Volksverschlüsselung®

Nutzung der Schlüssel/Zertifikate der Volksverschlüsselung

Informationen und Anleitungen für Endanwender

Levona Eckstein Jonathan Leppert Tatjana Rubinstein

1. Juni 2022

Inhaltsverzeichnis

Dokumenthistorie:

Version	*Datum*	*Beschreibung*
1.0	30.12.2016	Initiale Version
1.1	12.05.2022	Anpassung VV G02

1 Einleitung

Mit einem persönlichen Zertifikat der Volksverschlüsselung können Sie E-Mails und andere Daten digital signieren und/oder verschlüsseln sowie sich gegenüber Webseiten authentifizieren, die eine zertifikatsbasierte Client-Authentifizierung unterstützen.

In diesem Dokument finden Sie Informationen und Anleitungen, die Sie bei der Nutzung Ihres privaten Schlüssels und persönlichen Zertifikats der Volksverschlüsselung unter Windows in den E-Mail-Programmen und Web-Browsern unterstützen sollen. Außerdem wird beschrieben, wie Sie die Schlüssel/Zertifikate der Volksverschlüsselung auf andere Rechner verteilen können.

Für die Ausführungen in diesem Dokument setzen wir voraus, dass Ihnen ein Windows-System (Vista, Windows 7 oder neuer) zur Nutzung der Volksverschlüsselungs-Software zur Verfügung steht und Sie bereits ein Zertifikat der Volksverschlüsselung für Ihre E-Mail-Adresse besitzen.

Hinweis:
Das Dokument wird kontinuierlich fortgeschrieben. Wenn Sie Anmerkungen oder Verbesserungsvorschläge zum Dokument haben, schicken Sie uns bitte eine E-Mail an **info@volksverschluesselung.de**. Wir sind für jede Anregung dankbar.

2 Wozu kann ich meine Schlüssel/Zertifikate der Volksverschlüsselung verwenden?

Wenn Sie mittels der Volksverschlüsselungs-Software ein Zertifikat beantragen, erhalten Sie technisch gesehen für Ihre E-Mail-Adresse jeweils drei zusammenhängende X.509-Zertifikate für unterschiedliche Anwendungszwecke.

1. Mit dem **Verschlüsselungszertifikat** können Sie mit einem S/MIME-fähigen E-Mail-Programm Ihre E-Mail-Kommunikation oder andere Daten, wie beispielsweise PDF-Dokumente, verschlüsseln.
2. Mit dem **Signaturzertifikat** können Sie mit einem S/MIME-fähigen E-Mail-Programm Ihre E-Mails oder andere Daten, wie beispielsweise PDF-Dokumente, digital signieren.
3. Das **Authentifizierungszertifikat** kann in Browsern zur Anmeldung bei Diensten oder Web-Angeboten verwendet werden, sofern der Server nach einem persönlichen Zertifikat zur TLS-Client-Authentifizierung verlangt, zum Beispiel als Ergänzung oder als Ersatz zum herkömmlichen Login mit Benutzername und Passwort.

Im Kapitel Nutzung der Schlüssel/Zertifikate in S/MIME-fähigen E-Mail-Programmen wird das Signieren und Verschlüsseln einer E-Mail in S/MIME-fähigen

E-Mail-Programmen beschrieben, die von der Volksverschlüsselungs-Software unterstützt werden. Hier finden Sie auch Informationen, wie Sie die installierten Schlüssel/Zertifikate in Ihrem E-Mail-Programm überprüfen können. Das Kapitel Nutzung der Schlüssel/Zertifikate in Browsern enthält Informationen zur Verwendung der Schlüssel/Zertifikate in Chrome, Internet Explorer und Mozilla Firefox.

3 Nutzung der Schlüssel/Zertifikate in S/MIME-fähigen E-Mail-Programmen

Von der Volksverschlüsselungs-Software werden unter Windows verschiedene S/MIME-fähige E-Mail-Programme automatisch zur Nutzung der Schlüssel/Zertifikate konfiguriert. In diesem Kapitel wird das S/MIME-Verfahren zum Signieren und/oder Verschlüsseln von E-Mails und die Nutzung der Schlüssel/Zertifikate in den E-Mail-Programmen *Microsoft Office Outlook* und *Mozilla Thunderbird* beschrieben sowie Hilfestellungen im Umgang mit den Zertifikaten gegeben.

Da es von Outlook verschiedene Versionen gibt, konzentrieren sich die Ausführungen auf *Microsoft Office Outlook für Microsoft 365*. Anleitungen zu weiteren S/MIME-fähigen E-Mail-Programmen und anderen Outlook-Versionen finden Sie u.a. auf den Seiten der Universität Osnabrück Dort finden Sie auch Informationen zum Signieren und Verschlüsseln von E-Mails in Windows Live Mail.

3.1 So funktioniert S/MIME

Die Volksverschlüsselung stellt X.509 Zertifikate aus, die Sie für die sichere E-Mail-Kommunikation mittels S/MIME nutzen können. Das standardisierte Verfahren S/MIME erlaubt es, E-Mails auf zwei verschiedene Arten kryptographisch zu sichern. Mit S/MIME können E-Mails signiert und/oder Ende-zu-Ende verschlüsselt werden.

3.1.1 Signieren einer E-Mail

Durch das digitale Signieren einer E-Mail kann Ihr Kommunikationspartner überprüfen, ob der Inhalt der E-Mail auch tatsächlich von Ihnen stammt und bei der Übertragung nicht geändert wurde.

Wenn Sie eine E-Mail signieren, dann verwendet Ihr E-Mail-Programm hierfür den privaten Schlüssel zu Ihrem Signaturzertifikat, welcher beispielsweise von der Volksverschlüsselungs-Software in Ihrem E-Mail-Programm installiert wurde. Zunächst wird mittels einer Hashfunktion eine Prüfsumme über den Nachrichteninhalt erstellt. Diese wird dann mit dem privaten Schlüssel verschlüsselt. Die verschlüsselte Prüfsumme bildet dann die Signatur und wird an die E-Mail angehängt. Üblicherweise wird auch das Signaturzertifikat (genauer gesagt die gesamte Zertifizierungskette) an die signierte E-Mail angehängt.

Das E-Mail-Programm des Empfängers überprüft mit Hilfe des Signaturzertifikats des Senders die Gültigkeit der Signatur. Konkret bedeutet dies, dass die Signatur mit dem öffentlichen Schlüssel aus dem Signaturzertifikat entschlüsselt wird. Die enthaltene Prüfsumme wird dann mit der Prüfsumme verglichen, die vom Programm des Empfängers gebildet wurde. Die Signatur ist *gültig*, wenn die Prüfsummen übereinstimmen.

Der Empfänger muss zur Gültigkeitsprüfung auch alle zum Signaturzertifikat zugehörigen Zertifikate der übergeordneten Zertifizierungsstellen (CA-Zertifikate) in seinem E-Mail-Programm installiert haben. Anderenfalls wird das Signaturzertifikat als nicht vertrauenswürdig eingestuft und die Signatur als *ungültig* angezeigt. Ist der Empfänger Nutzer der Volksverschlüsselung und hat er sein E-Mail-Programm mit der Volksverschlüsselungs-Software konfiguriert, dann sind alle CA-Zertifikate der Volksverschlüsselung[1] bereits in seinem E-Mail-Programm installiert. Anderenfalls muss er die CA-Zertifikate manuell installieren, wie im Abschnitt *Installation der CA-Zertifikate der Volksverschlüsselung* unter Nutzung in Outlook für Microsoft 365 und Nutzung in Thunderbird beschrieben.

3.1.2 Ende-zu-Ende-Verschlüsseln einer E-Mail

Ende-zu-Ende-Verschlüsselung bedeutet, dass nur Sie und der Empfänger die verschlüsselte E-Mail lesen können und sichert Ihre E-Mail-Kommunikation damit gegen Kenntnisnahme durch unbefugte Dritte. Ende-zu-Ende-Verschlüsselung mittels S/MIME funktioniert nur, wenn sowohl Sender als auch Empfänger ein X.509-Zertifikat für S/MIME besitzen.

Wenn Sie eine E-Mail an einen Empfänger verschlüsselt senden möchten, benötigen Sie das **Verschlüsselungszertifikat des Empfängers**, denn die E-Mail wird mit dem öffentlichen Schlüssel des Empfängers verschlüsselt und auch nur dieser kann die E-Mail wieder entschlüsseln, da nur er den dazugehörigen privaten Schlüssel besitzt.

Wenn Sie eine E-Mail an mehrere Empfänger verschlüsselt senden möchten, ist es notwendig, dass Sie die Verschlüsselungszertifikate **aller** Empfänger kennen und in Ihrem E-Mail-Programm verfügbar sind.

Wie Sie das Zertifikat Ihres Empfängers erhalten, ist in Abschnitt Wie bekomme ich das Verschlüsselungszertifikat des Empfängers? beschrieben.

3.2 Was benötigt mein Kommunikationspartner, um mit mir vertraulich kommunizieren zu können?

Ihr Kommunikationspartner muss ebenfalls ein X.509-Zertifikat und ein S/MIME-fähiges E-Mail-Programm besitzen, wenn sie miteinander vertraulich kommunizieren möchten.

[1] https://volksverschluesselung.de/zertifikate.php

Besitzt ihr Kommunikationspartner ein Zertifikat der Volksverschlüsselung und hat er dieses im Verzeichnis der Volksverschlüsselung veröffentlicht, können Sie mit ihm i.d.R. sofort verschlüsselte E-Mails austauschen, wenn Sie Ihr E-Mail-Programm mit Hilfe der Volksverschlüsselungs-Software konfiguriert haben. Haben Sie oder ihr Kommunikationspartner das Zertifikat nicht veröffentlicht oder besitzt ihr Kommunikationspartner ein Zertifikat von einer anderen Zertifizierungsstelle, müssen zunächst die Zertifikate ausgetauscht werden. Verschiedene Möglichkeiten des Zertifikatsaustauschs sind im Abschnitt Wie bekomme ich das Verschlüsselungszertifikat des Empfängers? beschrieben.

3.3 Wie bekomme ich das Verschlüsselungszertifikat des Empfängers?

Wenn Sie E-Mails verschlüsselt versenden möchten, benötigen Sie, wie in Ende-zu-Ende-Verschlüsseln einer E-Mail beschrieben, das Verschlüsselungszertifikat des jeweiligen Empfängers.

Die Verschlüsselungszertifikate von Kommunikationspartnern, die ein Zertifikat der Volksverschlüsselung verwenden und dieses im Verzeichnisdienst der Volksverschlüsselung veröffentlicht haben, erhalten Sie automatisch, wenn Sie Ihr E-Mail-Programm mit der Volksverschlüsselungs-Software konfiguriert haben. In diesem Fall wird auch der Verzeichnisdienst der Volksverschlüsselung in Ihrem E-Mail-Programm eingerichtet und das E-Mail-Programm holt sich das Zertifikat automatisch aus dem Verzeichnis.

Anderenfalls stehen Ihnen folgende Möglichkeiten zur Verfügung, das Verschlüsselungszertifikat zu erhalten:

1. Zertifikatsaustausch mittels signierter E-Mail
   Sie tauschen mit Ihrem Kommunikationspartner eine signierte E-Mail aus, wie im Abschnitt *Austausch des Verschlüsselungszertifikats mittels signierter E-Mail* unter Nutzung in Outlook für Microsoft 365 und Nutzung in Thunderbird beschrieben.
2. Manuelle Konfiguration des Verzeichnisdienstes des Empfängers
   Möchten Sie den Verzeichnisdienst der Volksverschlüsselung ohne die Volksverschlüsselungs-Software nutzen oder hat Ihr Kommunikationspartner sein Zertifikat im Verzeichnisdienst einer anderen Zertifizierungsstelle veröffentlicht, können Sie für die automatische Zertifikatssuche in Outlook auch den Verzeichnisdienst manuell einrichten, wie in *Manuelle Konfiguration des Verzeichnisdienstes der Volksverschlüsselung* und *Manuelle Konfiguration des Verzeichnisdienstes einer fremden Zertifizierungsstelle* unter Nutzung in Outlook für Microsoft 365 und Nutzung in Thunderbird beschrieben.

3.4 Nutzung in Outlook für Microsoft 365

Diese Kapitel gibt Hilfestellungen bei der Verwendung der Schlüssel/Zertifikate der Volksverschlüsselung in *Microsoft Office Outlook für Microsoft 365* .

3.4.1 Voraussetzungen

Für die nachfolgenden Ausführungen setzen wir voraus, dass

1. Sie Outlook für Microsoft 365 auf Ihrem Rechner installiert und für Ihre E-Mail-Adresse ein Konto eingerichtet haben. Falls Sie beispielsweise ein Konto bei T-Online, GMX oder Web.de haben, so können Sie dieses auch in Outlook konfigurieren und verwenden. Anleitungen für das Einrichten eines E-Mail-Kontos in Outlook finden Sie bei Ihrem E-Mail-Anbieter.
2. Sie mit Hilfe der Volksverschlüsselungs-Software für die verwendete E-Mail-Adresse ein Zertifikat beantragt, heruntergeladen und Outlook für Microsoft 365 konfiguriert haben.
3. Ihr Kommunikationspartner ebenfalls ein S/MIME-fähiges E-Mail-Programm und ein Zertifikat der Volksverschlüsselung oder eines anderen Anbieters von S/MIME-Zertifikaten besitzt (vgl. Was benötigt mein Kommunikationspartner, um mit mir vertraulich kommunizieren zu können?).

3.4.2 Installation der CA-Zertifikate der Volksverschlüsselung

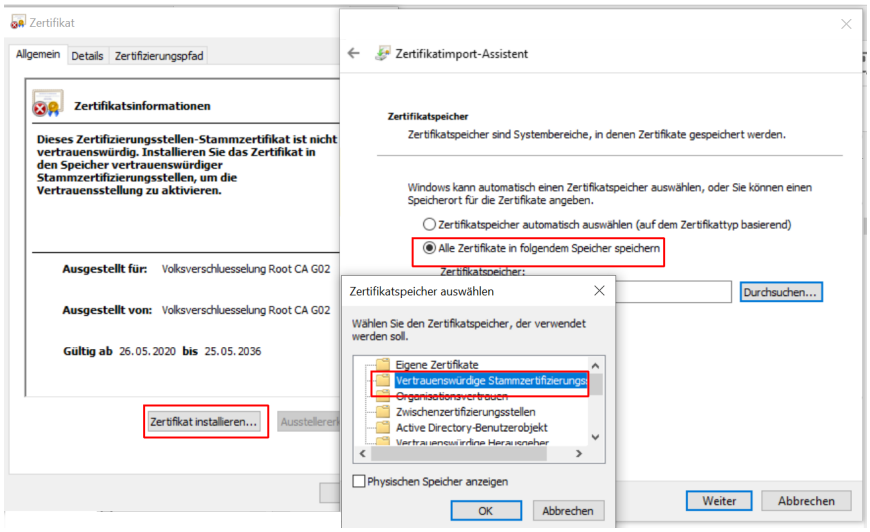
Um die Gültigkeit eines Zertifikats der Volksverschlüsselung prüfen zu können, muss die gesamte Zertifikatskette in Outlook installiert sein, d.h. das Wurzelzertifikat *Volksverschlüsselung Root-CA G02* und das Zertifikat der Private CA *Volksverschlüsselung Private-CA G02* müssen Outlook bekannt sein. Wenn Sie die Volksverschlüsselungs-Software zur Konfiguration Ihrer Anwendung verwenden, werden diese Zertifikate automatisch installiert.

Falls Sie die Volksverschlüsselungs-Software nicht verwenden wollen/können, dann müssen Sie die Zertifikate manuell importieren. Laden Sie hierzu die Zertifikate im Binärformat (DER) von der Webseite `https://volksverschluesselung.de/zertifikate.php` herunter und binden Sie sie wie folgt in Outlook ein.

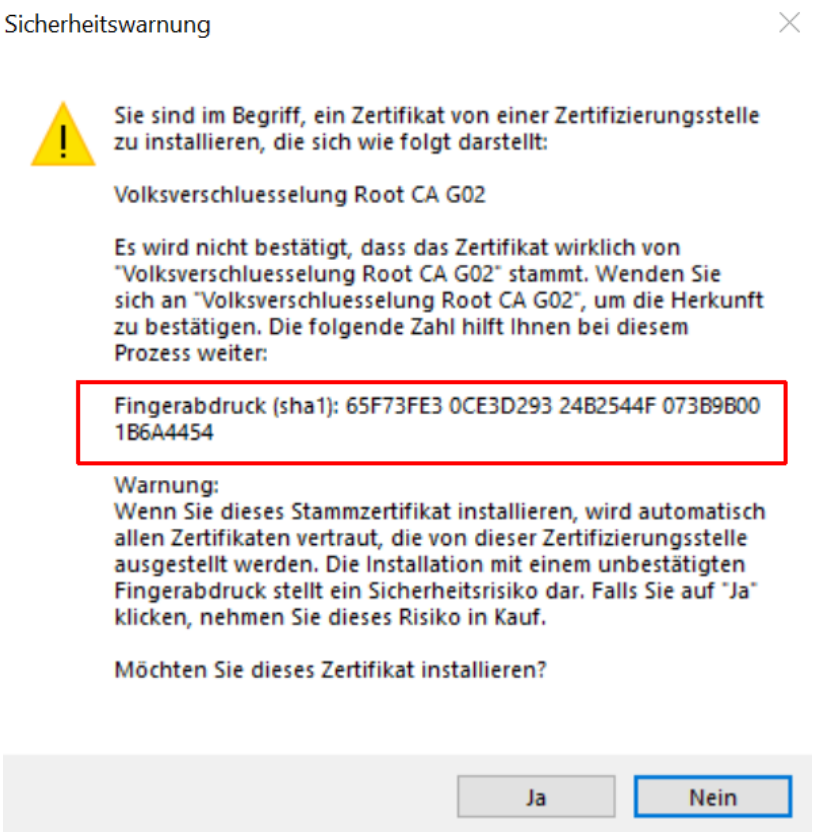
Import des Wurzelzertifikats

1. Klicken Sie mit der linken Maustaste auf die Zertifikatsdatei *VV-Root-G02-CA.der*.
2. Es öffnet sich ein Fenster *Datei öffnen - Sicherheitswarnung*. Klicken Sie auf **Öffnen**.
3. Es öffnet sich das Fenster *Zertifikat*. Klicken Sie auf **Zertifikat Installieren**.
4. Es öffnet sich der Zertifikatsimport-Assistent. Klicken Sie auf **Weiter**.

5. Klicken Sie auf **Alle Zertifikate in folgendem Speicher speichern** und wählen Sie **Vertrauenswürdige Stammzertifizierungsstellen**.

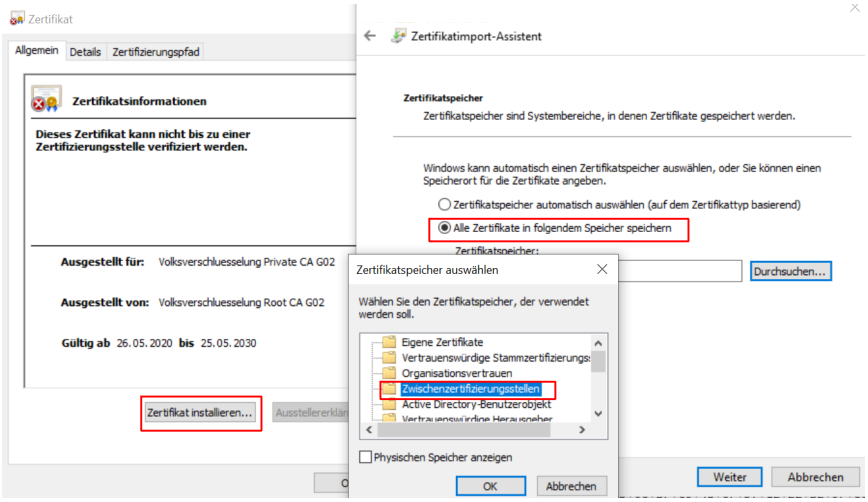


6. Klicken Sie auf **Weiter** und dann auf **Fertig stellen**. Es erscheint eine *Sicherheitswarnung*, denn Sie legen durch den Import des Wurzelzertifikats fest, dass Sie allen von dieser Zertifizierungsstelle ausgestellten Zertifikaten vertrauen wollen. Sie sollten hier den Fingerabdruck (SHA1 Prüfsumme) mit dem publizierten Fingerabdruck auf unserer Webseite vergleichen. Klicken Sie auf **Ja**, um das Zertifikat zu importieren.



Import des Zertifikats der Volksverschluesselung Private CA

1. Klicken Sie mit der linken Maustaste auf die Zertifikatsdatei *VV-Private-User-G02-CA.der* und führen Sie die Schritte 2 bis 4 wie zuvor beschrieben aus.
2. Klicken Sie auf **Alle Zertifikate in folgendem Speicher speichern** und wählen Sie **Zwischenzertifizierungsstellen**.



3. Klicken Sie auf **Weiter** und dann auf **Fertig stellen**.

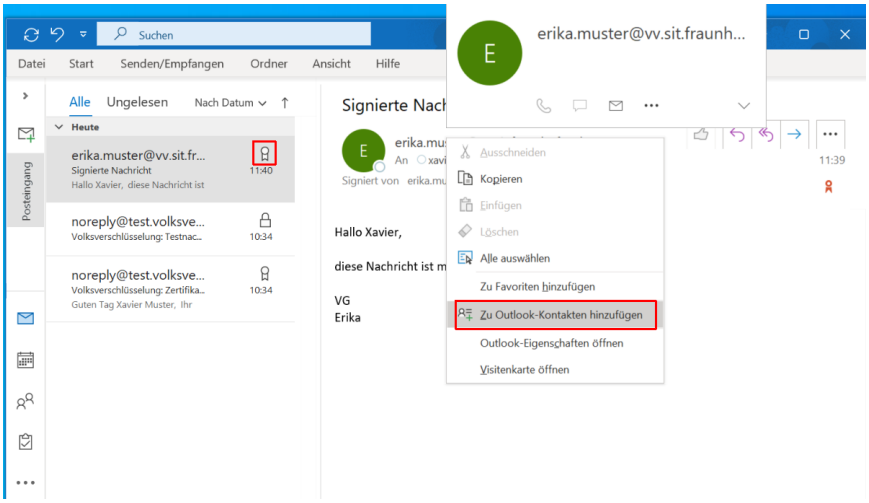
3.4.3 Austausch des Verschlüsselungszertifikats mittels signierter E-Mail

Eine einfache Möglichkeit sein Verschlüsselungszertifikat verfügbar zu machen, besteht darin, dem Kommunikationspartner eine signierte E-Mail zu senden. Bei einer signierten E-Mail wird i. d. R. auch das Verschlüsselungszertifikat des Absenders mitgesendet und dem E-Mail-Programm auf Empfängerseite bekannt gemacht.

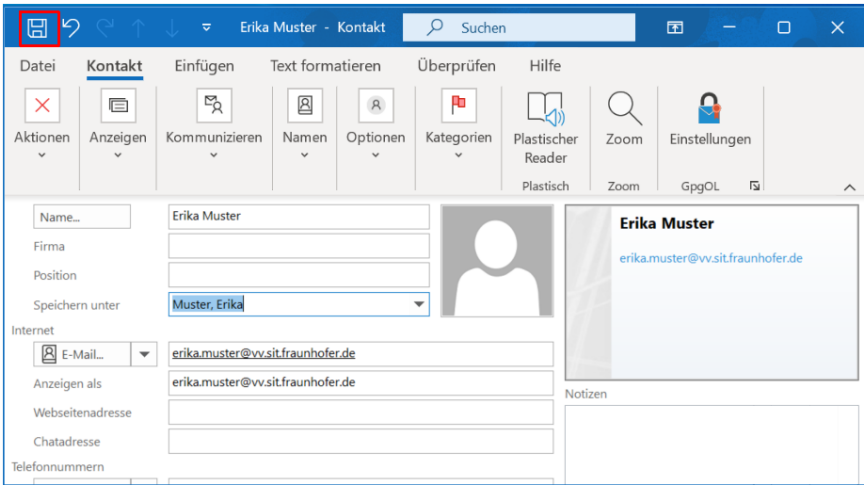
Hinweis: Im E-Mail-Programm des Empfängers der signierten Nachricht muss die Zertifikatskette der Volksverschlüsselung installiert sein, damit die Gültigkeit der Signatur überprüft werden kann. Falls der Empfänger die Volksverschlüsselungs-Software nicht verwendet, muss er die Zertifikate *Volksverschluesselung Root-CA G02* und *Volksverschluesselung Private-CA G02* manuell installieren, wie in Installation der CA-Zertifikate der Volksverschlüsselung beschrieben.

Gehen Sie bei Empfang der signierten E-Mail wie folgt vor:

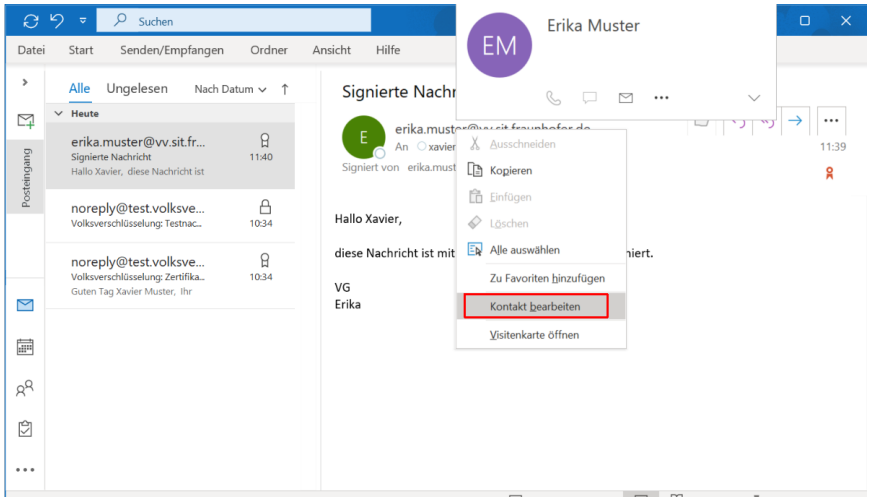
1. Öffnen Sie die signierte E-Mail von Ihrem Kommunikationspartner und fügen Sie die Adresse des Absenders zu Ihren Outlook-Kontakten hinzu. Gehen Sie hierzu auf die E-Mail-Adresse und drücken Sie die rechte Maustaste. Aus dem Kontextmenü wählen Sie **Outlook-Kontakten hinzufügen**.



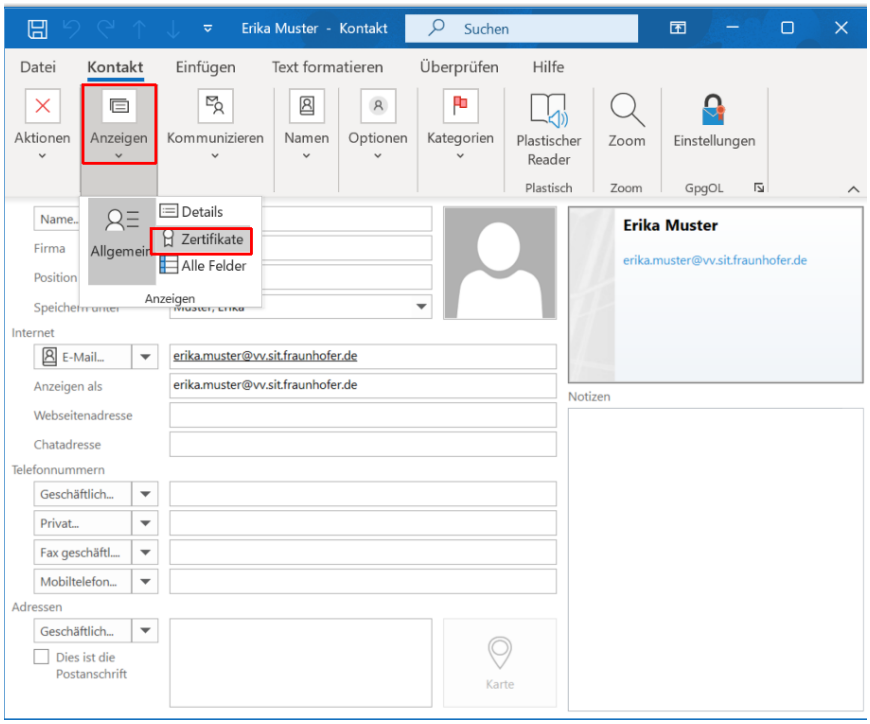
2. Der Kontakt wird angezeigt. Klicken Sie auf **Speichern**, um den Kontakt hinzuzufügen. Das Verschlüsselungszertifikat wird dabei automatisch mitgespeichert.



3. Sie können überprüfen, ob das Zertifikat auch tatsächlich gespeichert wurde. Gehen Sie hierzu auf die E-Mail-Adresse und drücken Sie die rechte Maustaste. Aus dem Kontextmenü wählen Sie **Kontakt bearbeiten**.



4. Wählen Sie nun **Anzeigen->Zertifikate**. Im Zertifikatsfenster sehen Sie das Zertifikat. Mit einem Doppelklick wird Ihnen das Zertifikat angezeigt.



3.4.4 Manuelle Konfiguration des Verzeichnisdienstes der Volksverschlüsselung

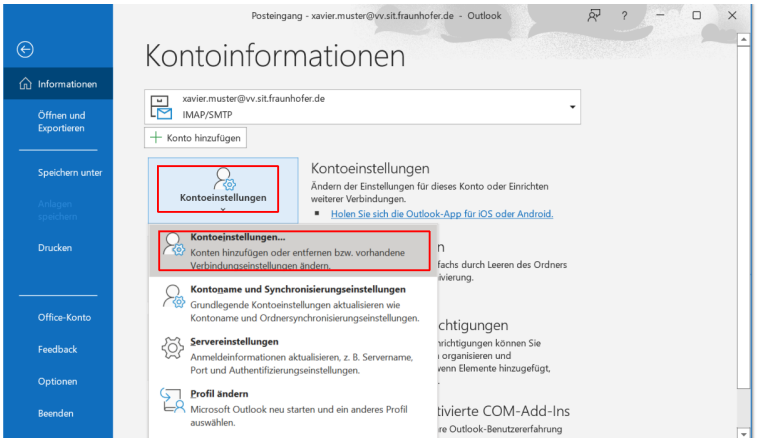
Die Volksverschlüsselung bietet einen öffentlichen LDAP (Lightweight Directory Access Protocol) Verzeichnisdienst an, in dem die Verschlüsselungszertifikate der Nutzer der Volksverschlüsselung veröffentlicht werden, sofern sie bei der Zertifikatsbeantragung hierzu ihre Einwilligung erteilt haben. Wenn der Verzeichnisdienst in Outlook für Microsoft 365 konfiguriert ist und der Kommunikationspartner sein Zertifikat im

Verzeichnisdienst der Volksverschlüsselung veröffentlicht hat, wird bei Eingabe seiner E-Mail-Adresse automatisch dessen Verschlüsselungszertifikat ausgewählt.

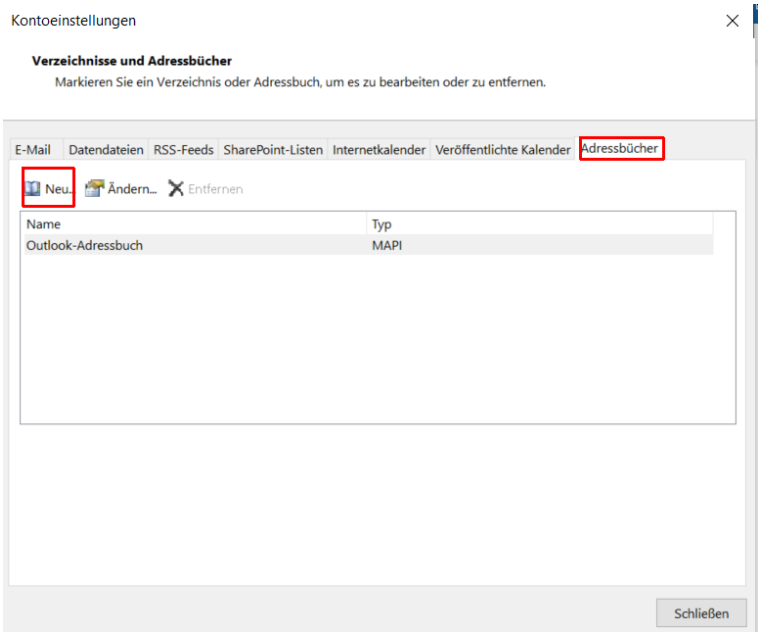
Wenn Sie die Volksverschlüsselungs-Software nicht verwenden, können Sie den Verzeichnisdienst der Volksverschlüsselung auch manuell konfigurieren, indem Sie ein neues Adressbuch einrichten. Hierfür benötigen Sie den Hostname, die Portnummer und den Basis-DN. Die Konfigurationsparameter des Verzeichnisdienstes der Volksverschlüsselung finden Sie auf unserer Webseite.

So richten Sie den Verzeichnisdienst der Volksverschlüsselung in Outlook für Microsoft 365 ein :

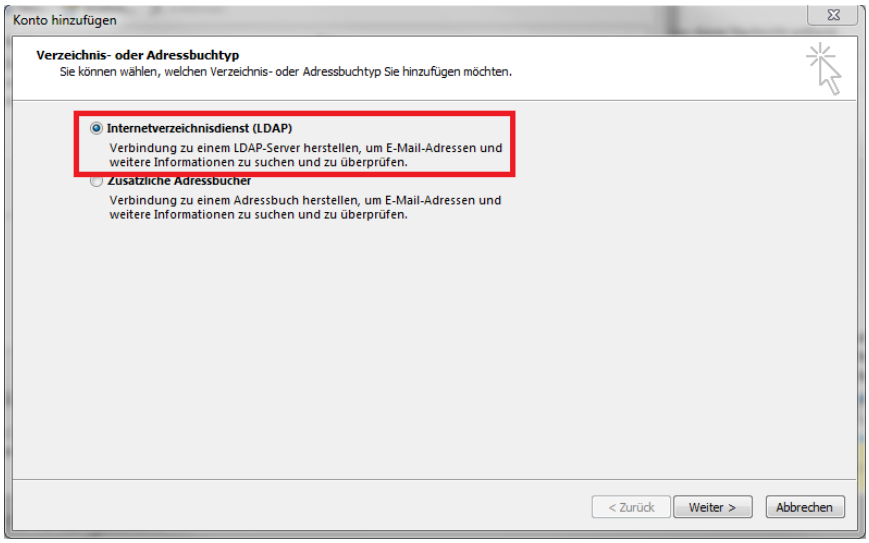
1. Öffnen Sie ihre Kontoeinstellungen, indem Sie in Outlook auf **Datei->Kontoeinstellungen->Kontoeinstellungen** klicken



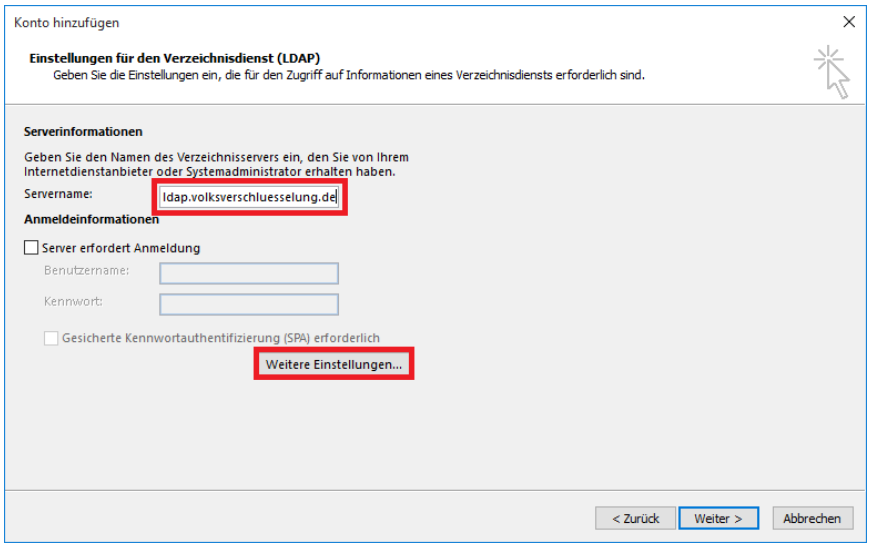
2. Es erscheint das Fenster *Kontoeinstellungen*. Wählen Sie **Adressbücher** und dann **Neu**.



3. Wählen Sie **Internetverzeichnis (LDAP)**.

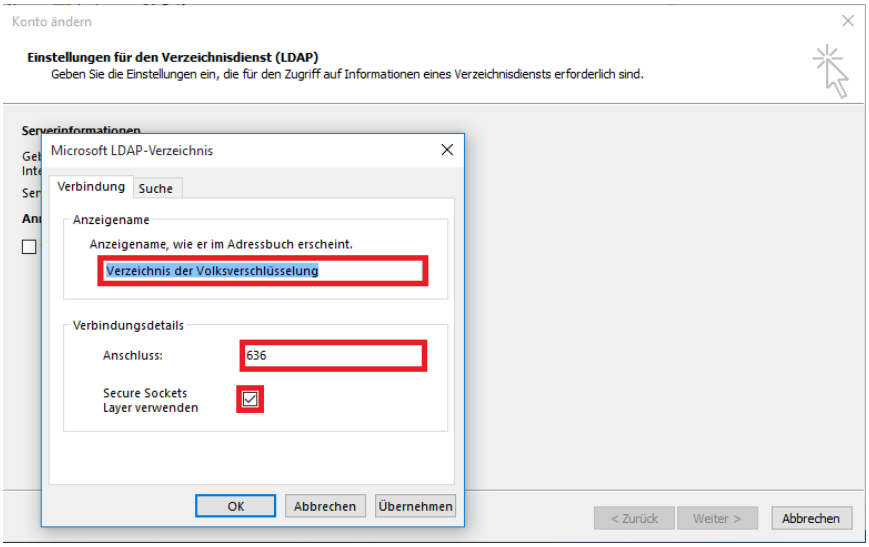


4. Geben Sie als Servername **ldap.volksverschluesselung.de** ein und gehen Sie auf **Weitere Einstellungen...**.



5. Tragen Sie die Konfigurationsdaten wie folgt in die Felder ein:

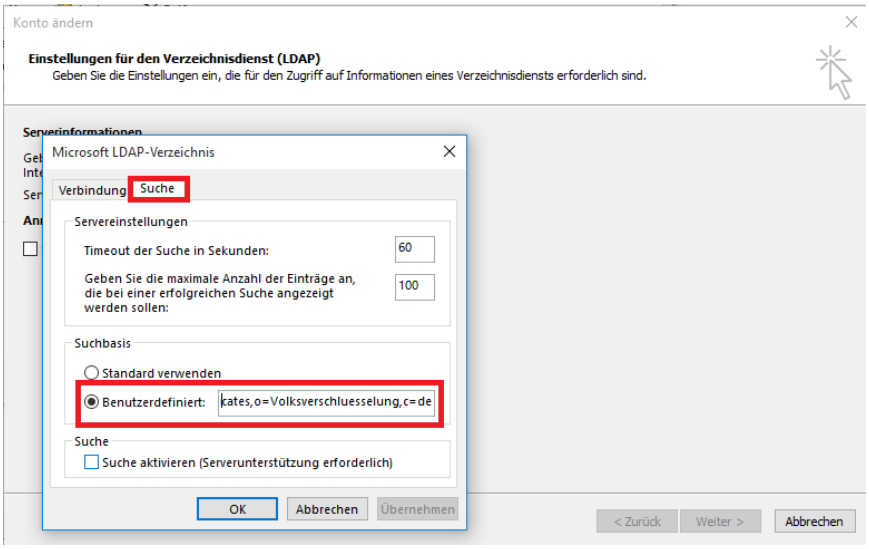
   - Anzeigename: Verzeichnis der Volksverschlüsselung (frei wählbar)
   - Anschluss: **636**
   - Setzen Sie ein Häkchen bei *Secure Sockets Layer verwenden*



6. Wechseln Sie auf den Karteireiter **Suche**

   - Wählen Sie **Suchbasis Benutzerdefiniert** und geben Sie folgenden Wert ein **ou=Certificates,o=Volksverschluesselung,c=de**

   - Bestätigen Sie mit **OK**



3.4.5 Manuelle Konfiguration des Verzeichnisdienstes einer fremden Zertifizierungsstelle

Hat Ihr Kommunikationspartner sein Zertifikat in einem Verzeichnisdienst eines anderen Zertifizierungsanbieters veröffentlicht, dann bitten Sie ihn, Ihnen die Konfigurationsdaten zu nennen: Hostname, Portnummer (mit/ohne SSL/TLS) und Basis-DN.

Wenn Ihnen die Konfigurationsdaten bekannt sind, können Sie den Verzeichnisdienst, wie im vorherigen Abschnitt beschrieben, in Outlook für Microsoft 365 einrichten.

3.4.6 Senden einer verschlüsselten E-Mail

Im Folgenden wird eine Möglichkeit beschrieben, wie Sie eine E-Mail für Ihren Kommunikationspartner in Outlook für Microsoft 365 verschlüsseln können.

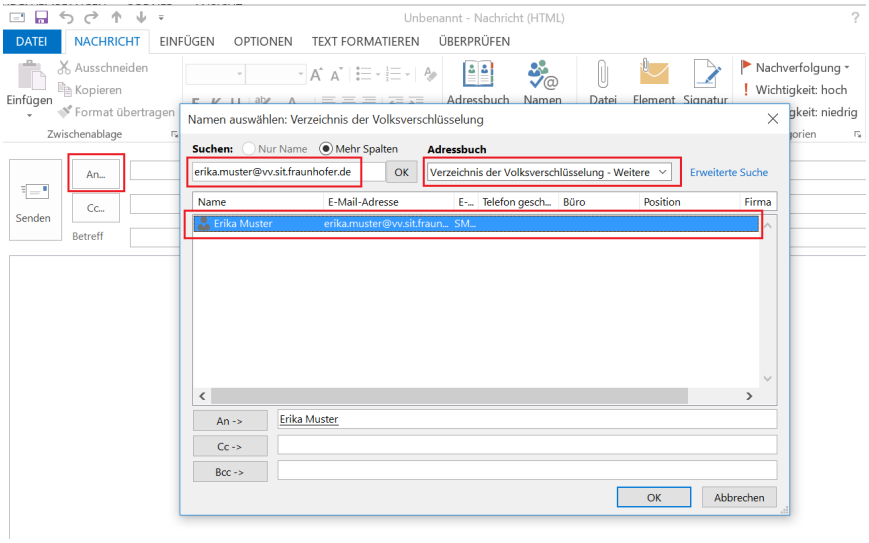
Im folgenden Beispiel wird davon ausgegangen, dass Ihr Kommunikationspartner ebenfalls ein Zertifikat der Volksverschlüsselung besitzt und dieses im Verzeichnis der Volksverschlüsselung veröffentlicht hat. In diesem Fall holt sich Outlook das Zertifikat *automatisch* aus dem konfigurierten Verzeichnisdienst der Volksverschlüsselung.

Für die Kommunikation mit einem Kommunikationspartner, dessen Zertifikat Sie noch nicht kennen, müssen Sie zuerst sein Zertifikat in Ihrem E-Mail-Programm verfügbar machen, wie in den vorhergehenden Abschnitten beschrieben.

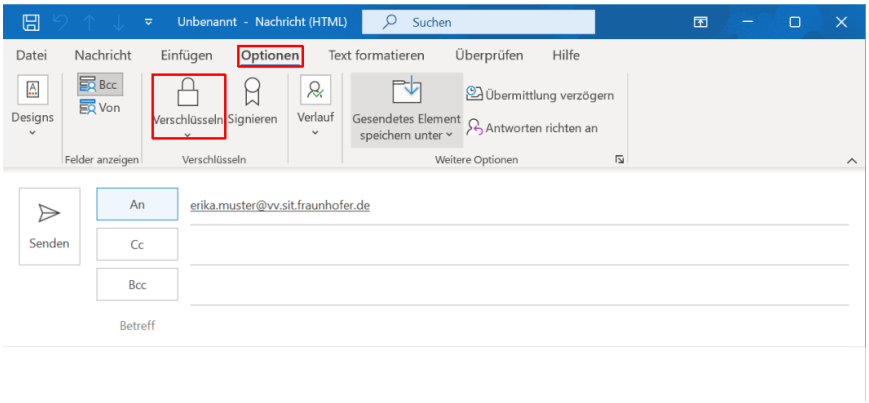
In Ihrem Ordner, in dem Ihre gesendeten E-Mails abgespeichert werden, können Sie eine verschlüsselte Nachricht an dem “Schloss-Symbol” erkennen. Jede verschlüsselte E-Mail wird auch mit Ihrem **Verschlüsselungszertifikat** verschlüsselt und in diesem Ordner abgelegt. Wenn Sie auf das Schloss-Symbol klicken, dann auf **Verschlüsselungsschicht->Details** anzeigen und dann auf **Zertifikat anzeigen**, sehen Sie Ihr Verschlüsselungszertifikat.

1. Suchen Sie die E-Mail-Adresse Ihres Kommunikationspartners im Verzeichnis der Volksverschlüsselung:

   - Wählen Sie **Neue Nachricht** und klicken Sie auf **An...**; es erscheint das Fenster *Namen auswählen. ….*
   - Wählen Sie unter **Adressbuch** das **Verzeichnis der Volksverschlüsselung**.
   - Geben Sie im Feld **Suche** die **vollständige E-Mail-Adresse** ein, klicken Sie auf **OK** und wählen Sie die Adresse mit einem **Doppelklick** aus.

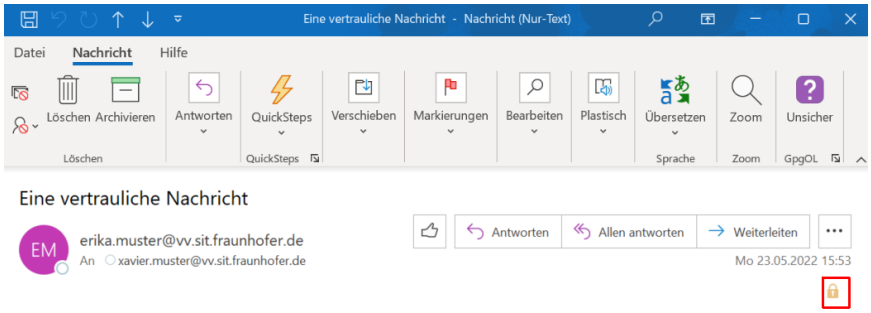


2. Nachdem Sie Ihre E-Mail verfasst haben, klicken Sie auf **Optionen**, dann auf das Icon mit der Beschriftung **Verschlüsseln** und schicken Sie anschließend Ihre E-Mail ab.



3.4.7 Empfang einer verschlüsselten E-Mail

Wenn Sie eine verschlüsselte E-Mail empfangen, wird diese automatisch beim Öffnen entschlüsselt, vorausgesetzt der private Schlüssel ist in Outlook für Microsoft 365 konfiguriert. Andernfalls erhalten Sie die Meldung: "“**Das Element kann im Lesebereich nicht angezeigt werden. Öffnen Sie das Element, um den Inhalt zu lesen**”". Das **Schloss-Symbol** zeigt an, dass die E-Mail vom Absender (hier: Erika Muster) verschlüsselt wurde.

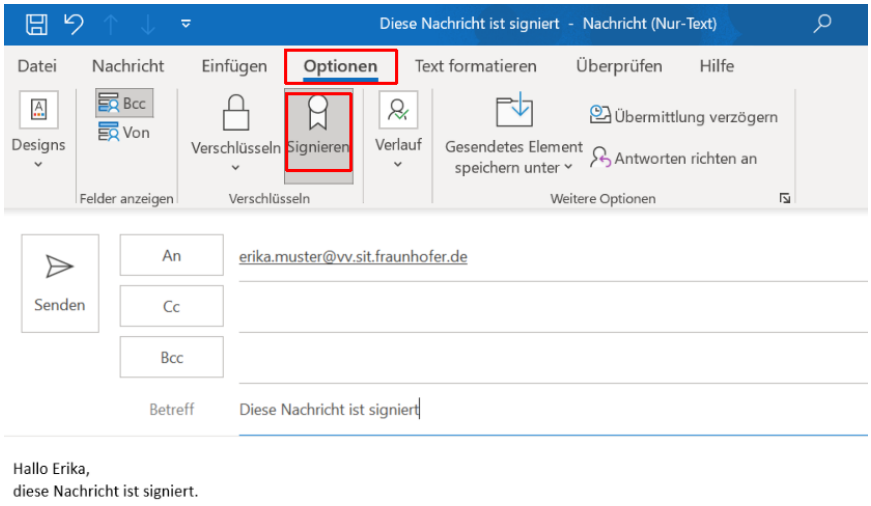


3.4.8 Senden einer signierten E-Mail

Für das Signieren Ihrer E-Mail wird Ihr privater Schlüssel zu Ihrem Signaturzertifikat verwendet, welcher von der Volksverschlüsselungs-Software bereits in Ihrem Outlook installiert wurde.

In Ihrem Ordner, in dem Ihre gesendeten E-Mails abgespeichert werden, können Sie eine signierte Nachricht an dem **Siegel-Symbol** erkennen.

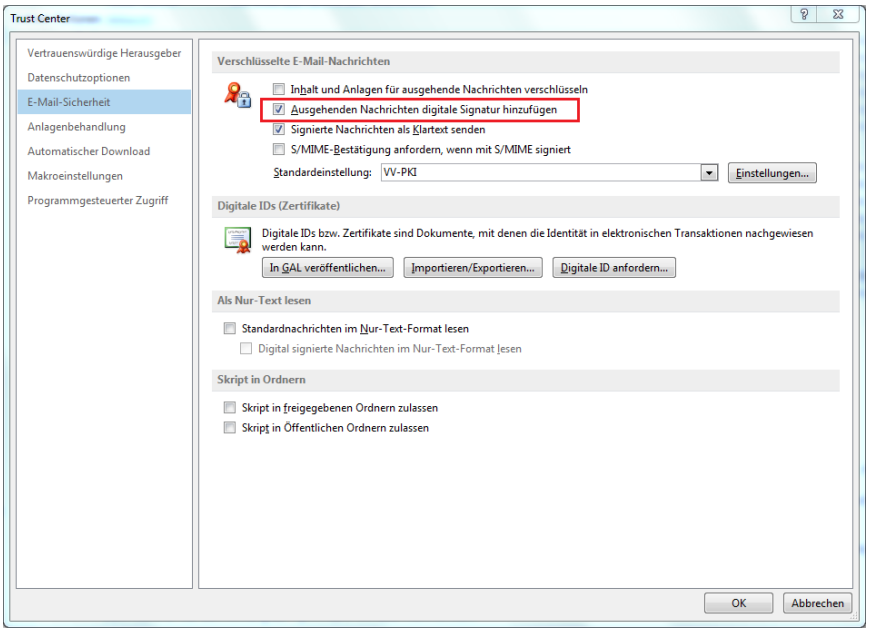
Nachdem Sie Ihre E-Mail verfasst haben, klicken Sie unter **Optionen** auf das Icon mit der Beschriftung **Signieren** und schicken anschließend über **Senden** Ihre E-Mail ab.



Hinweise: Sie können Outlook für Microsoft 365 so konfigurieren, dass jede neue E-Mail standardmäßig signiert wird. Außerdem sollten Sie signierte Nachrichten immer im Klartext versenden, damit auch Empfänger ohne S/MIME-Sicherheit die Nachricht lesen können. In Outlook ist dieses Kontrollkästchen standardmäßig aktiviert. Sie können die Einstellungen wie folgt vornehmen:

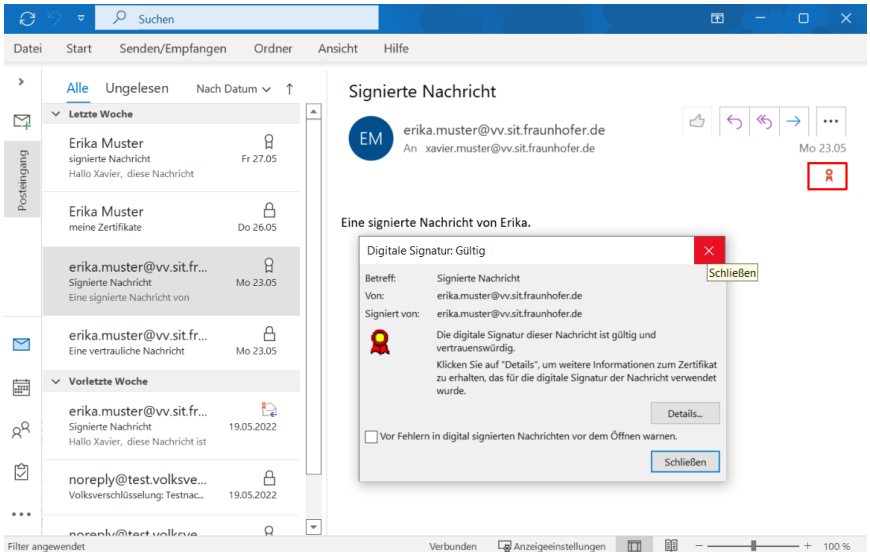
1. Wählen Sie **Datei** und dann **Optionen**.
2. Gehen Sie auf **Trust Center**.

3. Klicken Sie auf **Einstellungen für das Trust Center**.
4. Klicken Sie auf den Karteireiter **E-Mail-Sicherheit** und setzen Sie bei **Ausgehende Nachrichten digitale Signatur hinzufügen** ein Häkchen.

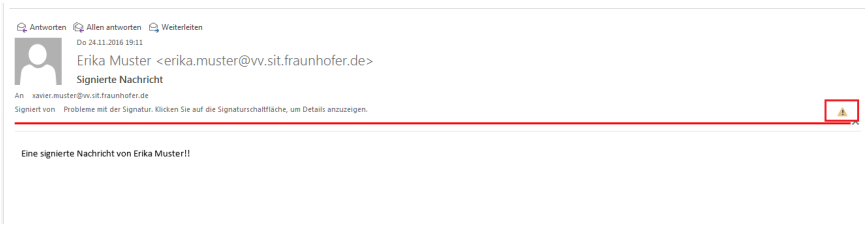


3.4.9 Empfang einer signierten E-Mail

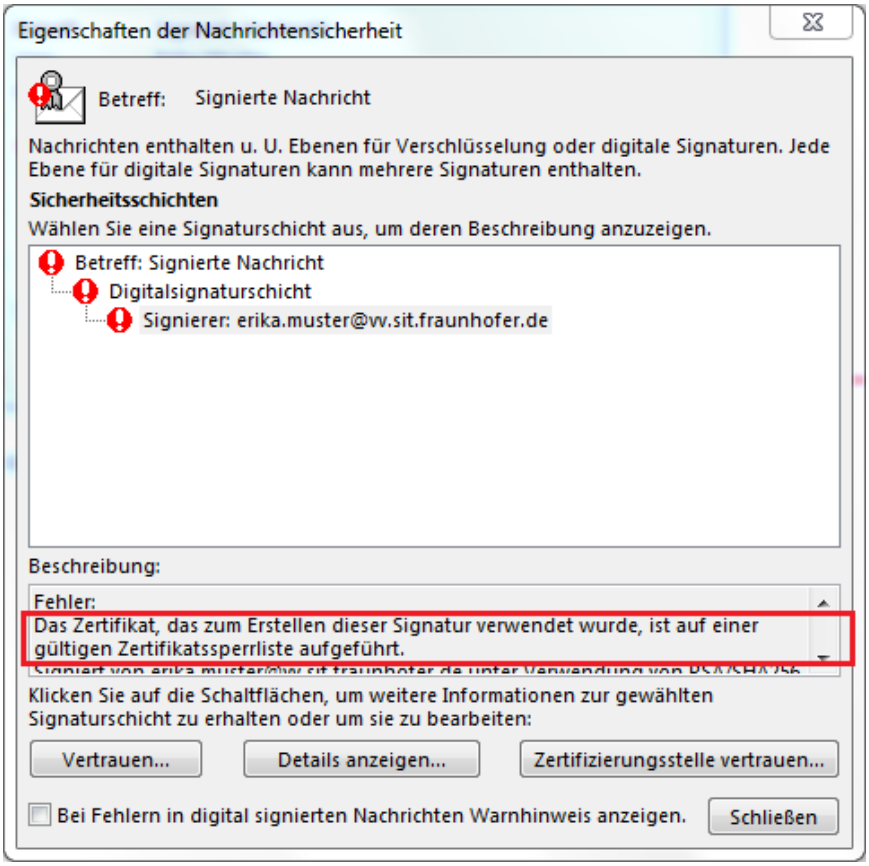
Eine signierte E-Mail erkennen Sie an dem **Siegel-Symbol**. Wenn Sie eine signierte E-Mail empfangen, prüft Outlook für Microsoft 365 die Gültigkeit der Signatur. Kann die Signatur nicht geprüft werden, da beispielsweise die CA-Zertifikate noch nicht importiert sind oder das Zertifikat zwischenzeitlich gesperrt wurde, erscheint eine Fehlermeldung. Wenn Sie auf das **Siegel-Symbol** klicken, erhalten Sie Informationen zum Signaturzertifikat des Senders:



Wurde die Signatur auf dem Transportweg manipuliert oder ist das Zertifikat des Senders gesperrt, wird dies anhand eines **gelben Warndreiecks** sichtbar:



Wenn Sie auf das **Warndreieck** und auf **Details** klicken, erhalten Sie weitere Informationen, z.B. ob das Zertifikat auf einer Sperrliste steht.



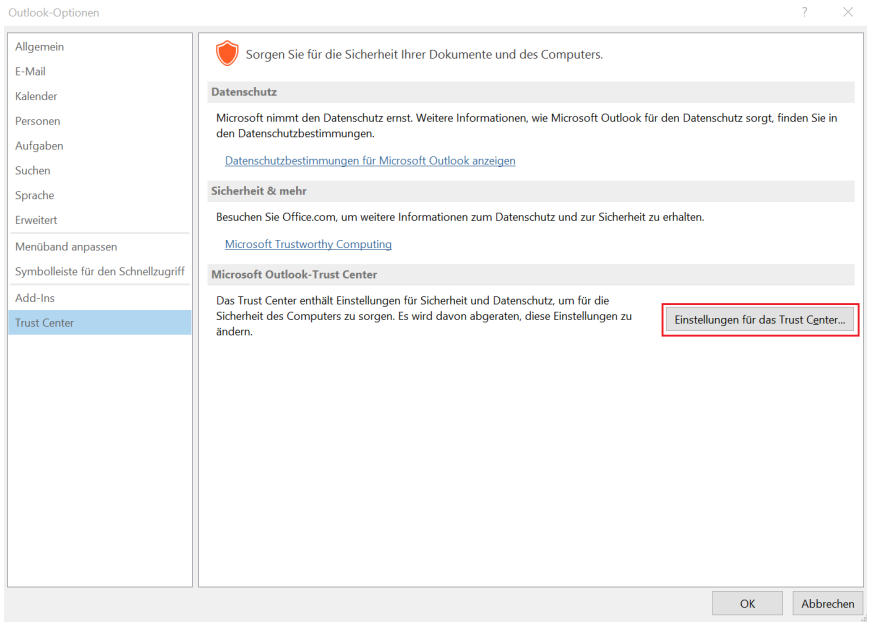
3.4.10 Senden einer signierten und verschlüsselten E-Mail

Wenn Sie eine signierte und verschlüsselte E-Mail versenden möchten, gehen Sie vor wie in den vorherigen Abschnitten beschrieben. In diesem Fall müssen vor dem Versand der E-Mail unter **Optionen** das Icon für die **Verschlüsselung** und für das **Signieren** ausgewählt werden.

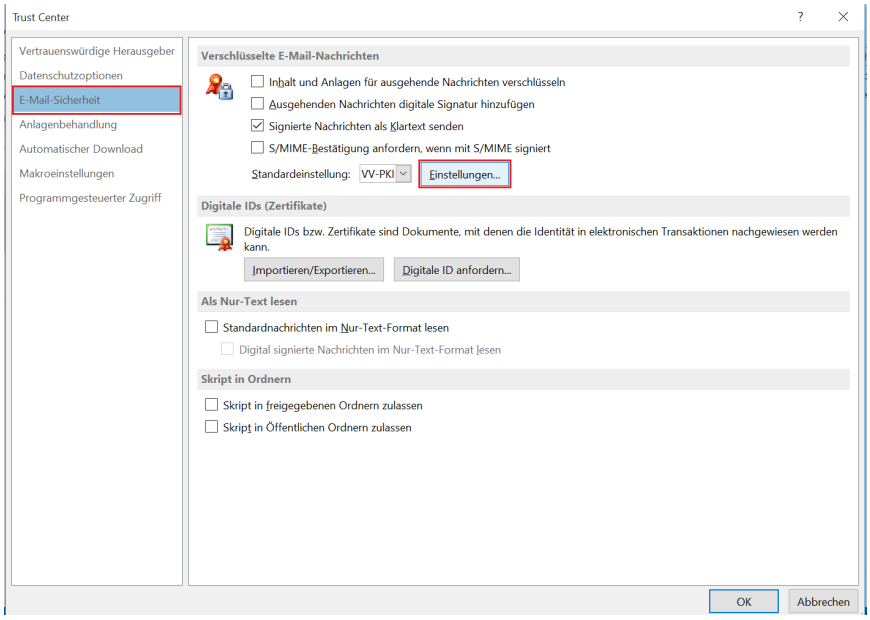
3.4.11 Kontrolle der installierten Zertifikate im Trustcenter

Wenn Sie überprüfen möchten, ob Ihre Zertifikate im Trustcenter von Outlook für Microsoft 365 installiert sind, dann können Sie wie folgt vorgehen:

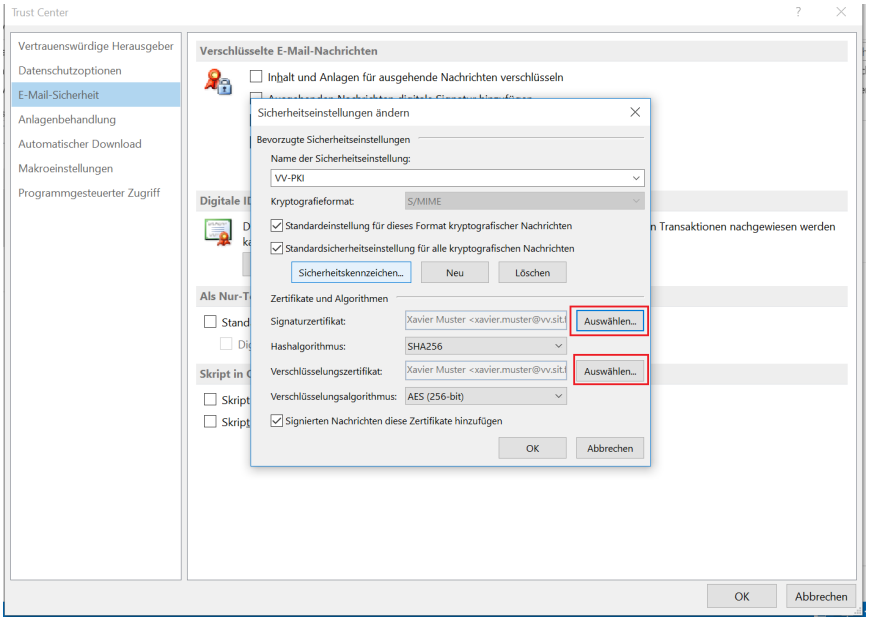
1. Wählen Sie **Datei**, dann **Optionen** und klicken Sie auf **Trust Center** und **Einstellungen für das Trust Center**.



2. Gehen Sie auf den Karteireiter **E-Mail Sicherheit** und klicken Sie auf **Einstellungen...**.



3. Im Fenster *Sicherheitseinstellungen ändern* können Sie überprüfen, ob Ihr Signaturzertifikat und Verschlüsselungszertifikat konfiguriert ist. Wird Ihr Zertifikat nicht angezeigt, können Sie durch einen Klick auf **Auswählen** die Liste der vorhandenen Zertifikate anzeigen lassen. Das Zertifikat der Volksverschlüsselung muss auf jeden Fall in der Liste erscheinen, auch wenn es nicht direkt ausgewählt ist. Outlook für Microsoft 365 wählt automatisch beim Signieren und Entschlüsseln von E-Mails das passende Zertifikat zur E-Mail-Adresse aus.



3.4.12 Nutzung mehrerer E-Mail-Konten

In Outlook können Sie mehrere E-Mail-Konten einrichten und für jede E-Mail-Adresse ein eigenes Zertifikat besitzen. Die verschlüsselte Kommunikation zwischen zwei installierten E-Mail-Konten findet genauso statt, wie die Kommunikation mit einem externen Kommunikationspartner, d.h. die Zertifikate müssen ggf. noch ausgetauscht werden (vgl. Wie bekomme ich das Verschlüsselungszertifikat des Empfängers?).

Wenn Sie für mehrere E-Mail-Konten in Outlook jeweils ein Zertifikat von der Volksverschlüsselung verwenden und diese mit Hilfe der Volksverschlüsselungs-Software in Outlook installieren, können Sie sofort die E-Mail-Konten in Outlook für eine vertrauliche und sichere Kommunikation verwenden. Jedes E-Mail-Konto wird mit dem eigenen persönlichen Zertifikat konfiguriert. Falls Sie für eine E-Mail-Adresse ein Zertifikat von einer anderen Zertifizierungsstelle verwenden möchten, müssen Sie dieses manuell in Outlook einrichten.

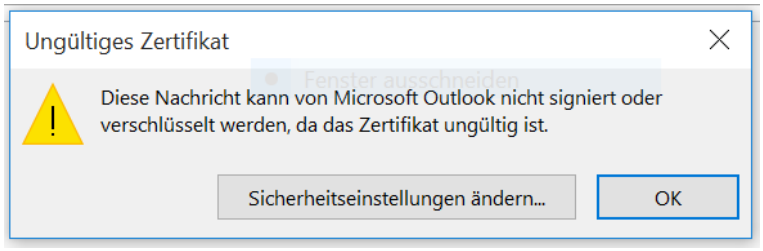
Welche Zertifikate in Outlook konfiguriert sind, können Sie gemäß Abschnitt Kontrolle der installierten Zertifikate im Trustcenter im Trust Center kontrollieren, wie folgendes Beispiel zeigt:

3.4.13 Nutzung eines gesperrten Zertifikats

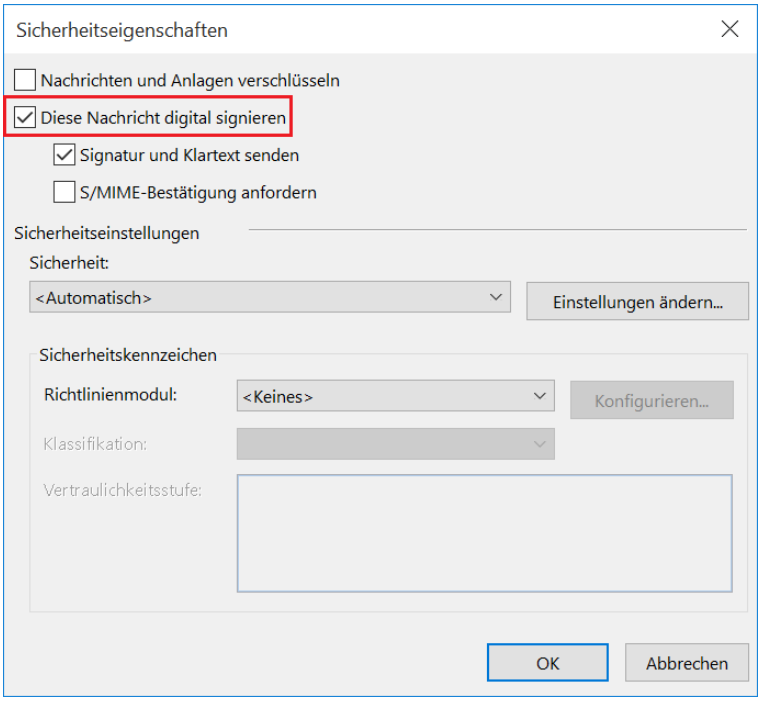
Sie können jederzeit Ihr Zertifikat vor Ablauf der Gültigkeit mit Hilfe der Volksverschlüsselungs-Software sperren lassen, beispielsweise wenn es fehlerhaft ist oder kompromittiert wurde. Hierbei ist zu beachten, dass immer alle drei Zertifikate gesperrt werden.

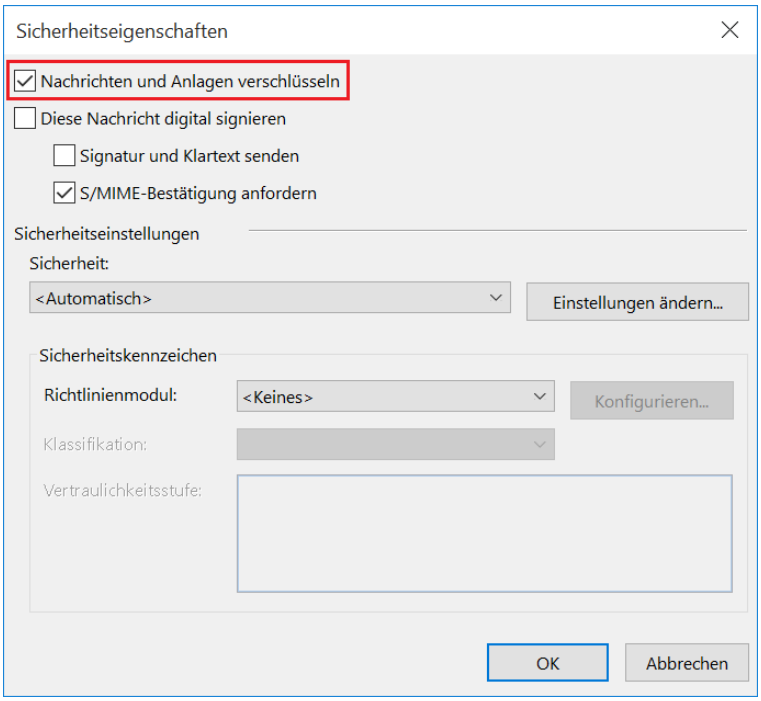
Erstellen Sie immer auch eine Sicherungskopie von Ihren gesperrten Zertifikaten und entfernen Sie diese nicht aus dem Windows Zertifikatsspeicher, da Sie ansonsten alte Nachrichten nicht mehr entschlüsseln können. Sollten gesperrte Zertifikate nicht mehr im Windows Zertifikatsspeicher vorliegen, können Sie diese mit Hilfe der Sicherungskopie und der Volksverschlüsselungs-Software wieder installieren.

Nach der Sperrung können Sie keine signierten und/oder verschlüsselte E-Mails mehr senden. Sie erhalten folgende Fehlermeldung:



Wenn Sie in den *Sicherheitseinstellung* die Häkchen entfernen, wird die Nachricht unsigniert bzw. unverschlüsselt versendet.





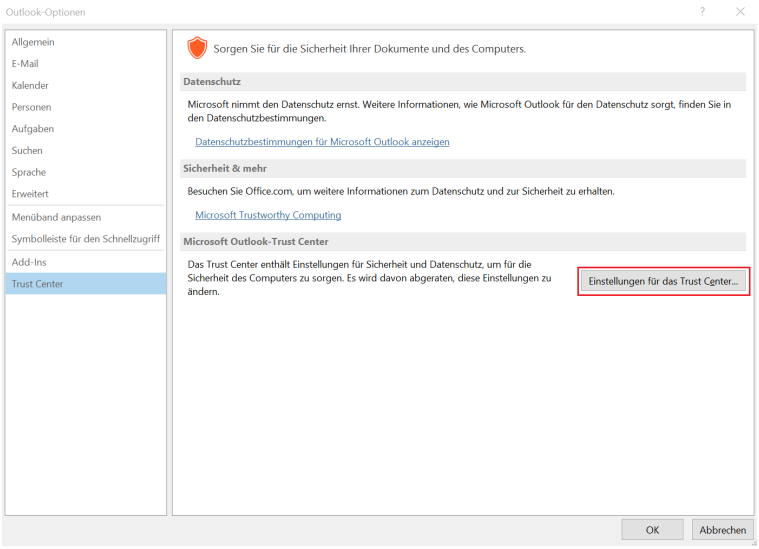
3.4.14 Zertifikate entfernen

Wenn Ihre Schlüssel/Zertifikate aus dem Trustcenter von Outlook und dem Windows Zertifikatsspeicher entfernt sind, können Sie für Sie verschlüsselte Nachrich-

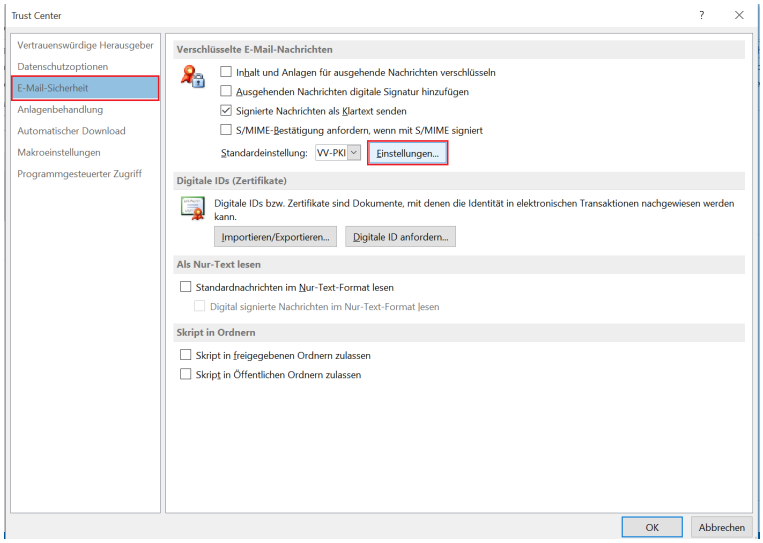
ten nicht mehr lesen. Sie können aber nachträglich die Schlüssel/Zertifikate mit der Volksverschlüsselungs-Software beispielsweise aus der Sicherungskopie wieder installieren.

Wenn Sie Ihre Schlüssel/Zertifikate in Outlook für Microsoft 365 entfernen möchten, gehen Sie wie folgt vor:

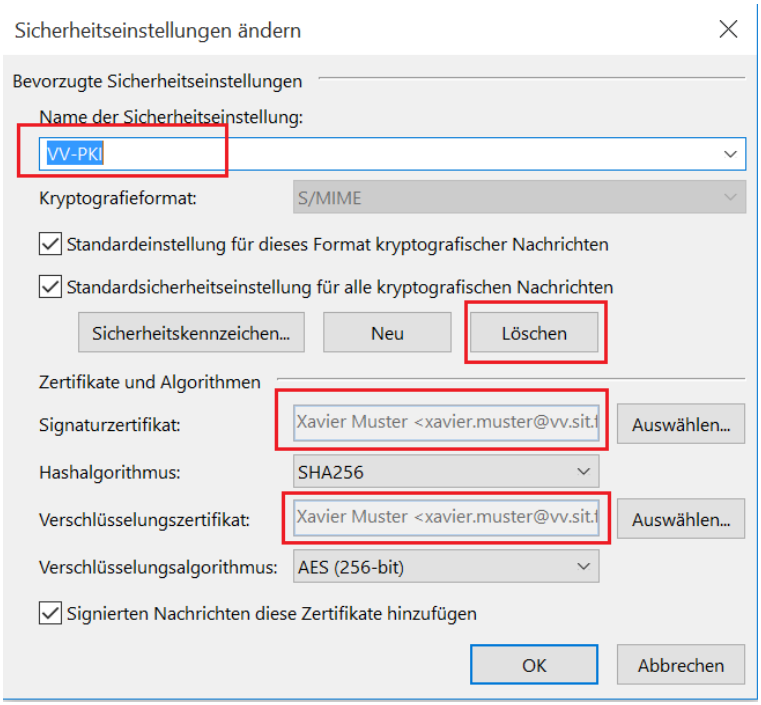
1. Wählen Sie **Datei**, dann **Optionen** und klicken Sie auf **Trust Center** und **Einstellungen für das Trust Center**



2. Gehen Sie auf den Karteireiter **E-Mail Sicherheit** und klicken Sie auf **Einstellungen...**.

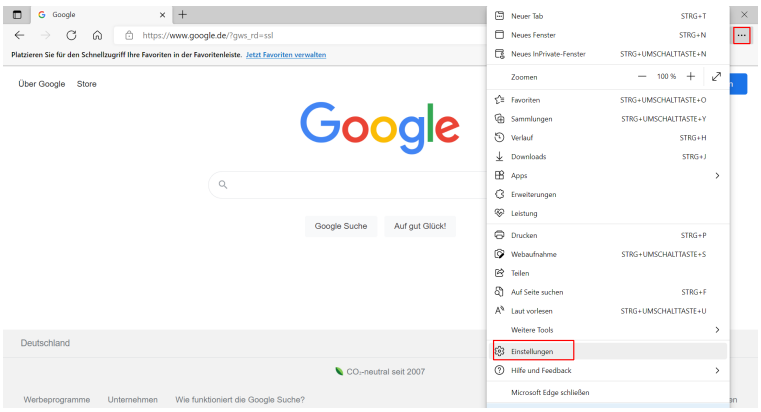


3. Wählen Sie im Fenster *Sicherheitseinstellungen ändern* Ihre Sicherheitseinstellung aus (in diesem Beispiel VV_PKI). Es werden Ihnen das Signatur- und Verschlüsselungszertifikat angezeigt. Klicken Sie auf **Löschen**.

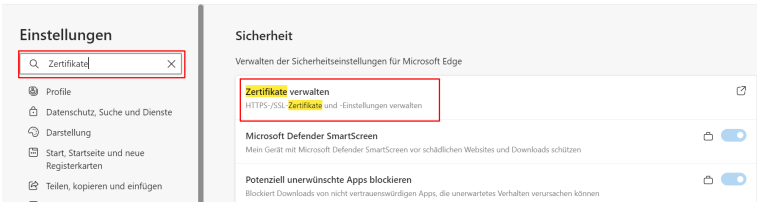


Hinweis: Wenn Sie Ihre Schlüssel/Zertifikate in Microsoft Anwendungen generell nicht mehr nutzen möchten, reicht es nicht aus, wenn Sie nur die Konfiguration im Trust Center löschen. Die Zertifikate müssen noch aus dem Windows Zertifikatspeicher gelöscht werden. Dazu gehe Sie wie folgt vor:

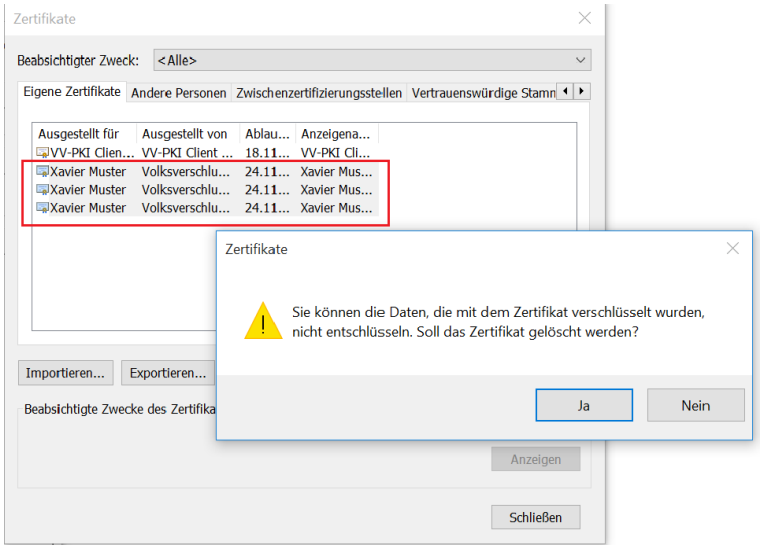
1. Klicken Sie z.B. im Microsoft Edge oben rechts auf das Zeichen "**...**" und weiter auf "**Einstellungen**".



2. Geben Sie im Suchfeld links oben "Zertifikate" ein und klicken Sie auf "**Zertifikate verwalten**" im rechten Fenster.



3. Wählen Sie **Eigene Zertifikate**. Markieren Sie die zu entfernenden Zertifikate und klicken Sie auf **Entfernen**.



3.5 Nutzung in Thunderbird

Dieser Abschnitt gibt Hilfestellungen bei der Verwendung der Schlüssel/Zertifikate der Volksverschlüsselung in *Thunderbird*.

3.5.1 Voraussetzungen

Für die nachfolgenden Ausführungen setzen wir voraus, dass

1. Sie Thunderbird auf Ihrem Rechner installiert und für Ihre E-Mail-Adresse ein Konto eingerichtet haben. Falls Sie beispielsweise ein Konto bei T-Online, GMX oder Web.de haben, so können Sie dieses auch in Thunderbird konfigurieren und verwenden. Anleitungen für das Einrichten eines E-Mail-Kontos in Thunderbird finden Sie bei Ihrem E-Mail-Anbieter.
2. Sie mit Hilfe der Volksverschlüsselungs-Software für die verwendete E-Mail-Adresse ein Zertifikat beantragt, heruntergeladen und Thunderbird konfiguriert haben.
3. Ihr Kommunikationspartner ebenfalls ein S/MIME-fähiges E-Mail-Programm und ein Zertifikat der Volksverschlüsselung oder eines anderen Anbieters von

S/MIME-Zertifikaten besitzt (vgl. Was benötigt mein Kommunikationspartner, um mit mir vertraulich kommunizieren zu können?).

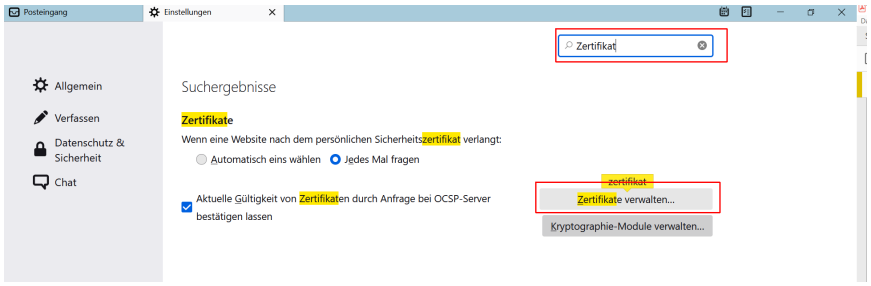
3.5.2 Installation der CA-Zertifikate der Volksverschlüsselung

Um die Gültigkeit eines Zertifikats der Volksverschlüsselung prüfen zu können, muss die gesamte Zertifikatskette in Thunderbird installiert sein, d.h. das Wurzelzertifikat *Volksverschlüsselung Root-CA G02* und das Zertifikat der Private CA *Volksverschlüsselung Private-CA G02* müssen Thunderbird bekannt sein. Wenn Sie die Volksverschlüsselungs-Software zur Konfiguration Ihrer Anwendung verwenden, werden diese Zertifikate automatisch installiert.

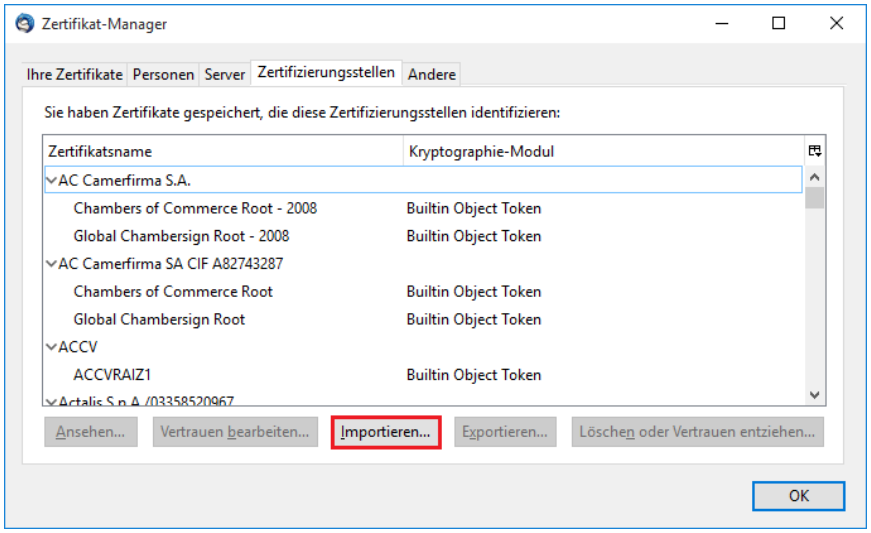
Falls Sie die Volksverschlüsselungs-Software nicht verwenden wollen/können, dann müssen Sie die Zertifikate manuell importieren. Laden Sie hierzu die Zertifikate im Binärformat (DER) von der Webseite `https://volksverschluesselung.de/zertifikate.php` herunter und binden Sie sie wie folgt in Thunderbird ein.

Import des Wurzelzertifikats

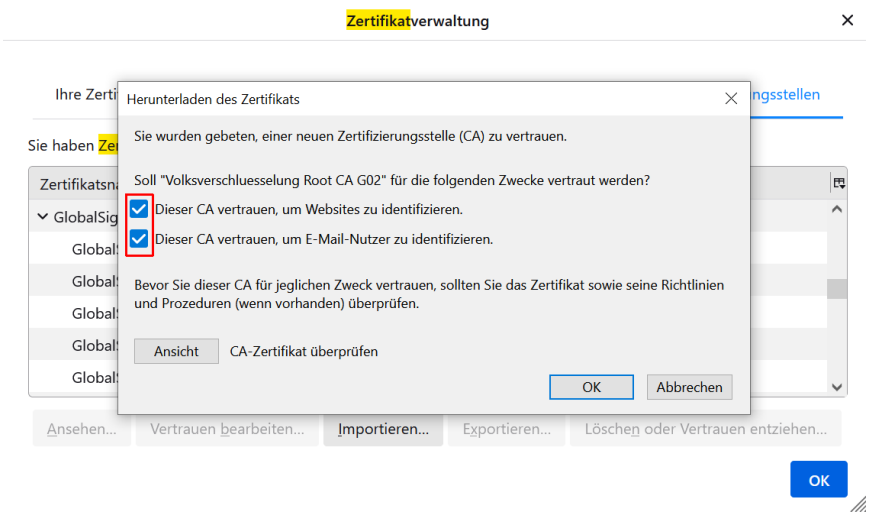
1. Gehen Sie auf Hamburger-Menü (drei Striche oben rechts) **-> Erweitert** und geben Sie **Zertifikate** im Suchfeld ein. Klicken Sie auf **Zertifikate verwalten**:



2. Gehen Sie auf den Karteireiter **Zertifizierungsstellen** und klicken Sie auf **Importieren**. Suchen Sie den Pfad, in dem Sie die zuvor heruntergeladenen Zertifikate abgelegt haben, und wählen Sie die Datei **VV-Root-G02-CA.cer** aus.

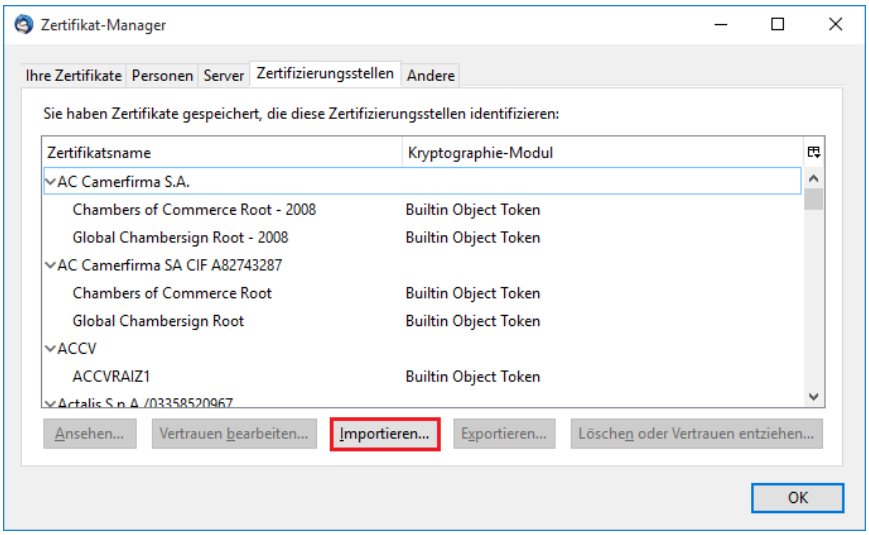


3. Setzen Sie in **allen** Feldern ein Häkchen und klicken Sie auf **OK**.

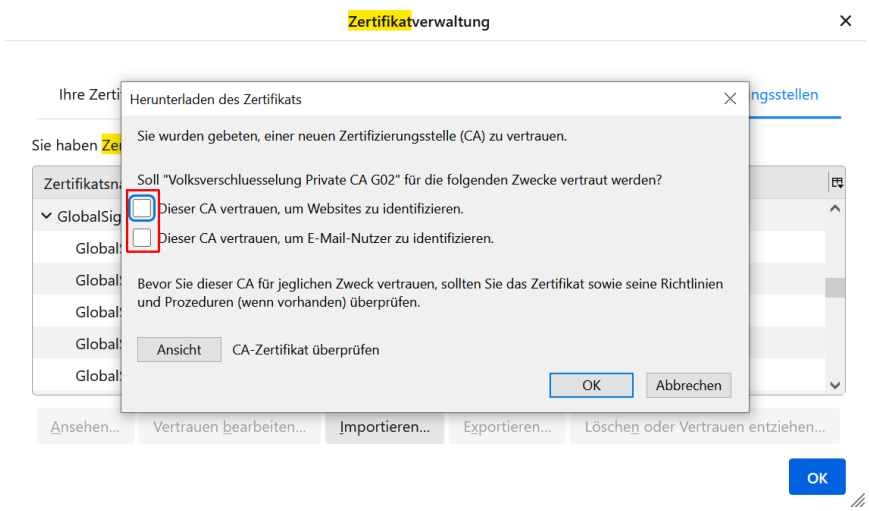


Import des Zertifikats der Volksverschluesselung Private CA

1. Gehen Sie auf den Karteireiter **Zertifizierungsstellen** und klicken Sie auf **Importieren**. Suchen Sie den Pfad, unter dem Sie die zuvor heruntergeladenen Zertifikate abgelegt haben und wählen Sie die Datei **VV-Private-User-G02-CA.cer** aus.



2. Setzen Sie in **keinem** Feld ein Häkchen und klicken Sie auf **OK**.

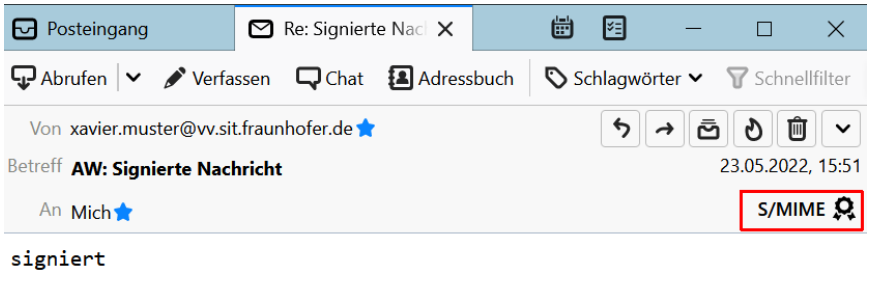


3.5.3 Austausch des Verschlüsselungszertifikats mittels signierter E-Mail

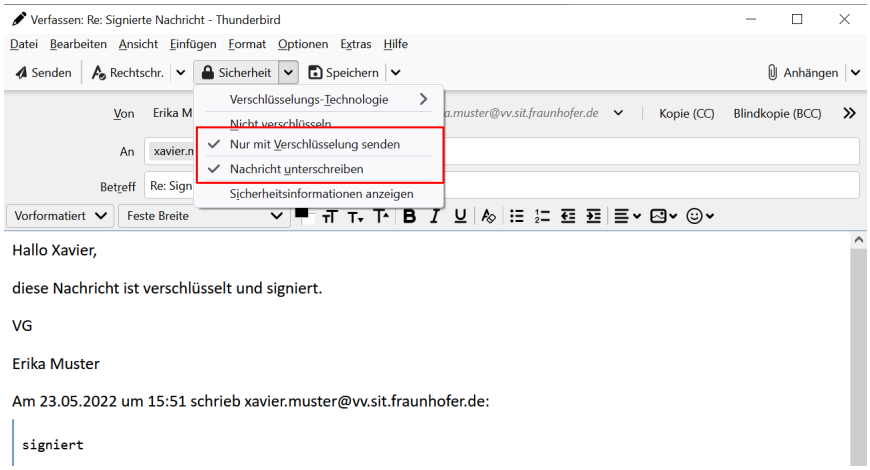
Eine Möglichkeit sein Verschlüsselungszertifikat verfügbar zu machen, besteht darin, dem Kommunikationspartner eine signierte E-Mail zu senden. Bei einer signierten E-Mail werden alle Zertifikate des Absenders mitgesendet und dem E-Mail-Programm auf Empfängerseite bekannt gemacht.

Hinweis: Im E-Mail-Programm des Empfängers der signierten Nachricht muss die Zertifikatskette der Volksverschlüsselung installiert sein, damit die Gültigkeit der Signatur überprüft werden kann. Falls der Empfänger die Volksverschlüsselungs-Software nicht verwendet, muss er die Zertifikate *Volksverschluesselung Root-CA G02* und *Volksverschluesselung Private-CA G02* manuell zu installieren, wie in Installation der CA-Zertifikate der Volksverschlüsselung beschrieben.

1. Ihr Kommunikationspartner sendet eine **signierte** Mail an Sie, die Sie an dem *S/MIME mit schwarzem Siegel* erkennen. Durch das Öffnen der signierten E-Mail wird der öffentliche Schlüssel aus dem Verschlüsselungszertifikat des Senders automatisch in den Zertifikatsspeicher von Thunderbird übernommen.



2. Sie können den öffentlichen Schlüssel Ihres Kommunikationspartners sofort nutzen, um **verschlüsselt** mit ihm zu kommunizieren.



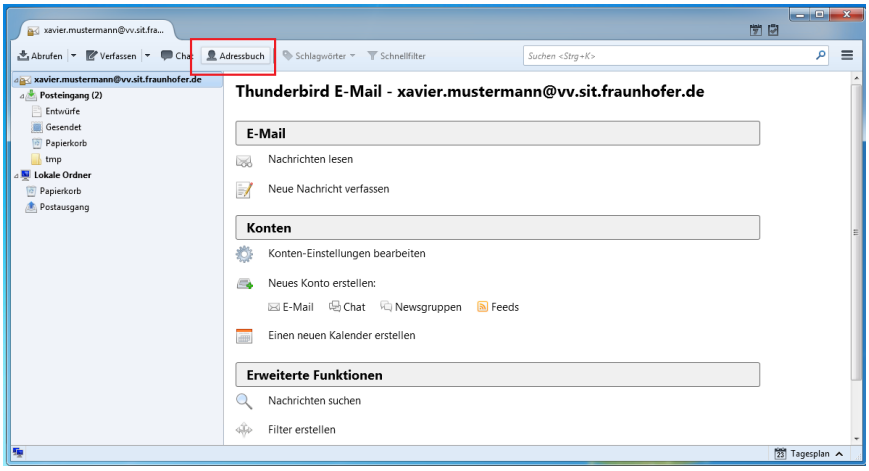
3.5.4 Manuelle Konfiguration des Verzeichnisdienstes der Volksverschlüsselung

Die Volksverschlüsselung bietet einen öffentlichen LDAP (Lightweight Directory Access Protocol) Verzeichnisdienst an, in dem alle Verschlüsselungszertifikate der Nutzer der Volksverschlüsselung zu finden sind, sofern sie bei der Zertifikatsbeantragung hierzu ihre Einwilligung erteilt haben.

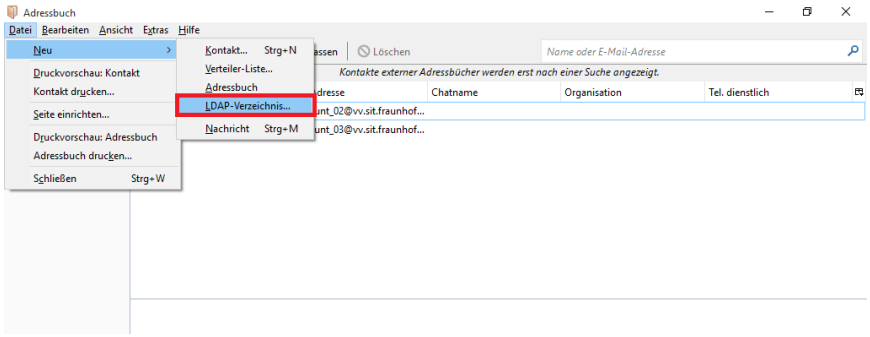
Wenn Sie die Volksverschlüsselungs-Software nicht verwenden, aber den Verzeichnisdienst der Volksverschlüsselung installieren wollen, um Personen zu finden, denen Sie eine verschlüsselte E-Mail schicken möchten, müssen Sie ein neues Adressbuch einrichten. Hierfür benötigen Sie den Hostname, den Basis-DN und die Portnummer. Die Konfigurationsparameter des Verzeichnisdienstes der Volksverschlüsselung finden Sie auf unserer Webseite.

So richten Sie den Verzeichnisdienst der Volksverschlüsslung in Thunderbird ein:

1. Öffnen Sie in Thunderbird das Adressbuch.

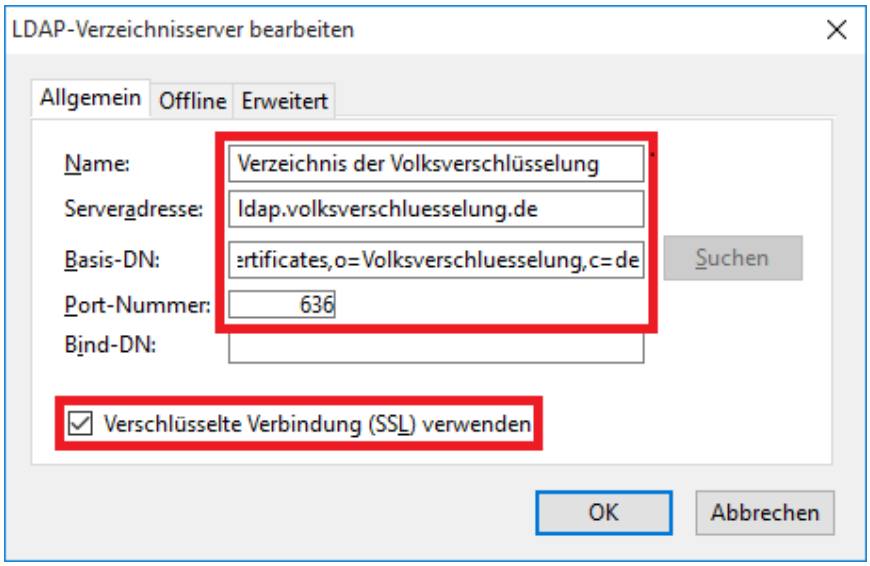


2. Erstellen Sie ein neues LDAP-Verzeichnis, indem Sie auf **Datei->Neu->LDAP-Verzeichnis** klicken.



3. Tragen Sie folgende Konfigurationsdaten in die Felder ein und bestätigen Sie dann alles mit **OK**.

   - Name: Verzeichnis der Volksverschlüsselung (Name frei wählbar)
   - Serveradresse: **ldap.volksverschluesselung.de**
   - Basis-DN: **ou=Certificates,o=Volksverschluesselung,c=de**
   - Port-Nummer: **636**
   - Bei **Verschlüsselte Verbindung (SSL) verwenden:** ein Häkchen setzen



3.5.5 Manuelle Konfiguration des Verzeichnisdienstes einer fremden Zertifizierungsstelle

Hat Ihr Kommunikationspartner sein Zertifikat in einem Verzeichnisdienst eines anderen Zertifizierungsanbieters veröffentlich, dann bitten Sie ihn, Ihnen die Konfigurationsdaten zu nennen: Hostname, Portnummer (mit/ohne SSL/TLS) und Basis-DN.

Wenn Ihnen die Konfigurationsdaten bekannt sind, können Sie den Verzeichnisdienst, wie im vorherigen Abschnitt beschrieben, in Thunderbird einrichten.

3.5.6 Senden einer verschlüsselten E-Mail

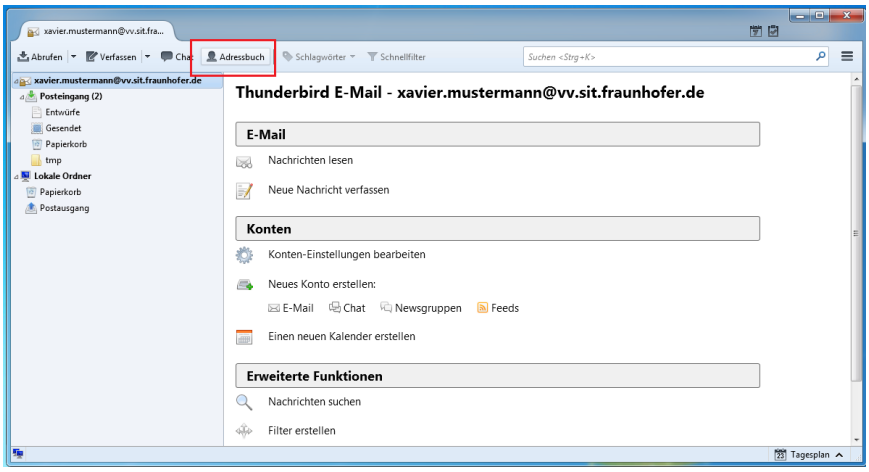
Im Folgenden wird eine Möglichkeit beschrieben, wie Sie in Thunderbird eine verschlüsselte E-Mail für Ihren Kommunikationspartner erzeugen können.

In diesem Beispiel wird vorausgesetzt, dass Ihr Kommunikationspartner ebenfalls ein Zertifikat der Volksverschlüsselung besitzt und sein Zertifikat im Verzeichnis veröffentlicht hat.

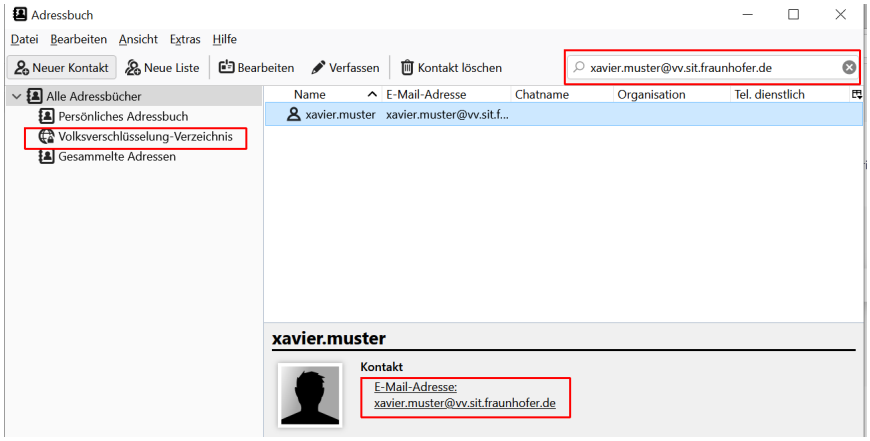
Für die Kommunikation mit einem Kommunikationspartner, dessen Zertifikat Sie noch nicht kennen, müssen Sie zuerst sein Zertifikat in Ihrem E-Mail-Programm verfügbar machen, wie in den vorhergehenden Abschnitten beschrieben wurde.

In dem Ordner, in dem Ihre gesendeten E-Mails abgespeichert werden, können Sie eine verschlüsselte Nachricht an dem “Schloss-Symbol” erkennen. Jede verschlüsselte E-Mail wird auch mit Ihrem **Verschlüsselungszertifikat** verschlüsselt und in diesem Ordner abgelegt.

1. Öffnen Sie das **Adressbuch**.

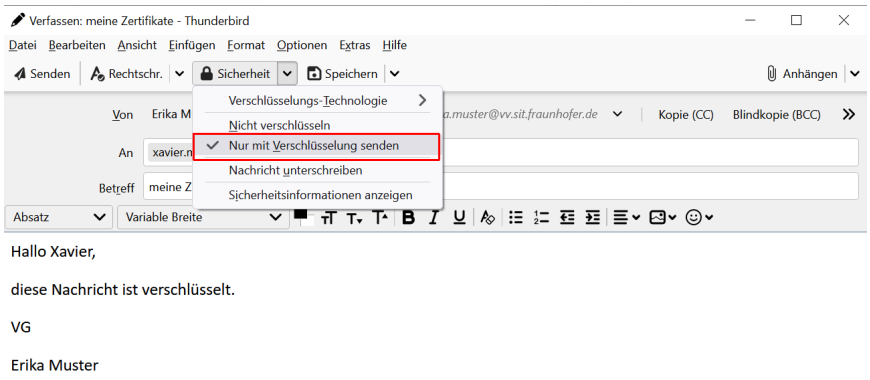


2. Suchen Sie die E-Mail-Adresse Ihres Kommunikationspartners:
   - Gehen Sie unter **Alle Adressbücher** auf das **Verzeichnis der Volksverschlüsselung**.
   - Geben Sie in der **Suche** die **vollständige E-Mail-Adresse** ein.
   - Klicken Sie auf die E-Mail-Adresse und dann im Fenster *Kontakte* erneut auf die E-Mail-Adresse, um eine E-Mail zu schreiben.



3. Geben Sie Ihre Nachricht ein und verschlüsseln Sie diese wie folgt:

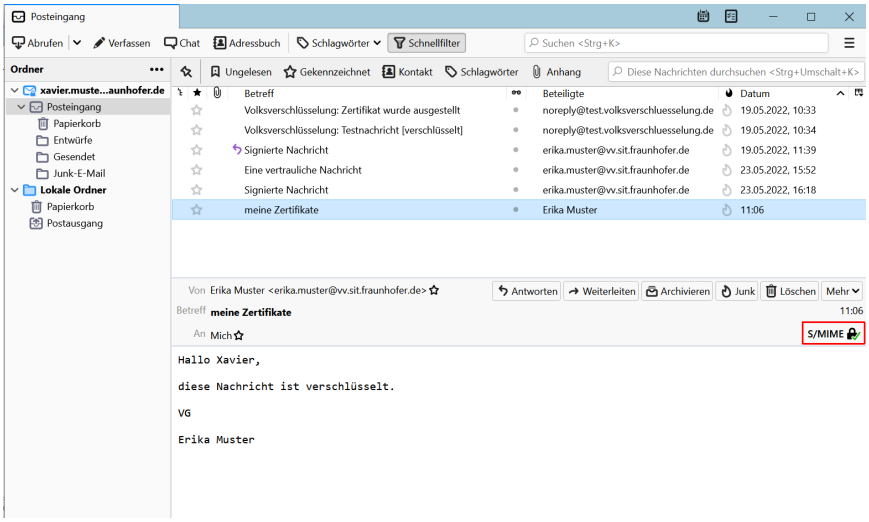
   - Gehen Sie auf **Sicherheit**.
   - Wählen Sie die Option **Nur mit Verschlüsselung senden** aus und senden Sie Ihre E-Mail.



Hinweis: Nach einer einmaligen erfolgreichen vertraulichen Kommunikation können Sie die E-Mail-Adresse Ihres Kommunikationspartner direkt aus einer E-Mail oder aus Ihrer Kontaktliste entnehmen. Seine Zertifikate sind dann schon dem Thunderbird bekannt.

3.5.7 Empfang einer verschlüsselten E-Mail

Wenn Sie eine verschlüsselte E-Mail empfangen, können Sie diese sofort lesen, wenn Sie Ihren privaten Schlüssel in Thunderbird beispielsweise mit Hilfe der Volksverschlüsselungs-Software konfiguriert haben. Das **Schloss-Symbol** zeigt an, dass die E-Mail vom Absender verschlüsselt wurde.

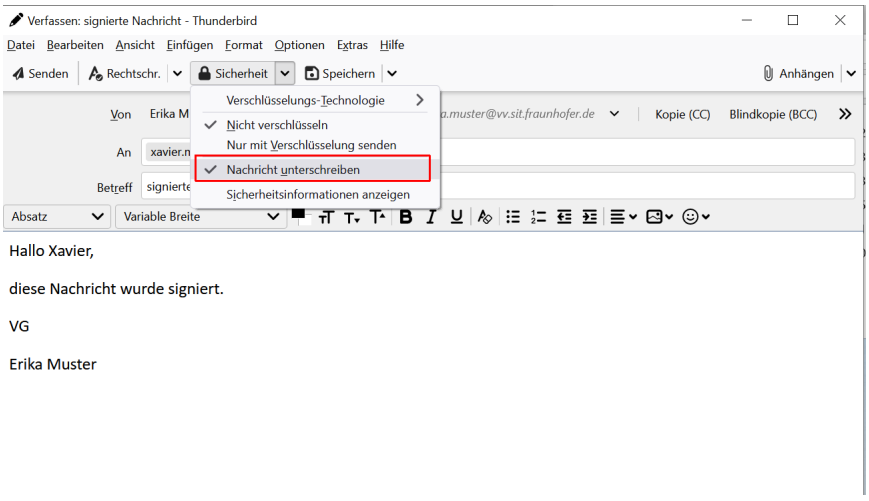


3.5.8 Senden einer signierten E-Mail

Für das Signieren Ihrer E-Mail wird Ihr gültiges Signaturzertifikat verwendet. Wenn Sie Thunderbird mit Hilfe der Volksverschlüsselungs-Software konfiguriert haben, ist dieses bereits installiert.

In dem Ordner, in dem Ihre gesendeten E-Mails abgespeichert werden, können Sie eine signierte Nachricht an dem **S/MIME mit einem schwarzen Siegel** erkennen.

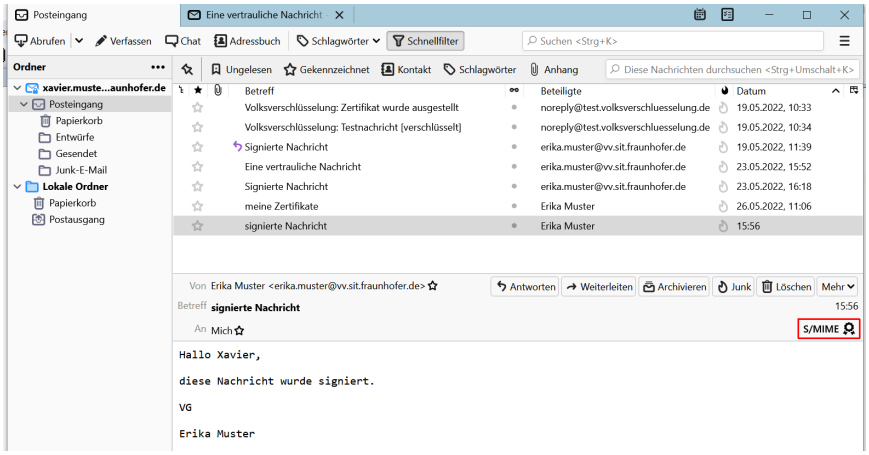
Wenn Sie Ihre E-Mail verfasst haben, gehen Sie auf **Sicherheit**, wählen die Option **Nachricht unterschreiben** aus und senden dann ihre E-Mail.



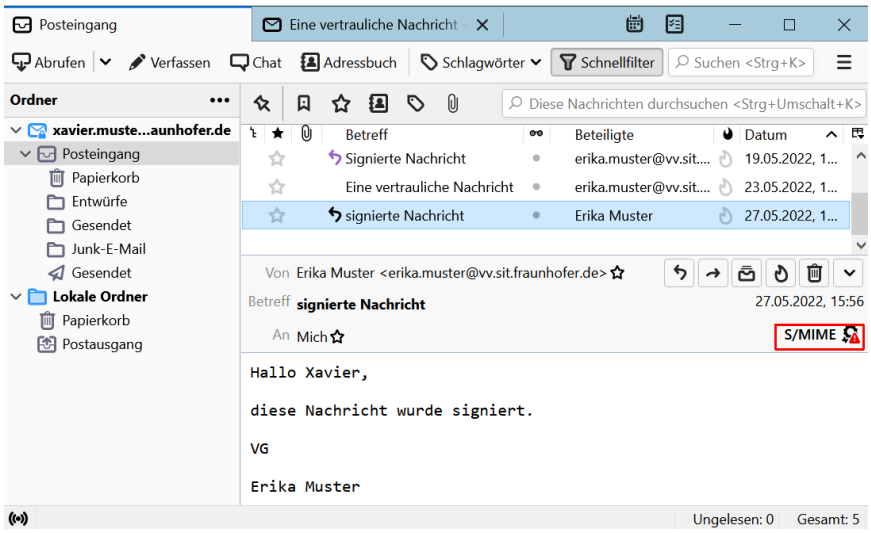
3.5.9 Empfang einer signierten E-Mail

Eine signierte E-Mail erkennen Sie an dem **S/MIME mit einem schwarzen Siegel**. Wenn Sie eine signierte E-Mail empfangen, prüft Thunderbird automatisch die Gültigkeit der Signatur.

Wenn Sie auf das Signatur-Symbol klicken, erhalten Sie Informationen zum Signaturzertifikat des Senders.



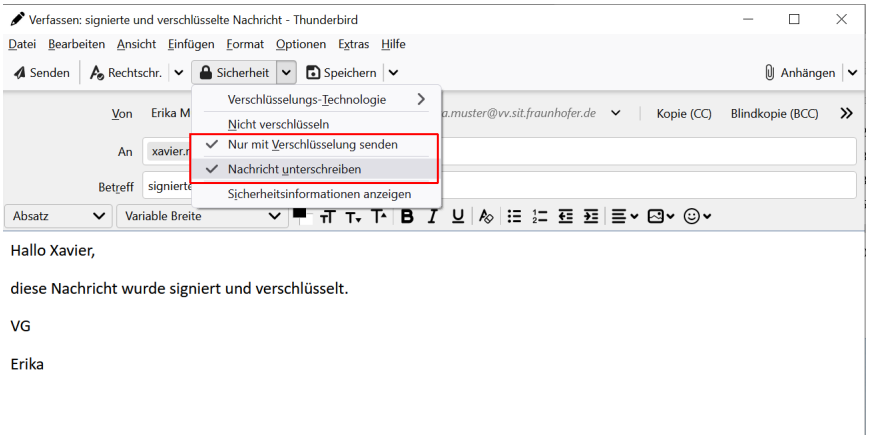
Wurde die Signatur auf dem Transportweg manipuliert oder ist das Zertifikat des Senders gesperrt, wird es anhand eines **Siegel mit einem roten Warndreieck** sichtbar:



3.5.10 Senden einer signierten und verschlüsselten E-Mail

Wenn Sie eine signierte und verschlüsselte E-Mail versenden möchten, gehen Sie vor, wie in den vorherigen Abschnitten beschrieben. In diesem Fall müssen vor dem Ver-

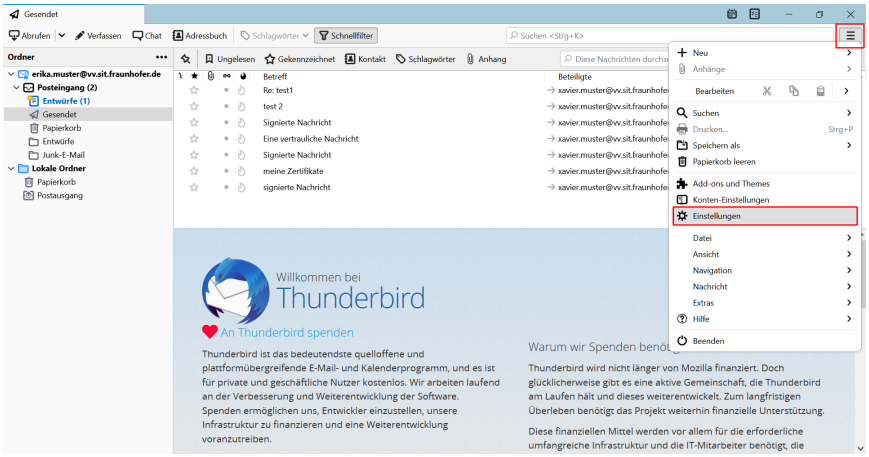
sand der Nachricht die Optionen **Nur mit Verschlüsselung senden** und **Nachricht unterschreiben** ausgewählt werden.



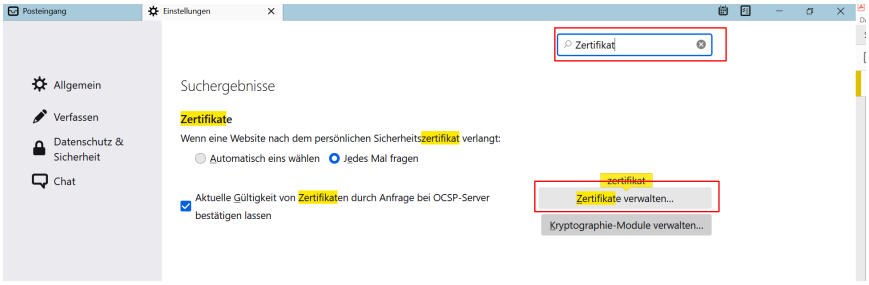
3.5.11 Kontrolle der installierten Zertifikate in Einstellungen

In Thunderbird können Sie sich unter **Einstellungen** alle Details zu den installierten Zertifikaten ansehen.

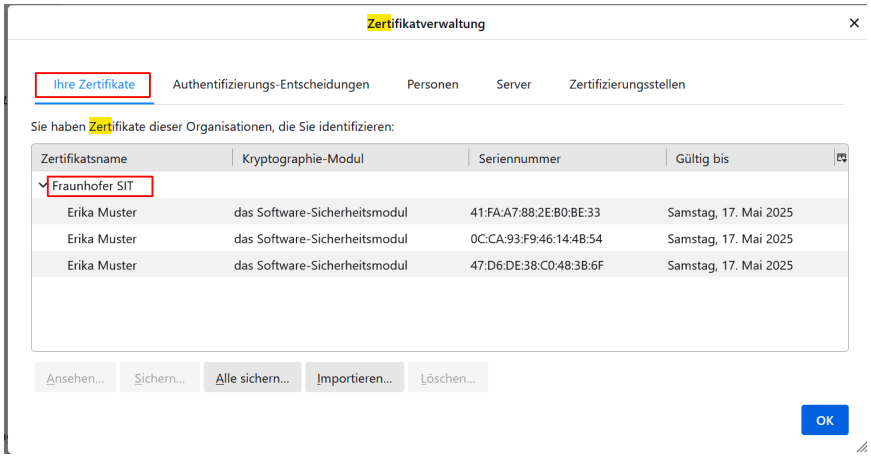
1. Gehen Sie im *Anwendungsmenü* zu **Einstellungen**.



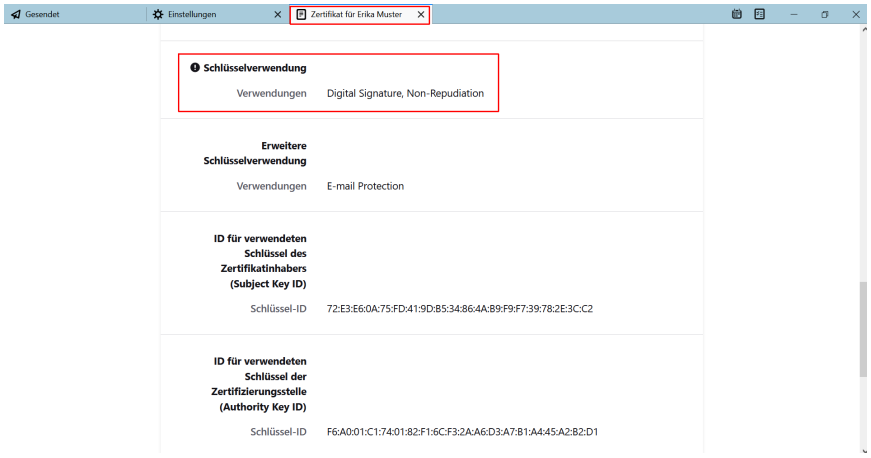
2. Geben Sie im Suchfeld links oben "Zertifikate" ein und klicken Sie auf "**Zertifikate verwalten**" im rechten Fenster.



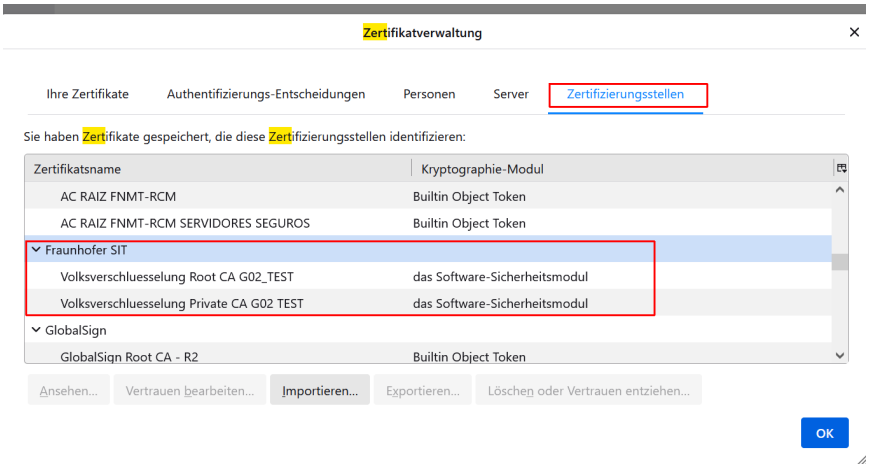
3. Wählen Sie den Karteireiter **Ihre Zertifikate**. Suchen Sie nach Ihren drei Volksverschlüsselungs-Zertifikaten. Sie finden Ihre Zertifikate der Volksverschlüsselung unter **Fraunhofer SIT**



4. Um überprüfen zu können, ob das Zertifikat erfolgreich installiert und verifiziert wurde, klicken Sie auf ein Zertifikat und auf Button “Ansehen”. In den Feldern *Schlüsselverwendung* und *Erweiterte Schlüsselverwendung* sehen Sie, ob es sich um das Verschlüsselungs-, Signatur- oder Authentifizierungszertifikat handelt.



Wenn Sie die Zertifikate der *Volksverschluesselung Root-CA G02* und *Volksverschluesselung Private-CA G02* kontrollieren möchten, gehen Sie zum Karteireiter **Zertifizierungsstellen**.



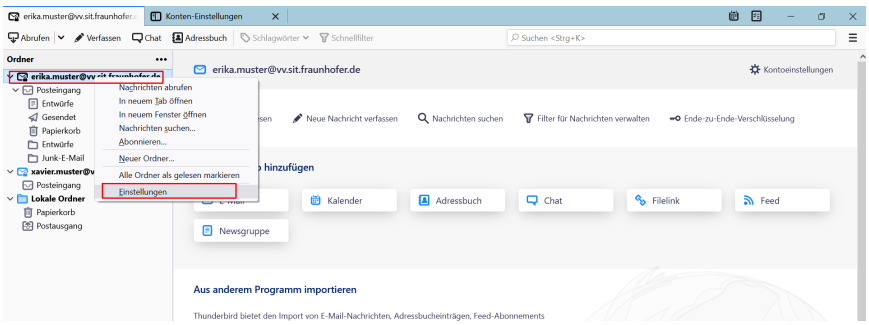
3.5.12 Nutzung mehrerer E-Mail-Konten

In Thunderbird können Sie mehrere E-Mail-Konten einrichten und für jede E-Mail-Adresse ein eigenes Zertifikat besitzen. Die verschlüsselte Kommunikation zwischen zwei installierten E-Mail-Konten findet genauso statt, wie die Kommunikation mit einem externen Kommunikationspartner, d.h. die Zertifikate müssen ggf. noch ausgetauscht werden (vgl. Wie bekomme ich das Verschlüsselungszertifikat des Empfängers?).

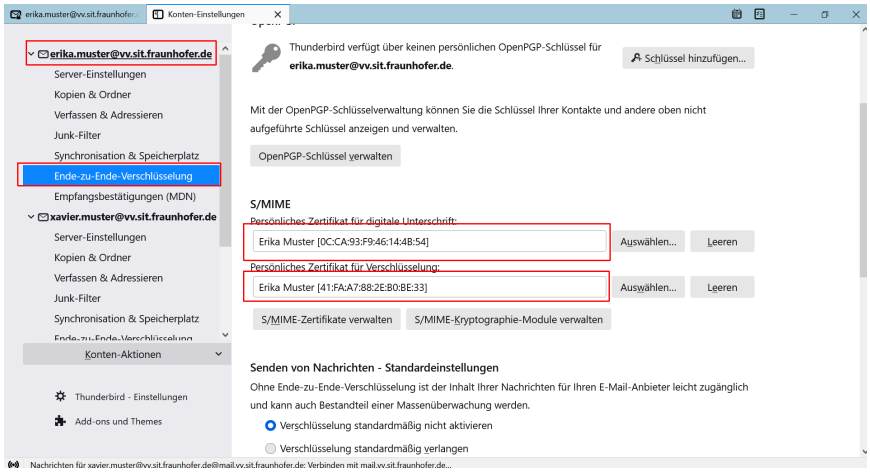
Wenn Sie für mehrere E-Mail-Konten in Thunderbird jeweils ein Zertifikat von der Volksverschlüsselung verwenden und diese mit Hilfe der Volksverschlüsselungs-Software in Thunderbird installieren, können Sie sofort die E-Mail-Konten in Thunderbird für eine vertrauliche und sichere Kommunikation verwenden. Falls Sie für eine E-Mail-Adresse ein Zertifikat von einer anderen Zertifizierungsstelle verwenden möchten, müssen Sie dieses manuell in Thunderbird einrichten.

Jedes E-Mail-Konto wird mit dem eigenen persönlichen Zertifikat konfiguriert. Sie können es wie folgt kontrollieren:

1. Klicken Sie mit der rechten Maustaste auf das entsprechende E-Mail-Konto und klicken Sie auf **Einstellungen**.



2. Gehen Sie zum Menüpunkt **Ende-zu-Ende-Verschlüsselung** und kontrollieren im rechten Fenster, welche Zertifikate für das Konto konfiguriert sind.

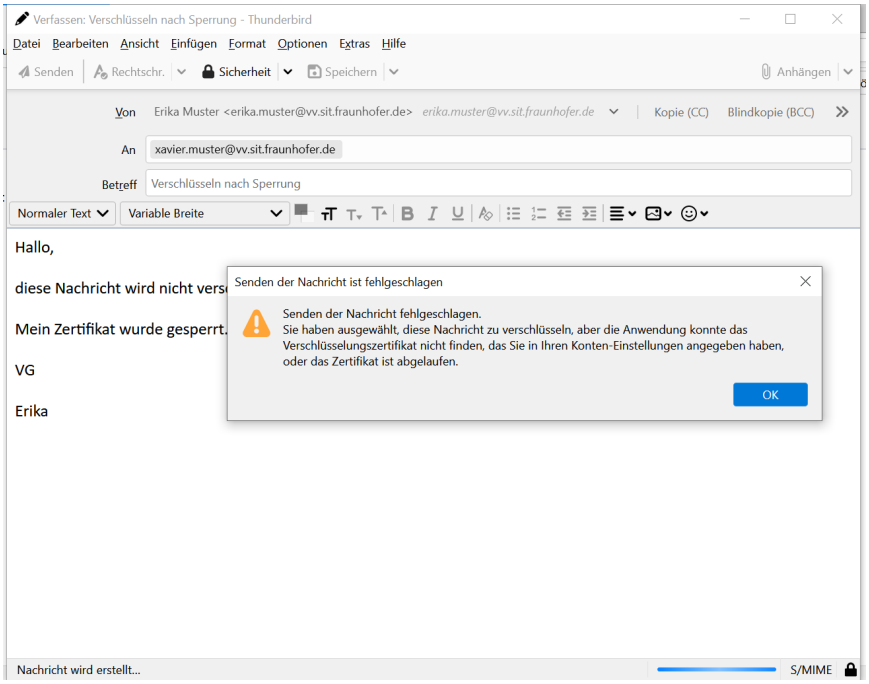


3.5.13 Nutzung eines gesperrten Zertifikats

Sie können jederzeit Ihr Zertifikat vor Ablauf der Gültigkeit mit Hilfe der Volksverschlüsselungs-Software sperren lassen, beispielsweise wenn es fehlerhaft ist oder kompromittiert wurde. Hierbei ist zu beachten, dass immer alle drei Zertifikate gesperrt werden.

Erstellen Sie immer auch eine Sicherungskopie von Ihren gesperrten Zertifikaten und entfernen Sie diese nicht aus dem Zertifikatsspeicher von Thunderbird, da Sie ansonsten alte Nachrichten nicht mehr entschlüsseln können. Sollten gesperrte Zertifikate nicht mehr im Zertifikatsspeicher vorliegen, können Sie diese mit Hilfe der Sicherungskopie und der Volksverschlüsselungs-Software wieder installieren.

Sie können keine *signierte* oder *verschlüsselte* Nachrichten mit einem gesperrten Zertifikat weiter versenden. Ihre Kommunikationspartner können Ihnen keine *verschlüsselten* Nachrichten mehr senden, da Ihr Zertifikat nicht mehr gültig ist. Beim Versenden erscheint folgende Fehlermeldung:

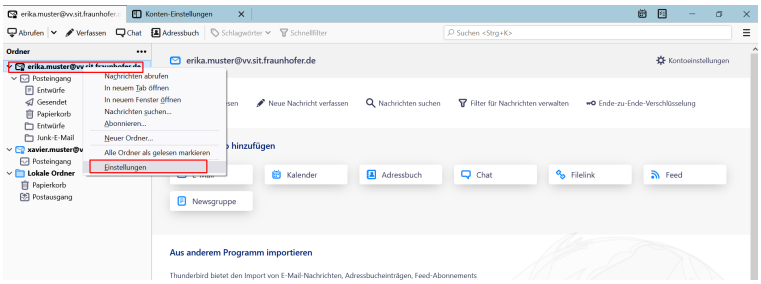


3.5.14 Zertifikate entfernen

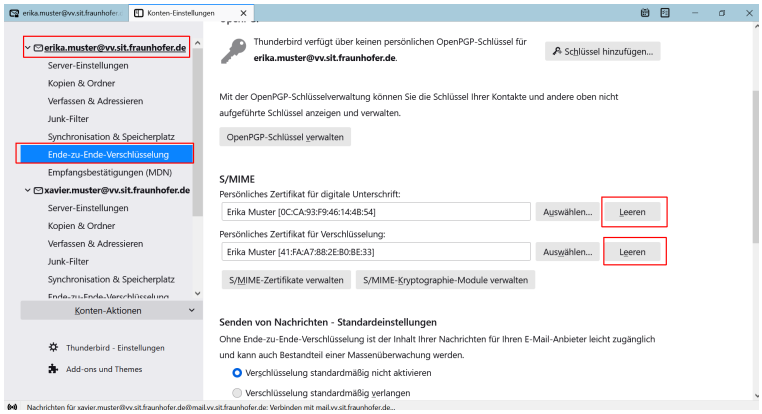
Wenn Ihre Schlüssel/Zertifikate aus dem Zertifikatsspeicher von Thunderbird entfernt sind, können Sie für Sie verschlüsselte Nachrichten nicht mehr lesen. Sie können aber nachträglich die Schlüssel/Zertifikate mit der Volksverschlüsselungs-Software beispielsweise aus der Sicherungskopie wieder installieren.

Wenn Sie in Thunderbird Ihre Schlüssel/Zertifikate aus Ihrem E-Mail-Konto und aus dem Zertifikatsspeicher entfernen wollen, gehen Sie wie folgt vor:

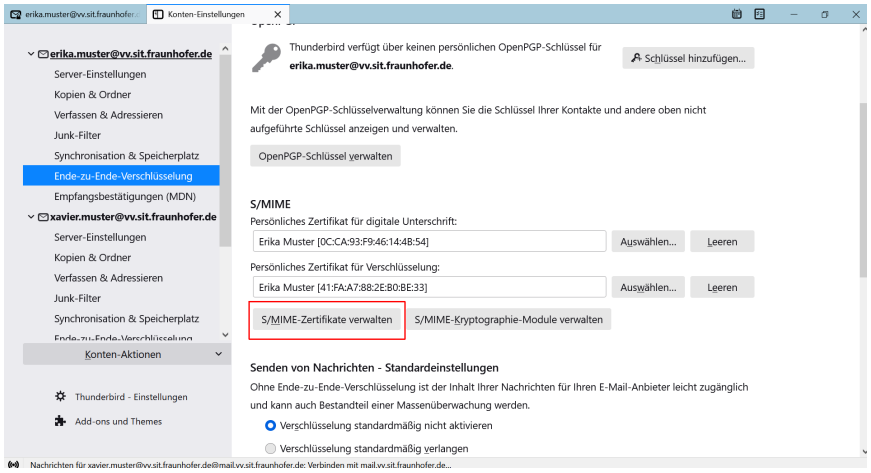
1. Klicken Sie mit der rechten Maustaste auf das E-Mail-Konto und klicken Sie auf **Einstellungen**.



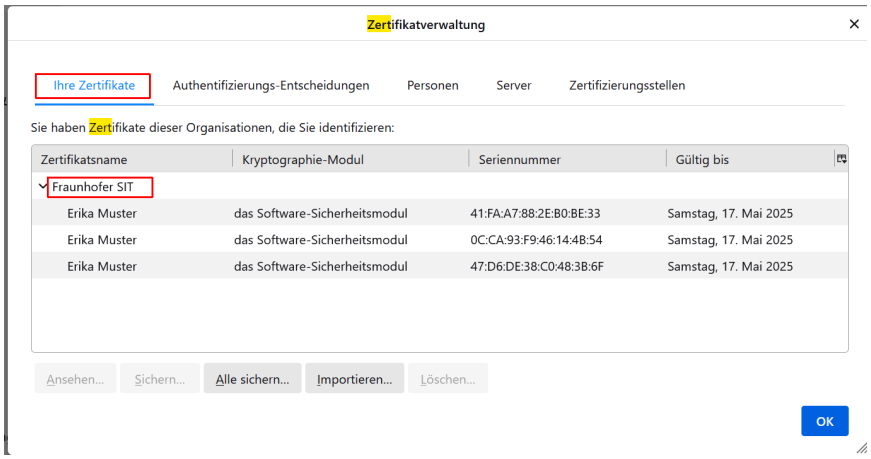
2. Gehen Sie zum Menüpunkt **Ende-zu-Ende-Verschlüsselung** und klicken Sie im rechten Fenster auf **Leeren**, sowohl für die *Digitale Unterschrift* als auch für die *Verschlüsselung*.



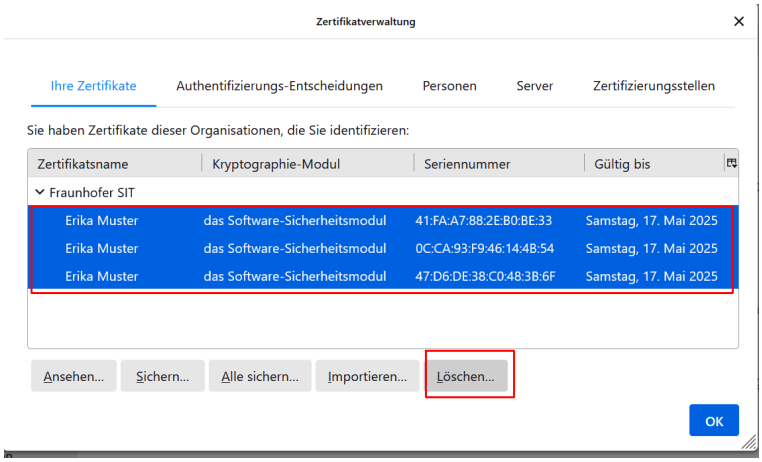
3. Klicken Sie auf **Zertifikate verwalten**.



4. Wählen Sie den Karteireiter **Ihre Zertifikate**.

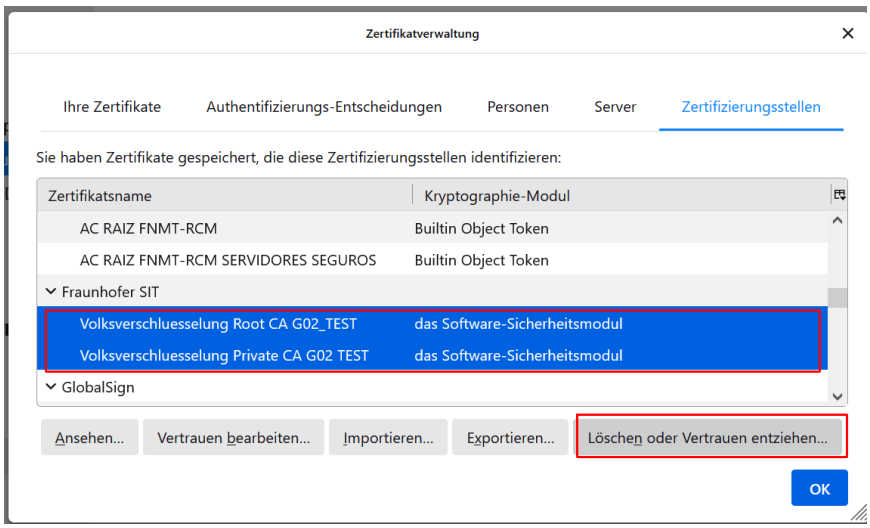


5. Suchen Sie nach Ihren drei Volksverschlüsselungs-Zertifikaten, markieren Sie diese und klicken Sie auf **Löschen**.

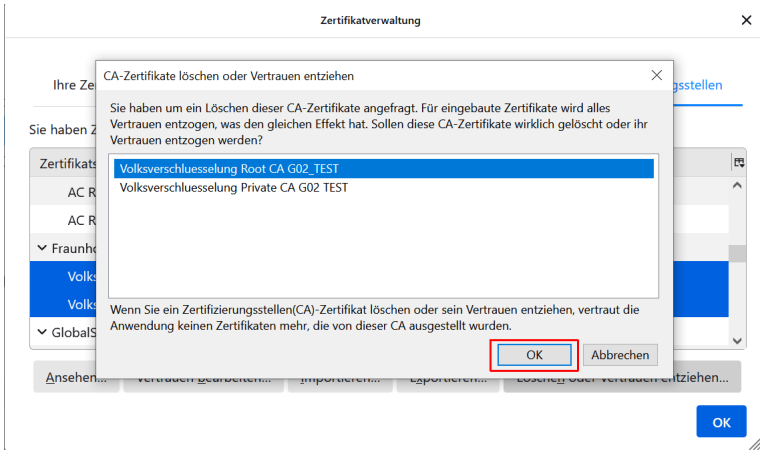


Wenn keiner Ihrer Kommunikationspartner ein Zertifikat der Volksverschlüsselung besitzt, können Sie auch die Zertifikate der *Volksverschluesselung Root-CA G02* und *Volksverschluesselung Private-CA G02* löschen.

1. Gehen Sie zum Karteireiter **Zertifizierungsstellen**. Suchen Sie nach den Zertifikaten der *Volksverschluesselung Root-CA G02* und *Volksverschluesselung Private-CA G02*, markieren Sie diese und klicken Sie auf **Löschen oder Vertrauen entziehen**.



2. Bestätigen Sie die Meldung **CA-Zertifikat löschen oder Vertrauen entziehen** mit **OK**.


Zertifikatverwaltung
CA-Zertifikate löschen oder Vertrauen entziehen
Sie haben um ein Löschen dieser CA-Zertifikate angefragt. Für eingebaute Zertifikate wird alles Vertrauen entzogen, was den gleichen Effekt hat. Sollen diese CA-Zertifikate wirklich gelöscht oder ihr Vertrauen entzogen werden?
Volksverschluesselung Root CA G02_TEST
Volksverschluesselung Private CA G02 TEST
Wenn Sie ein Zertifizierungsstellen(CA)-Zertifikat löschen oder sein Vertrauen entziehen, vertraut die Anwendung keinen Zertifikaten mehr, die von dieser CA ausgestellt wurden.
OK
Abbrechen
OK

4 Nutzung der Schlüssel/Zertifikate in Browsern

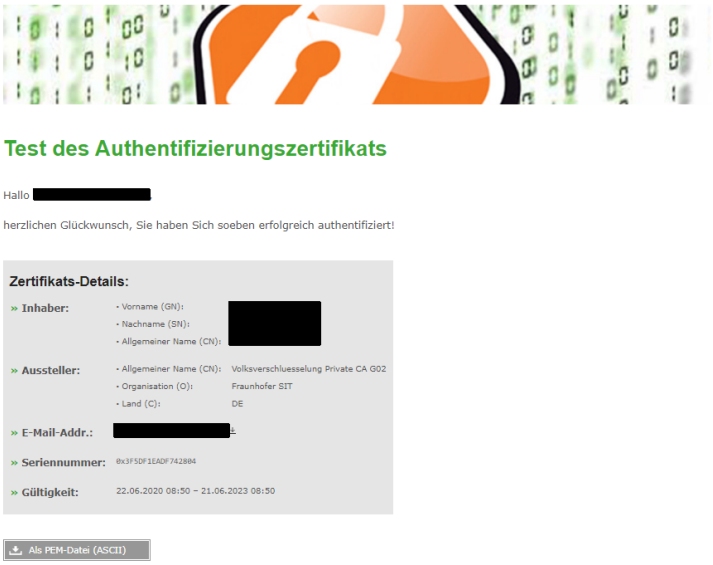
Die Volksverschlüsselungs-Software importiert alle drei Zertifikate der Volksverschlüsselung sowie das Zertifikat der *Volksverschluesselung Root-CA G02* und der *Volksverschluesselung Private-CA G02* in den Zertifikatsspeicher, der von dem jeweiligen Browser verwendet wird. Die Zertifikate stehen somit allen Anwendungen zur Verfügung, die diesen Zertifikatsspeicher nutzen.

Das Authentifizierungs-Zertifikat der Volksverschlüsselung kann für die Anmeldung an Diensten bzw. Web-Portalen verwendet werden, die eine SSL/TLS-Client-Authentifizierung verlangen.

Der folgende Link ermöglicht Ihnen, die erfolgreiche Einrichtung Ihres Browser und die Authentifizierung mittels Ihrem Authentifizierungs-Zertifikat zu testen:

https://volksverschluesselung.de/portal/

Konnte die Authentifizierung erfolgreich durchgeführt werden, wird Ihnen folgende Seite angezeigt:



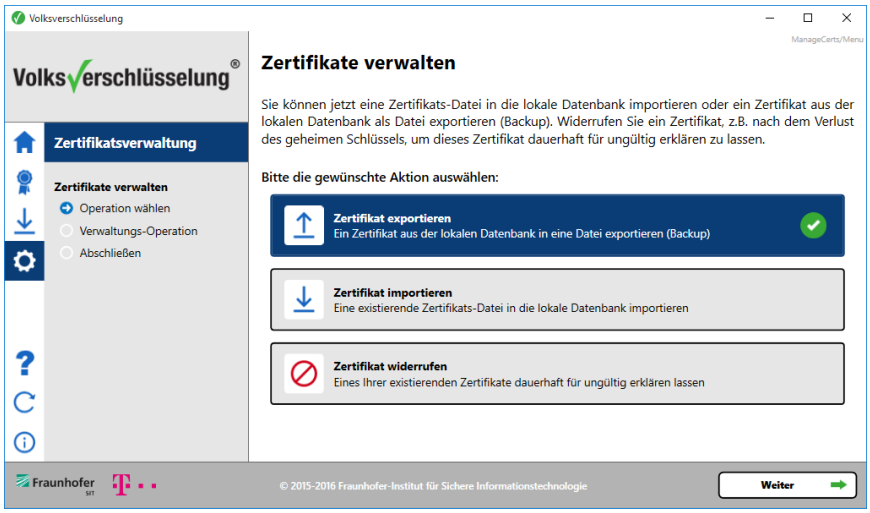
5 Nutzung der Schlüssel/Zertifikate auf anderen Rechnern

5.1 Export der Schlüssel/Zertifikate aus der Volksverschlüsselungs-Software

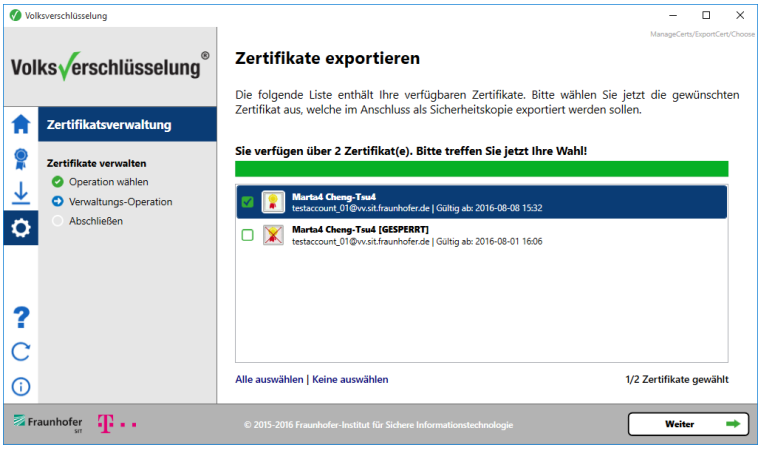
Um die Zertifikate auf anderen Rechnern nutzen zu können, müssen sie zunächst aus der Volksverschlüsselungs-Software in eine Datei exportiert werden. Um möglichst viele Zielsysteme zu unterstützen, werden drei unterschiedliche Formate zum Export bereitgestellt:

- **.vv-backup**: Die Datei enthält sowohl alle Ihre Schlüsselpaare, als auch Ihr Sperrpasswort. Dieses Exportformat sollten Sie wählen, wenn Sie Ihre Schlüssel/Zertifikate in Ihre Anwendungen auf einem anderen Windows-Rechner mit Hilfe der Volksverschlüsselungs-Software automatisch importieren möchten.
- **.zip**: Die Datei enthält alle Ihre Schlüsselpaare je eine **p12**-Datei pro Schlüsselpaar (s. nächster Punkt). Das Sperrpasswort wird nicht mitexportiert. Dieses Exportformat sollten Sie wählen, wenn Sie Ihre Schlüssel/Zertifikate auf einem iOS, Android oder Mac-Gerät verwenden möchten.
- **.p12**: Die Datei enthält alle Ihre Schlüsselpaare. Wenn Sie Ihre Schlüssel/Zertifikate in einen Schlüssel-Container im PKCS#12-Format exportieren, können Sie Ihre Schlüssel/Zertifikate auf einer anderen Betriebssystemplattform, wie beispielsweise Linux, in Ihre E-Mail-Programme und Browser manuell importieren.

1. Gehen Sie im Hauptmenü auf den Menüpunkt **Zertifikatsverwaltung** und wählen Sie **Zertifikat exportieren**.

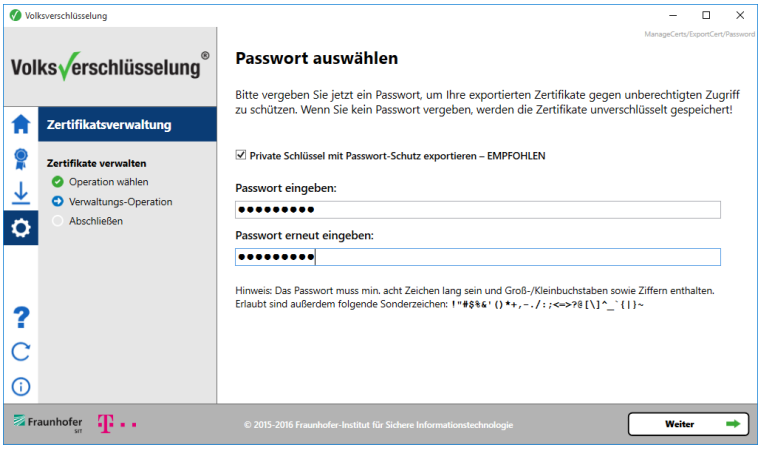


2. Sie erhalten die Möglichkeit, ein oder mehrere Schlüssel/Zertifikate auszuwählen.



3. Wählen Sie das Zielverzeichnis aus und geben Sie einen Namen ein. Alternativ können Sie den voreingestellten Namen übernehmen. Wählen Sie das Export-Format aus:

4. Geben Sie ein sicheres Passwort ein.



5.2 Verteilung auf andere Windows-Rechner

Übertragen Sie die Datei im Format **.vv-backup** auf Ihr Windows-Zielsystem. Installieren Sie die Volksverschlüsselungs-Software auf dem Zielsystem. Gehen Sie im Hauptmenü auf den Menüpunkt **Zertifikatsverwaltung** und wählen Sie **Zertifikat importieren**. Wählen Sie die Datei aus und geben Sie das beim Export ausgewählte Passwort ein.

Jetzt können Sie mit Hilfe der Volksverschlüsselungs-Software Ihre Schlüssel/Zertifikate wieder in den E-Mail-Programmen und Browsern automatisch installieren.

5.3 Verteilung der Schlüssel auf andere Plattformen, die nicht von der Volksverschlüsselungs-Software unterstützt werden

Wenn Sie normalerweise kein Windows-System nutzen, dann können Sie in einer Windows-Systemumgebung Ihre Zertifikate beantragen, diese exportieren und dann auf eine beliebige Plattform übertragen. Die Konfiguration Ihrer Anwendungen auf dem Zielsystem müssen Sie dann allerdings manuell durchführen.

5.3.1 Export für MacOS, Linux und Android

Sie können Ihre Zertifikate in eine **zip**- oder **p12**-Datei exportieren, wie in Export der Zertifikate aus der Volksverschlüsselungs-Software beschrieben. Übertragen Sie diese Datei auf Ihr Zielsystem. Die Konfiguration Ihrer Anwendungen auf dem Zielsystem müssen Sie dann allerdings manuell durchführen. Es existieren zahlreiche Anleitungen im Internet, die den Import einer P12-Datei in eine Anwendung beschreiben.

Beispielsweise für **Apple Mail** und die Android-App **R2Mail2** (Android App), finden Sie Anleitungen u.a. auf den Seiten der Universität Osnabrück. Nähere Informationen zur Nutzung der Schlüssel und Zertifikate unter Android, erhalten Sie auf Nachfrage. Senden Sie hierzu eine Mail an info@volksverschluesselung.de.

5.3.2 Export für iOS

Eine Anleitung zur Nutzung von Schlüsseln der Volksverschlüsselung unter iOS erhalten Sie auf Nachfrage. Senden Sie hierzu eine Mail an info@volksverschluesselung.de.