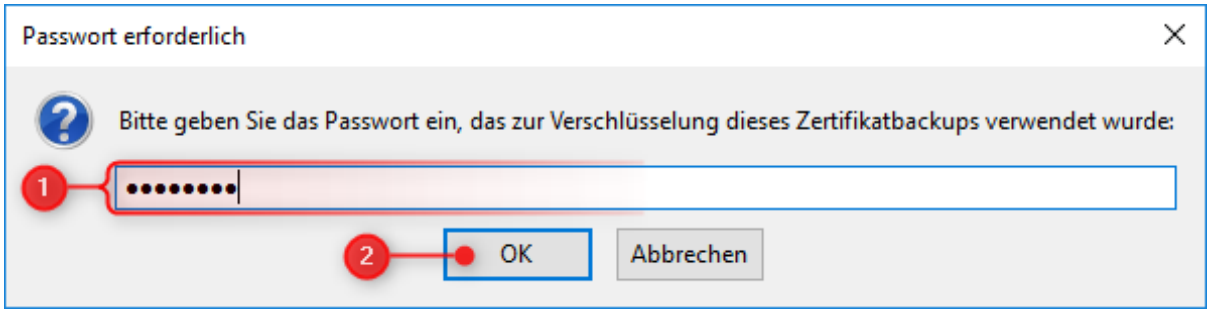


Abbildung 13 Abfrage der Transport-PIN

In der Zertifikatsverwaltung sollten Sie nun beide Zertifikate mit Ihrem Namen sehen. Schließen Sie die Zertifikatsverwaltung mit einem Klick auf `OK`.

Hinweis: Schließen Sie noch nicht die Kontoeinstellungen zur `S/MIME-Sicherheit`; diese werden im folgenden Schritt noch benötigt.

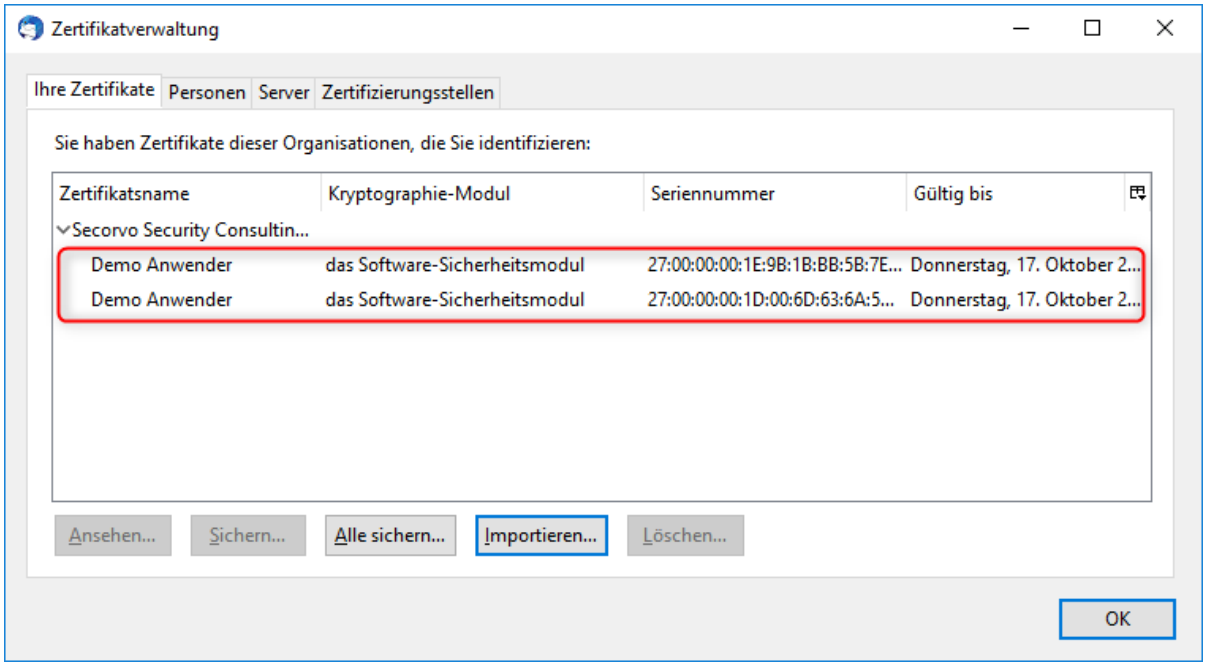


Abbildung 14: Abschluss des Zertifikatimport-Assistenten

Wichtig: Nach erfolgreichem Import der Zertifikate ins System sollten Sie die beiden `.p12` Dateien, die Sie in Schritt 1 angelegt haben, wieder löschen.

Wechseln Sie nun auf den Reiter `Zertifizierungsstelen`. Suchen Sie in der Liste nach PKI1-Verwaltung und wählen Sie die `PCA-1-Verwaltung-15` (ggf. mit abweichender Jahreszahl) aus. Klicken Sie danach auf `Vertrauen bearbeiten…` .

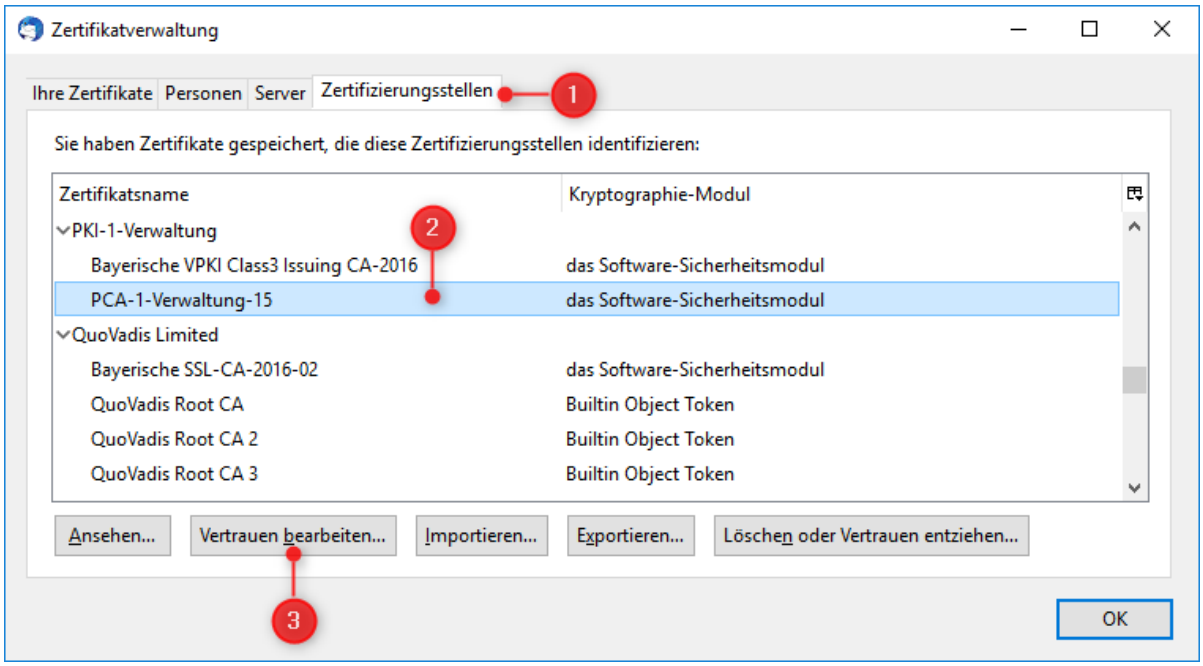


Abbildung 15 Liste der Zertifizierungsstellen

Setzen Sie ein Häkchen bei `Dieses Zertifikat kann Mail-Benutzer identifizieren` und bestätigen Sie den Dialog mit `OK`. Sie können danach die Zertifikatsverwaltung ebenfalls mit `OK` bestätigen.

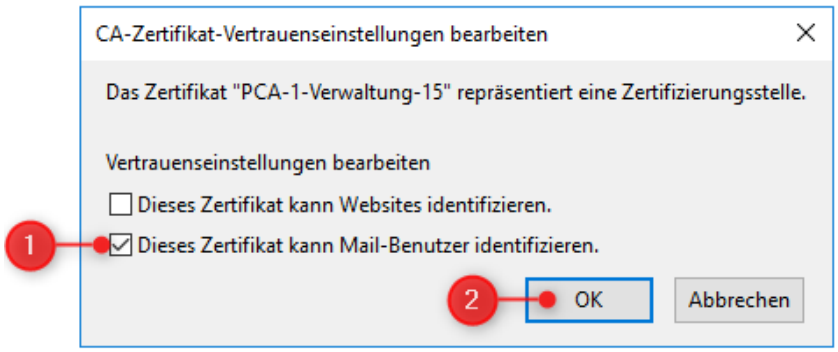


Abbildung 16 Vertrauenseinstellungen der Zertifizierungsstelle bearbeiten

Bevor Sie E-Mails verschlüsseln oder signieren können, müssen Sie Thunderbird so einstellen, dass es Ihre neuen, soeben importierten Zertifikate der Bayern-PKI, dafür nutzt.

Klicken Sie im Konten-Einstellungen-Dialog zur `S/MIME-Sicherheit` bei Digitale Unterschrift auf `Auswählen`….

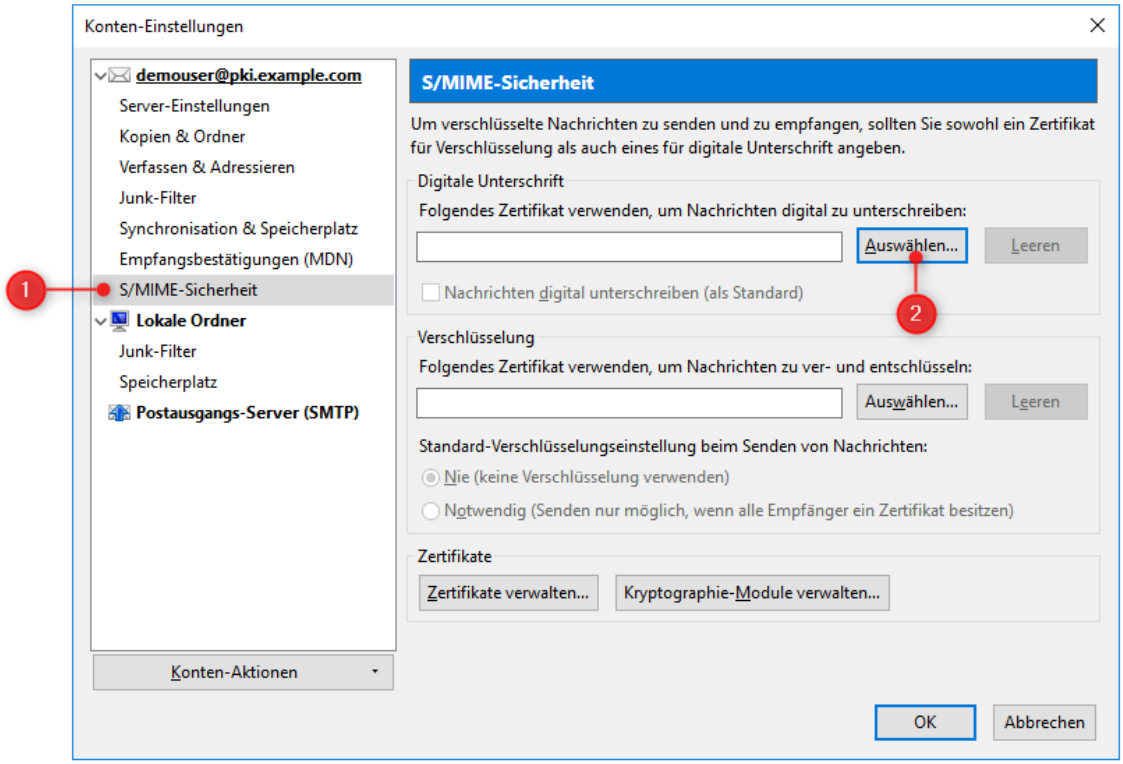


Abbildung 17 Auswählen des Signaturzertifikats

Wählen Sie Ihr Signaturzertifikat aus und bestätigen Sie die Auswahl mit `OK`.

Hinweis: Im Regelfall wird ihnen in diesem Dialog als einziges Zertifikat zur Auswahl das zuvor importierte Signaturzertifikat der Bayern-PKI angeboten.

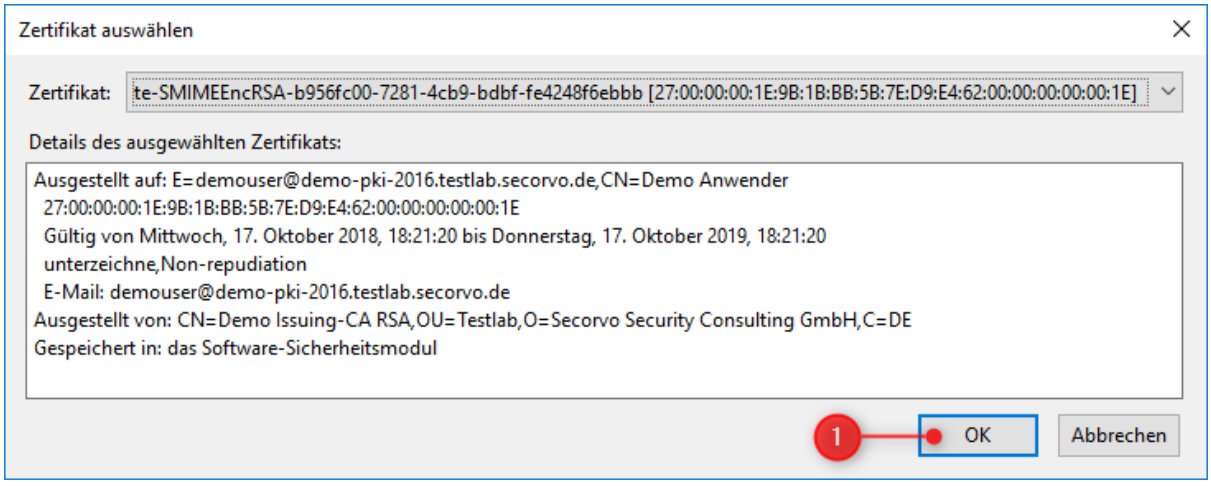


Abbildung 18 Bestätigung des Signaturzertifikats

Bestätigen Sie den Hinweis auf die Einrichtung eines Verschlüsselungszertifikats mit `Ja`.

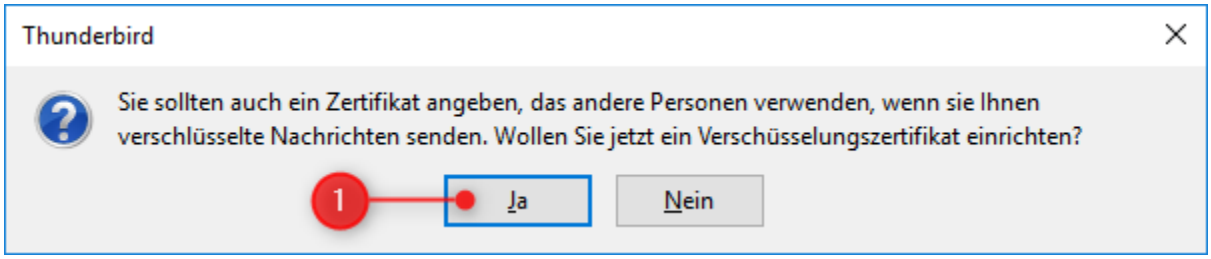


Abbildung 19 Abfrage zur Einrichtung eines Verschlüsselungszertifikats

Wählen Sie Ihr Verschlüsselungszertifikat aus und bestätigen Sie die Auswahl mit `OK`.

Hinweis: Im Regelfall wird ihnen in diesem Dialog als einziges Zertifikat zur Auswahl das zuvor importierte Signaturzertifikat der Bayern-PKI angeboten.

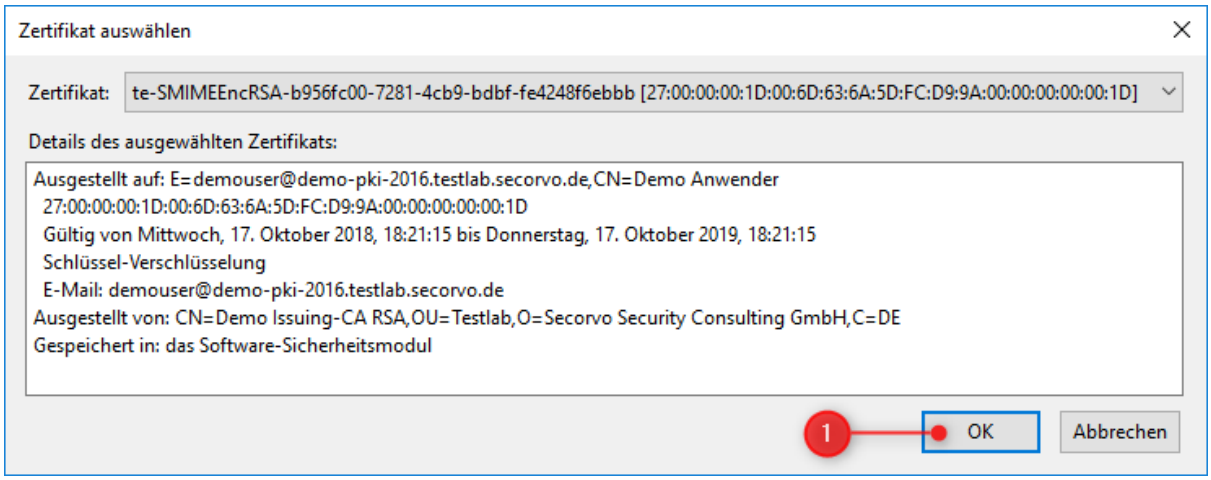


Abbildung 20 Bestätigung des Verschlüsselungszertifikats

Nun sollten sowohl das Signaturzertifikat als auch das Verschlüsselungszertifikat eingerichtet worden sein. Prüfen Sie, dass in den S/MIME-Sicherheit-Einstellungen unter `Digitale Unterschrift` und `Verschlüsselung` bereits Ihr Name voreingestellt ist, der aus Ihren neuen Zertifikaten ausgelesen wurde. Schließen Sie den Konten-Einstellungen-Dialog mit einem Klick auf `OK`.

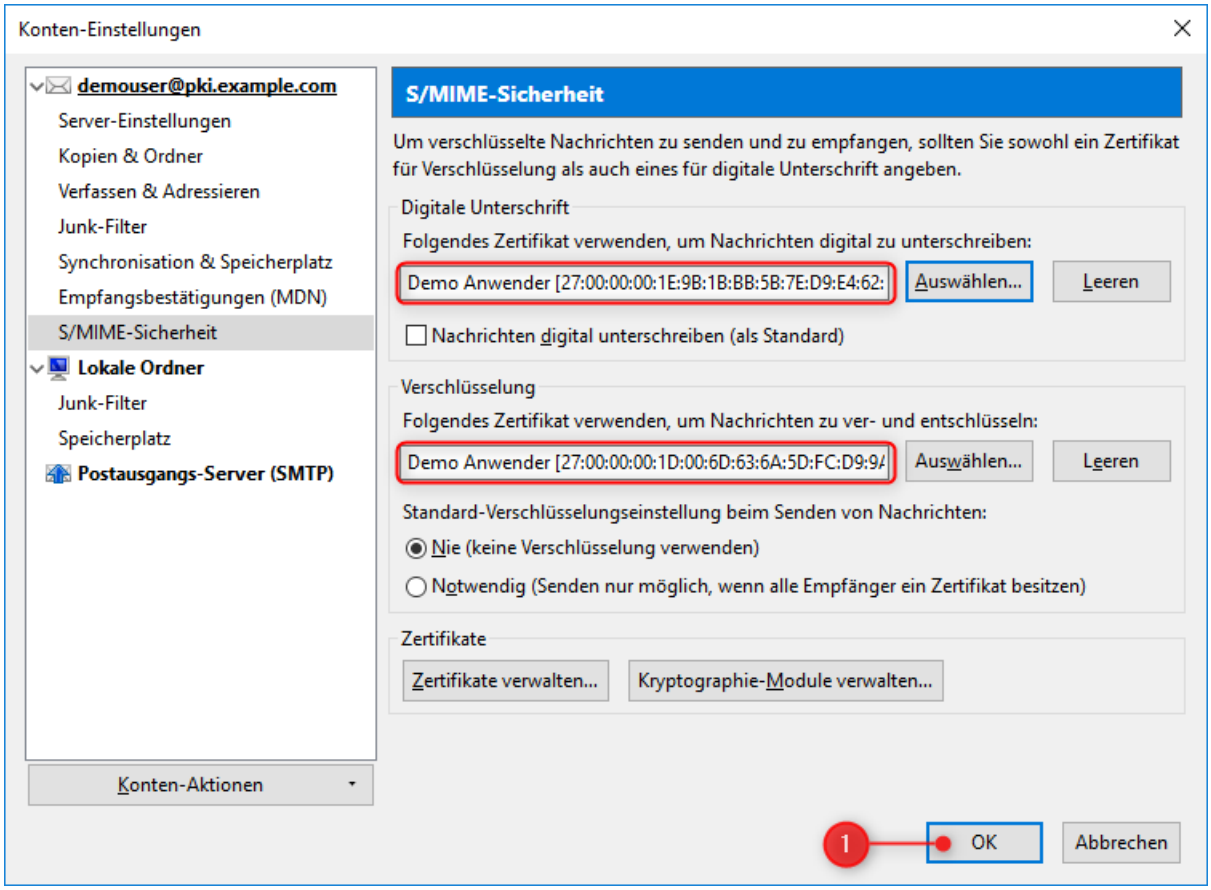


Abbildung 21 Auswahl der Zertifikate abschließen

Hinweis: Falls unter `Digitale Unterschrift` und/oder `Verschlüsselung` 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 oben in diesem Abschnitt 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).

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 Thunderbird deren Verschlüsselungszertifikate. Thunderbird 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 das Adressbuch in Thunderbird indem Sie zunächst auf den `Menüknopf` klicken und `Extras > Adressbuch` auswählen.
Hinweis: Alternativ können Sie das Adressbuch auch durch die Tastenkombination `Strg + Umschalt + B` öffnen.

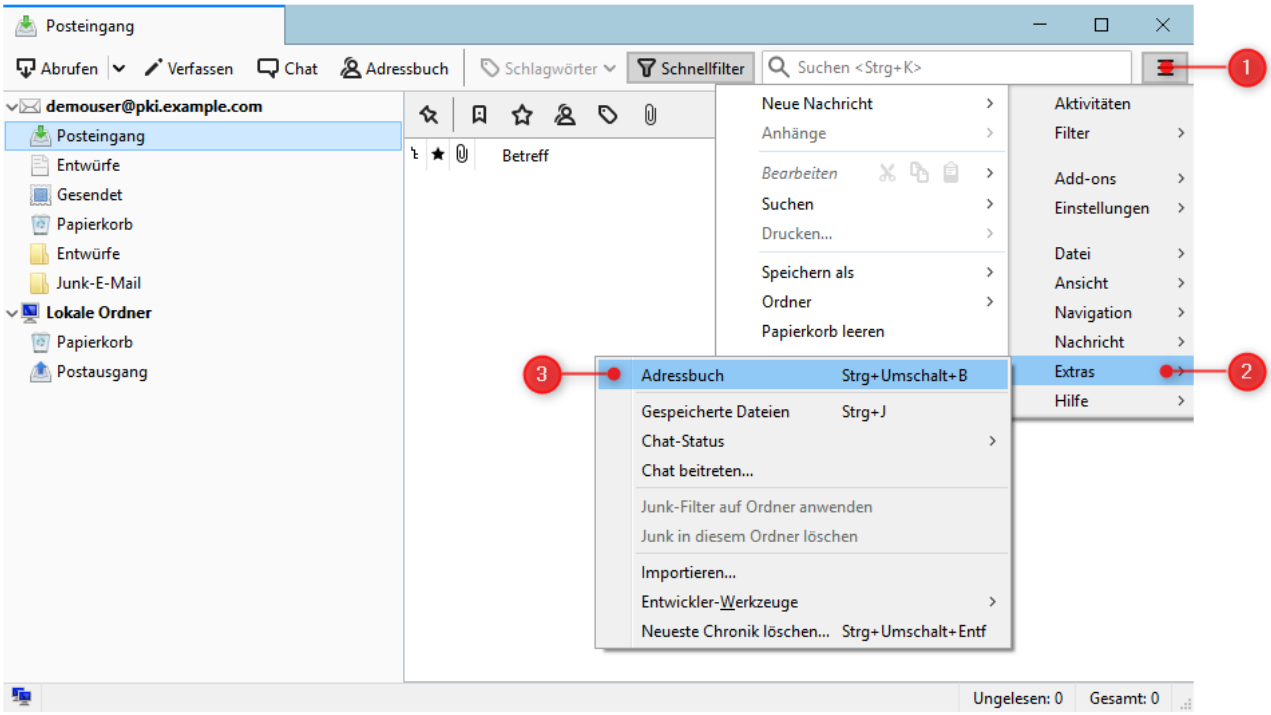


Abbildung 22 Aufrufen des Adressbuches

Im Adressbuch können Sie nun die Verbindung zum LDAP-Verzeichnis einrichten. Klicken Sie dazu auf `Datei > Neu > LDAP-Verzeichnis` um den Dialog zum Hinzufügen eines LDAP-Verzeichnisses zu öffnen.

Hinweis: Möglicherweise haben Sie 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 25), dann können Sie die restlichen Schritte in diesem Kapitel überspringen.

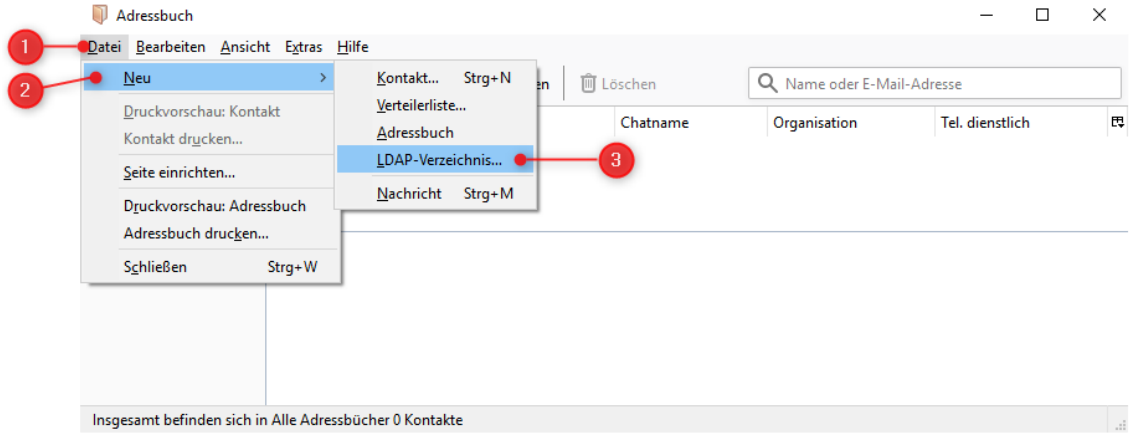


Abbildung 23 Hinzufügen eines LDAP-Verzeichnisses

Geben Sie in den Eigenschaften bei `Name` und `Serveradresse`

`directory.bybn.de`
bzw. für den externen Verzeichnisdienst `directory.bayern.de`

ein. Geben Sie als Wert bei Basis-DN

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

ein und setzen Sie das Häkchen bei `Verschlüsselte Verbindung (SSL) verwenden`. Schließen Sie das Eigenschaftenfenster mit `OK`.

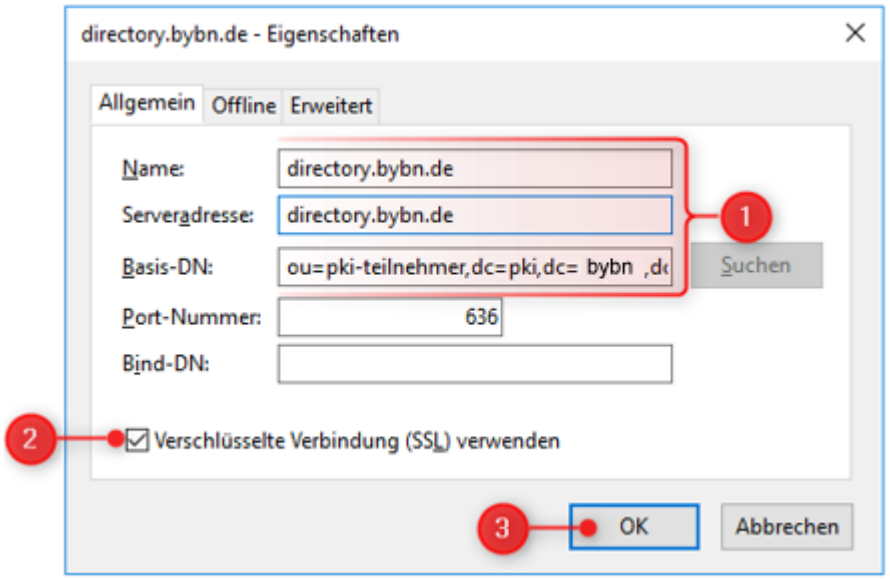


Abbildung 24 Einstellungen des LDAP-Verzeichnisses

Die Verbindung mit den Verzeichnisdiensten der Bayern-PKI ist nun eingerichtet. Überprüfen Sie ob der Verzeichnisdienst unter `Alle Adressbücher` angezeigt wird und schließen Sie das Adressbuch.

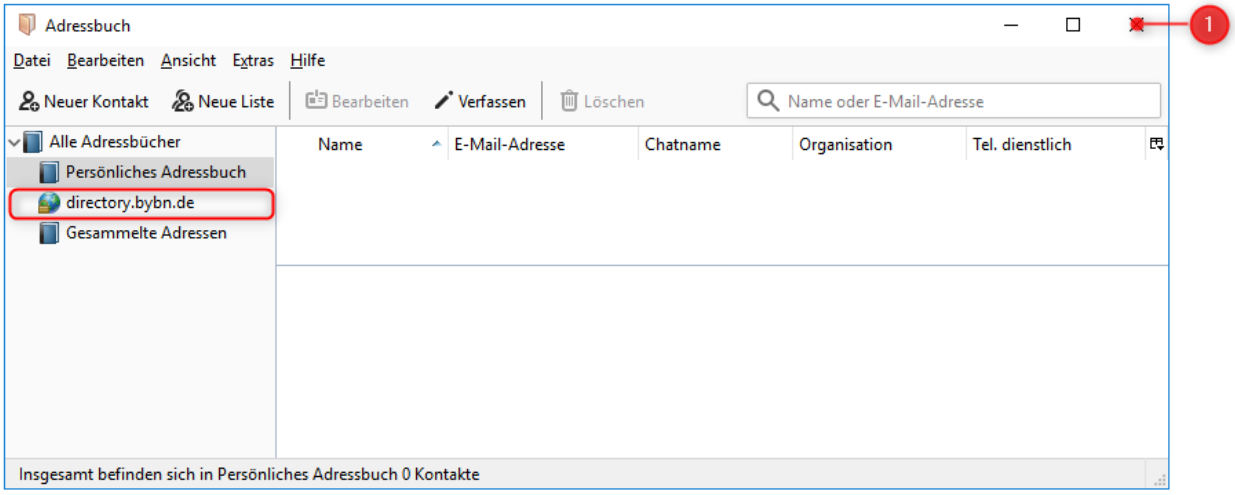


Abbildung 25 Adressbuch in Thunderbird

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 Thunderbird-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. Wie Sie Empfänger über den Verzeichnisdienst auswählen können, wird in diesem Kapitel beschrieben.

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.

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

3.1.1 Regelfall

Damit Sie verschlüsselte E-Mails senden können muss Thunderbird das Verschlüsselungszertifikat des Empfängers kennen. Wählen Sie den Empfänger daher immer über das LDAP-Verzeichnis aus, da dort bereits die Verschlüsselungszertifikate hinterlegt sind.

Erstellen Sie wie üblich eine neue E-Mail-Nachricht und blenden Sie im Fenster der gerade neu erstellten Nachricht die Kontakte-Sidebar mit einem Klick auf `Ansicht > Kontakte-Sidebar` ein.

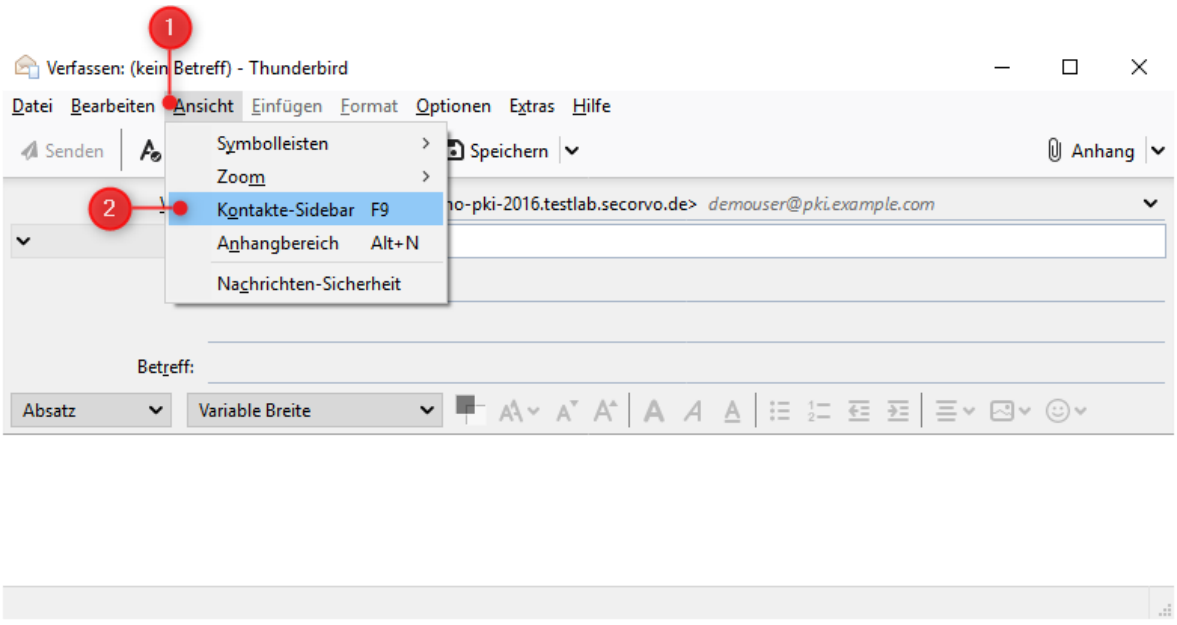


Abbildung 26 Einblenden der Kontakte-Sidebar

Wählen Sie unter `Adressbuch` das in 2.3 konfigurierte LDAP-Verzeichnis aus.

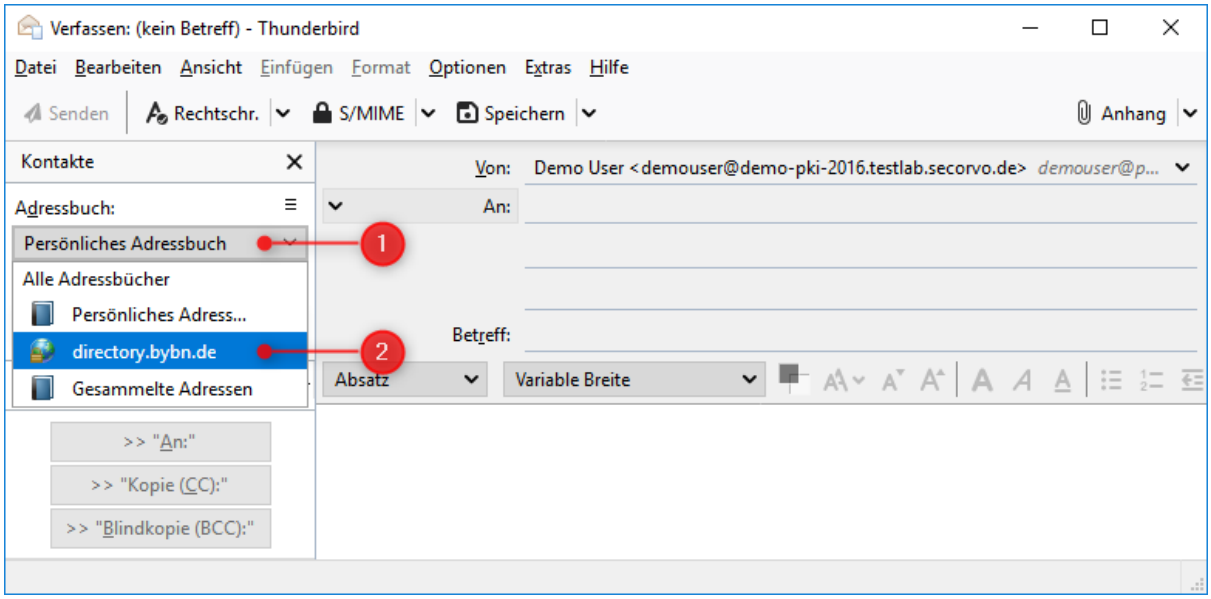


Abbildung 27 Auswählen des LDAP-Verzeichnisses als Adressbuch

Nun können Sie nach Kontakten suchen und den gewünschten Empfänger auswählen. Mit einem Klick auf `>> "An:"` können Sie den gewählten Kontakt als Empfänger zur E-Mail hinzufügen.

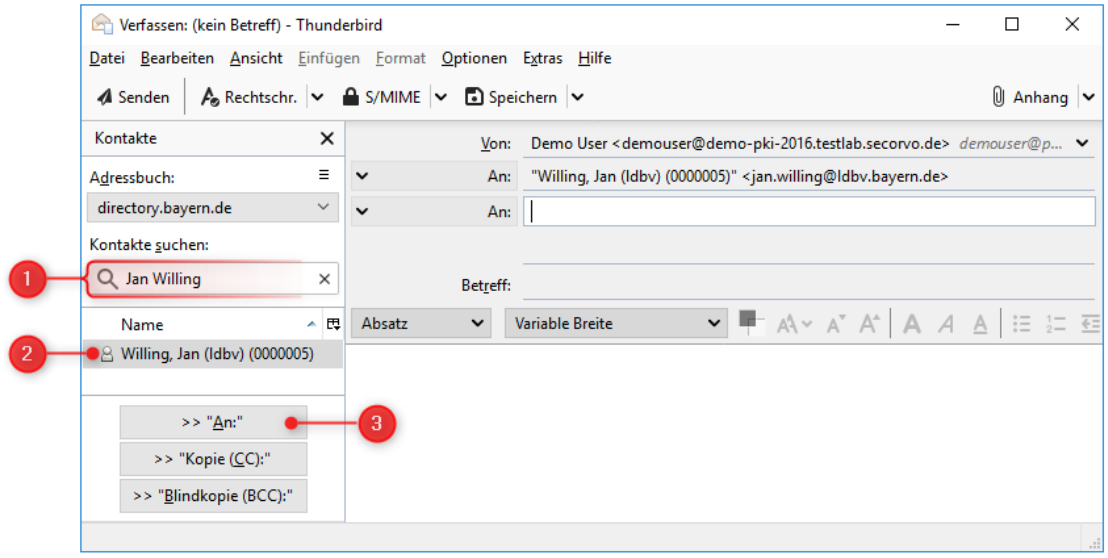


Abbildung 28 Suchen und Hinzufügen von Kontakten

Solange Sie diese E-Mail noch nicht gesendet haben, können Sie unter `S/MIME` über die beiden Menüpunkte für `Nachricht verschlüsseln` und `Nachricht unterschreiben` auswählen, ob und wie die E-Mail gesichert werden soll.

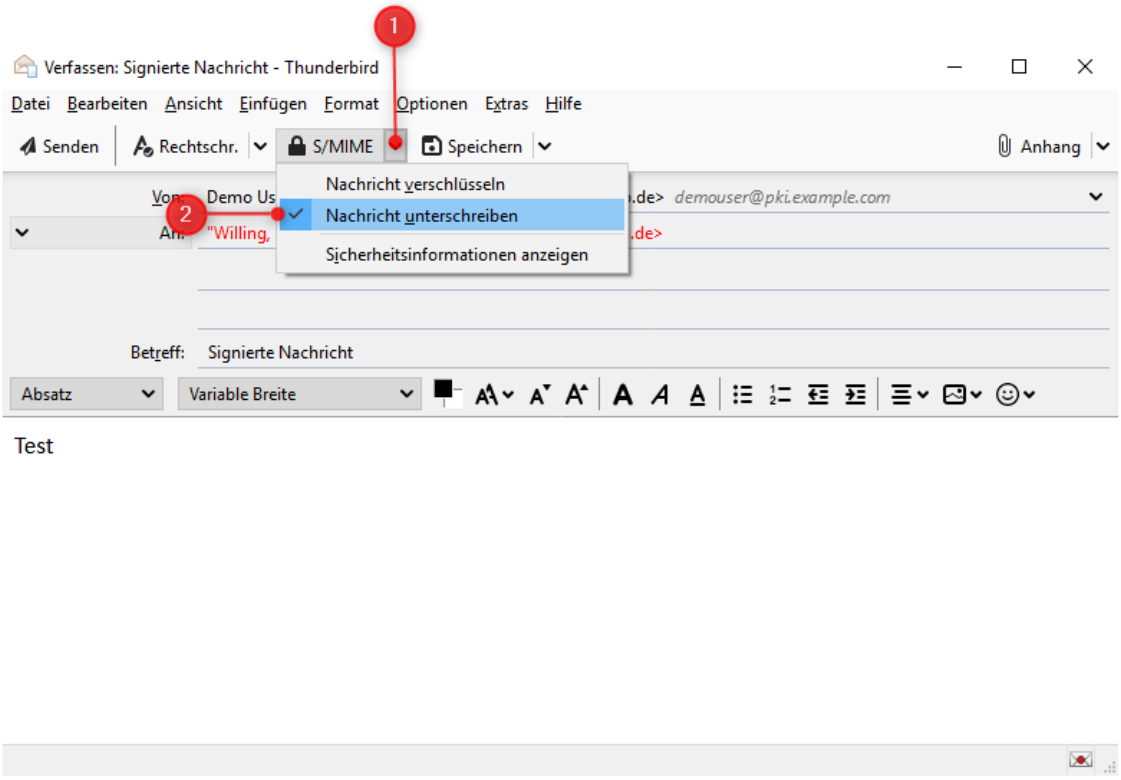


Abbildung 29 Auswahl der Sicherungsoptionen einer E-Mail

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

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.

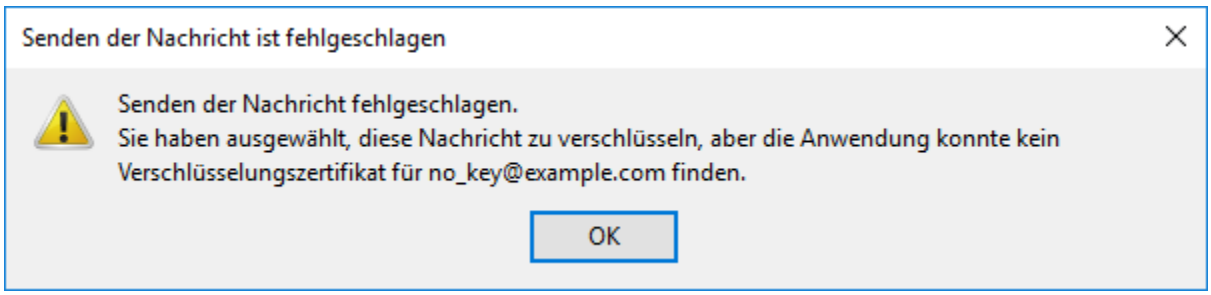


Abbildung 30 Senden einer Nachricht ohne Verschlüsselungszertifikat

Hinweis: E-Mails, die Sie verschlüsselt senden, werden auch für Sie als Absender verschlüsselt und so im Ausgangsportfach (`Gesendet` bzw. `Sent`) abgelegt. Beim Lesen selbst gesendeter verschlüsselter E-Mails gilt sinngemäß das gleiche wie unten für den Empfang von verschlüsselten E-Mails beschrieben.

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 Thunderbird importieren und für die Funktionsadresse einrichten.

Thunderbird 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 ist die Option `Nachricht verschlüsseln` bereits aktiviert; ggf. müssen Sie sie deaktivieren. Im Gegensatz dazu wird die Option `Nachricht unterschreiben` bei einer Antwort auf eine signierte E-Mail nicht übernommen.

Des Weiteren sind bei der Antwort auf eine E-Mail die Empfängerfelder bereits vorbelegt. Falls Thunderbird beim Senden der E-Mail nicht alle Verschlüsselungszertifikate findet (vgl. Abbildung 30), sollten Sie ggf. die vorbelegten Empfänger löschen und über das Adressbuch wieder neu hinzufügen, damit Thunderbird darüber die Verschlüsselungszertifikate empfangen kann.

Bei **Weiterleitungen** gilt das gleiche wie bei Antworten. Auch hier wird die Option `Nachricht verschlüsseln` bereits entsprechend der weitergeleiteten E-Mail aktiviert.

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

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

Der Empfang von verschlüsselten und/oder signierten E-Mail-Nachrichten funktioniert wie gewohnt und erfordert keine zusätzlichen Maßnahmen.

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 eines dieser zwei Symbole können Sie sich genauere Informationen zu der bei dieser E-Mail angebrachten Signatur bzw. Verschlüsselung anzeigen lassen.

Das Brief-und-Siegel-Symbol bedeutet, dass die E-Mail-Nachricht signiert wurde. Das Schloss-Symbol bedeutet, dass die E-Mail-Nachricht verschlüsselt wurde.

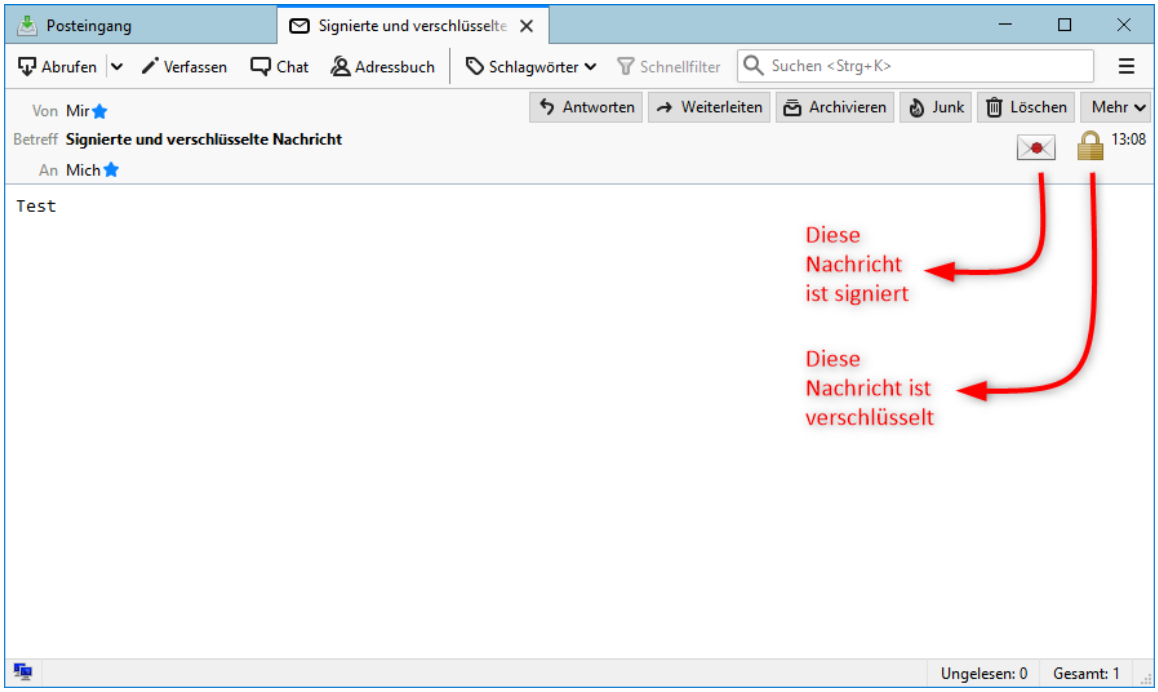


Abbildung 31 Kennzeichnung der Sicherungsoptionen einer Nachricht

4 Hinweise für den Administrator

4.1 Sperrstatus überprüfen

Seit Thunderbird 25 unterstützt die Software nur noch das Online Certificate Status Protocol (OCSP) zur Überprüfung des Sperrstatus eines Zertifikats. Die korrekte OCSP-Server-Adresse entnimmt Thunderbird dabei direkt aus den S/MIME-Zertifikaten der Bayern-PKI. Eine Konfiguration von Sperrlisten (CRLs) ist nicht möglich und nicht erforderlich.

4.2 Verteilen der Stammzertifikate

Die Stammzertifikate der Bayern-PKI werden beim Import der eigenen Zertifikate durch den Anwender bereits eingerichtet. Wenn die Stammzertifikate auch unabhängig davon in den Thunderbird-Clients vorhanden sein sollen, können diese auch zentral verteilt werden.

Thunderbird verwaltet eine eigene Liste vertrauenswürdiger Stammzertifikate und greift dabei nicht auf dem Zertifikatsspeicher des Betriebssystems zurück. Die Stammzertifikate werden in der Datei `cert9.db` im Profilordner des Thunderbird-Anwenders hinterlegt. Administratoren können die Stammzertifikate für die Thunderbird-Clients ausrollen, indem nach der Installation von Thunderbird diese Datei ausgetauscht wird.

Dazu ist zunächst eine Thunderbird-Installation einzurichten und die Stammzertifikate der Bayern-PKI dort zu importieren. Danach kann die Datei `cert9.db` unter

`%AppData%\Thunderbird\Profiles\<Präfix>.<Profil_Name>\cert9.db`

als Referenz verwendet und an einen anderen Speicherort kopiert werden.

Beim ersten Start von Thunderbird durch einen Benutzer wird ein neues E-Mai-Profil mit dem Namen `default` angelegt und ein zufälliges Präfix für den Ordnernamen gewählt, bspw. `votp3c8q`. Der Profil-Ordnername in diesem Beispiel wäre dementsprechend `votp3c8q.default`.

Diese Datei kann nun über einen Verteilmechanismus an die Clients ausgerollt werden. Dies sollte am besten direkt nach dem Anlegen des E-Mail Profils des Benutzers geschehen und nicht zu einem späteren Zeitpunkt, da in dieser Datei beim Import der Schlüsseldateien (vgl. Kapitel 2.2) auch die Signatur- und Verschlüsselungszertifikate des Anwenders gespeichert werden.

Hinweis: Die privaten Schlüssel der Anwender werden nicht in der Datei `cert9.db`, sondern in der separaten Datei `key4.db` abgelegt.

4.3 Zurücksetzen eines vergessenen Master-Passworts

Falls ein Benutzer sein Master-Passwort vergessen hat, kann es ggf. zurückgesetzt werden. Alle gespeicherten Passwörter sowie die Zertifikate und Schlüssel des Benutzers werden dabei gelöscht. Alle sonstigen Thunderbird-Einstellungen des Benutzers und dessen lokal gespeicherten E-Mails bleiben erhalten.

Zum Zurücksetzen muss nach dem Start von Thunderbird durch den betroffenen Benutzer wie folgt vorgegangen werden:

Bei der Frage nach dem Master-Passwort auf `Abbrechen` klicken.

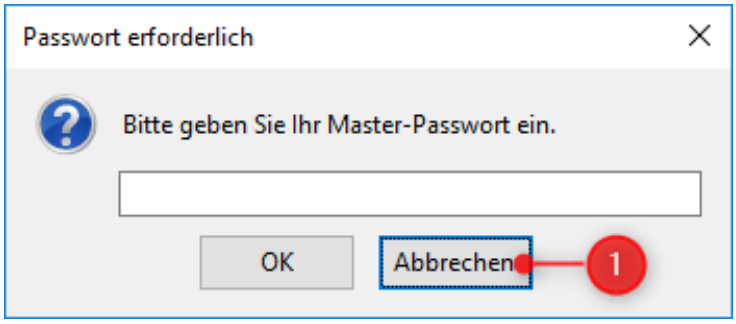


Abbildung 32 Abfrage des Master-Passwort in Thunderbird

Öffnen Sie über den `Menüknopf` > `Extras` > `Entwickler-Werkzeuge` > `Fehlerkonsole` die Fehlerkonsole.

Hinweis: Alternativ können Sie die Fehlerkonsole auch mit der Tastenkombination `Strg + Umschalt + J` öffnen.

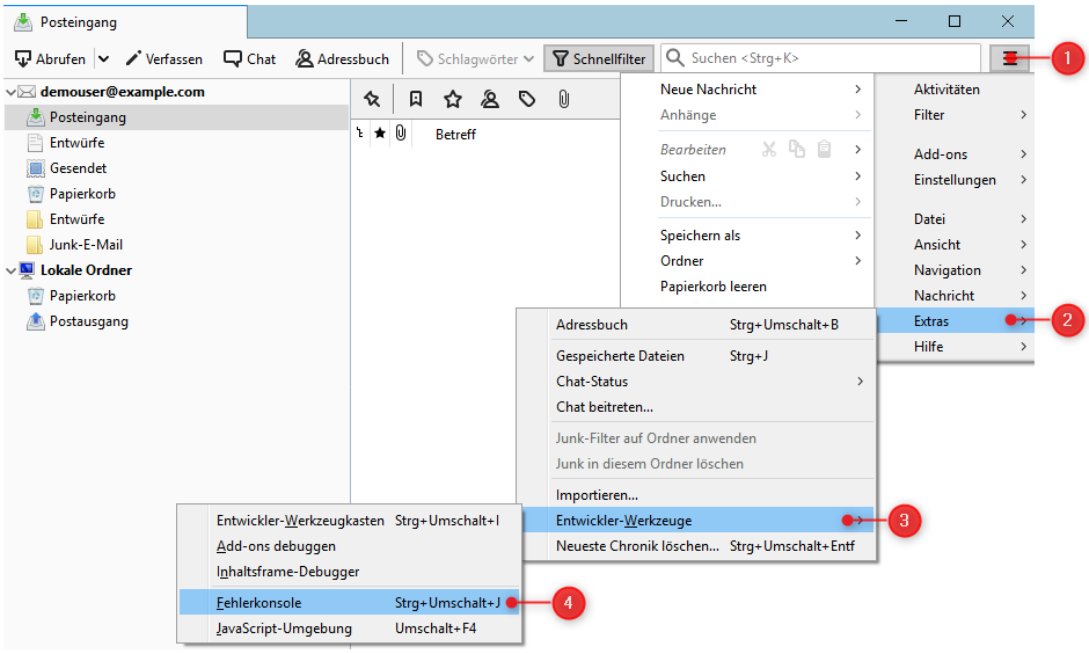


Abbildung 33 Öffnen der Fehlerkonsole in Thunderbird

Über die Eingabezeile am unteren Rand der Fehlerkonsole können Sie über den Befehl `openDialog("chrome://pippki/content/resetpassword.xul")` eingeben und mit der Eingabetaste bestätigen, um den Dialog zum Zurücksetzen des Master-Passworts zu öffnen.

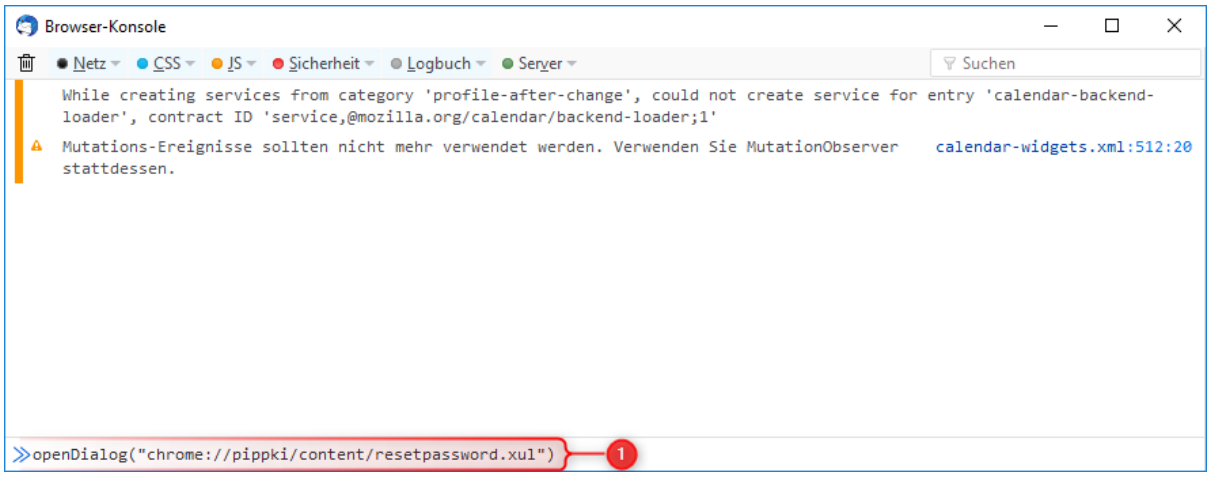


Abbildung 34 Befehl zum Öffnen des Dialogs um das Master-Passwort zurückzusetzen

Klicken Sie auf `Zurücksetzen` um das Master-Passwort zurückzusetzen. Dabei werden alle gespeicherten Kennwörter, Formulardaten, persönliche Zertifikate und private Schlüssel gelöscht.

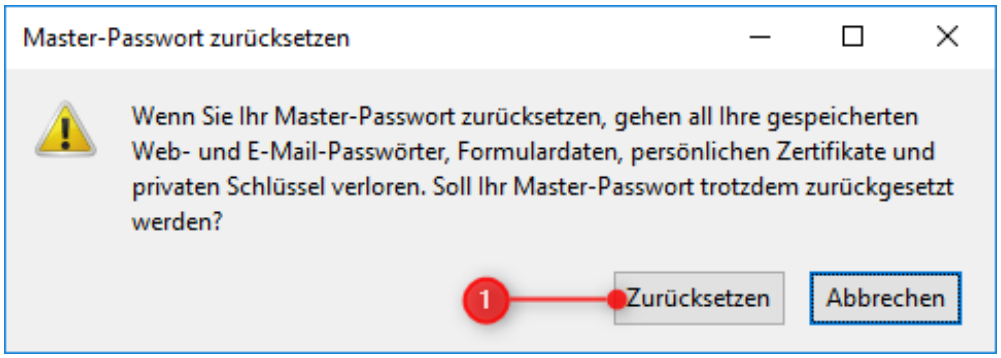


Abbildung 35 Dialog um das Master-Passwort zurückzusetzen

Bestätigen Sie den nachfolgenden Dialog mit `OK` um den Vorgang abzuschließen. Sie können die Fehlerkonsole schließen und Thunderbird nun neustarten.

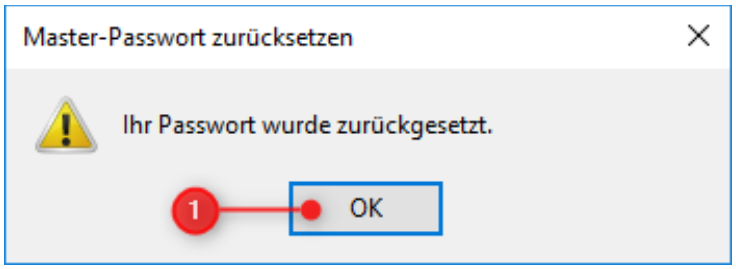


Abbildung 36 Bestätigung der Rücksetzung des Master-Passworts

Nach dem Neustart von Thunderbird muss der betroffene Benutzer wie in Kapitel 2.1 beschrieben ein neues Master-Passwort setzen und ggf. die Kennwörter der E-Mail Postfächer neu hinterlegen. Anschließend müssen die Zertifikate der Bayern-PKI erneut wie in Kapitel 2.2 beschrieben importiert werden.

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