Fraunhofer Competence Center PKI

PKI-Contacts - PKI für Fraunhofer Kontakte

Anleitung für Kommunikationspartner der Fraunhofer-Gesellschaft

Autor[en]:
Uwe Bendisch

Stand: 03.02.2017

Version 1.2

Dokumenthistorie:

VERSION	DATUM	ÄNDERUNG	AUTOR
1.2	03.02.2017	Überarbeitung der Abschnitte 4, 4.1.2, 4.1.2.1 und 4.1.2.2	Uwe Bendisch
1.1	15.10.2013	Überarbeitung des Abschnitts 1.2	Uwe Bendisch
1.0	10.01.2012	Freigabe für Produktivbetrieb	Uwe Bendisch

Verteiler/Zielgruppe:

Dieses Dokument wendet sich an Kommunikationspartner der Fraunhofer-Gesellschaft, die ihre E-Mail-Kommunikation mit Mitarbeiterinnen und Mitarbeitern der Fraunhofer-Gesellschaft zertifikatsbasiert absichern wollen und selbst noch keine Zertifikate für diesen Zweck besitzen.

Bemerkungen/Hinweise:

Dieses Dokument wurde mit besonderer Sorgfalt bearbeitet. Für möglicherweise trotzdem vorhandene Fehler und deren Auswirkungen kann jedoch keine Haftung übernommen werden.
Anmerkungen oder Änderungswünsche zum Dokument können Sie dem CC-PKI jederzeit gerne über den Fraunhofer Service Desk (servicedesk@fraunhofer.de) mitteilen.

Interne Angaben:

Dateiname: PKI-Contacts_Anleitung_Extern (V 1.2).docx
Zeitpunkt: 03.02.2017
Bearbeiter: Uwe Bendisch

Inhalt

Einleitung 1

1 Zertifikat eines Fraunhofer Mitarbeiters erhalten 2

1.1 Ein Zertifikat per E-Mail erhalten 2

1.2 Ein Zertifikat über die Website der *PKI-Contacts* herunterladen 2

2 Ein eigenes Zertifikat beantragen 6

2.1 Ein eigenes Zertifikat mit dem Microsoft Internet Explorer beantragen 7

2.2 Ein eigenes Zertifikat mit Mozilla Firefox beantragen 10

3 Ein eigenes Zertifikat aus dem Browser exportieren 15

3.1 Ein eigenes Zertifikat aus dem Microsoft Internet Explorer exportieren 15

3.2 Ein eigenes Zertifikat aus Mozilla Firefox exportieren 24

4 Zertifikate im E-Mail-Client nutzen 27

4.1 Den E-Mail-Client für die Zertifikatsnutzung vorbereiten 27

4.1.1 Integration des Wurzelzertifikats der PKI für Fraunhofer Kontakte 27

4.1.1.1 Wurzelzertifikat der PKI für Fraunhofer Kontakte in den Microsoft-Zertifikatspeicher aufnehmen 29

4.1.1.2 Wurzelzertifikat der PKI für Fraunhofer Kontakte in den Zertifikatspeicher von Mozilla Thunderbird aufnehmen 32

4.1.2 Integration der Wurzelzertifikate / Zertifikatsketten der PKI für Fraunhofer Mitarbeiter 34

4.1.2.1 Wurzelzertifikate / Zertifikatsketten der PKI für Fraunhofer Mitarbeiter in den Microsoft-Zertifikatspeicher aufnehmen 36

4.1.2.2 Wurzelzertifikate / Zertifikatsketten der PKI für Fraunhofer Mitarbeiter in den Zertifikatspeicher von Mozilla Thunderbird aufnehmen 37

4.2 Ein eigenes Zertifikat in den E-Mail-Client aufnehmen 37
4.2.1 Ein eigenes Zertifikat in den Microsoft-Zertifikatspeicher aufnehmen 37
4.2.1.1 Ein eigenes Zertifikat in Microsoft Outlook 2010 konfigurieren 45
4.2.1.2 Ein eigenes Zertifikat in Microsoft Outlook 2007 konfigurieren 47
4.2.1.3 Ein eigenes Zertifikat in Microsoft Outlook 2003 konfigurieren 49
4.2.2 Ein eigenes Zertifikat in Mozilla Thunderbird aufnehmen und konfigurieren 52
4.3 Ein Zertifikat eines Fraunhofer Mitarbeiters in den E-Mail-Client aufnehmen 55
4.3.1 Ein Zertifikat eines Fraunhofer Mitarbeiters in Microsoft Outlook 2010 aufnehmen 56
4.3.2 Ein Zertifikat eines Fraunhofer Mitarbeiters in Microsoft Outlook 2007 aufnehmen 58
4.3.3 Ein Zertifikat eines Fraunhofer Mitarbeiters in Microsoft Outlook 2003 aufnehmen 61
4.3.4 Ein Zertifikat eines Fraunhofer Mitarbeiters in Mozilla Thunderbird aufnehmen 63
4.4 Senden von signierten und/oder verschlüsselten E-Mails 65
4.4.1 Senden von signierten und/oder verschlüsselten E-Mails mit Microsoft Outlook 2010 66
4.4.2 Senden von signierten und/oder verschlüsselten E-Mails mit Microsoft Outlook 2007 66
4.4.3 Senden von signierten und/oder verschlüsselten E-Mails mit Microsoft Outlook 2003 67
4.4.4 Senden von signierten und/oder verschlüsselten E-Mails mit Mozilla Thunderbird 69

5 Ein eigenes Zertifikat sperren 70

5.1 Anforderung der Zertifikatssperrung eines eigenen Zertifikats per E-Mail 70
5.2 Ein eigenes Zertifikat mit Hilfe der Revozierungsnachricht endgültig sperren 72

Einleitung

Innerhalb dieses Dokuments wird beschrieben, wie Sie sicher mit Mitarbeiterinnen und Mitarbeitern der Fraunhofer-Gesellschaft über E-Mail kommunizieren können.

Für eine verschlüsselte Kommunikation benötigen Sie und der Fraunhofer Mitarbeiter jeweils ein digitales Zertifikat. Fraunhofer Mitarbeiter sind bereits weitestgehend mit digitalen Zertifikaten ausgestattet.

Um auch Ihnen die Möglichkeit zu geben, ein Zertifikat für die Kommunikation mit Fraunhofer zu erhalten, betreibt die Fraunhofer-Gesellschaft, genauer: das Competence Center Public Key Infrastructures der Fraunhofer-Gesellschaft, eine eigene Public Key Infrastruktur (PKI), die von der PKI für Fraunhofer Mitarbeiter vollständig getrennt ist. Sie wird als *PKI-Contacts* bezeichnet (PKI für Fraunhofer Kontakte) und stellt Zertifikate für externe Kommunikationspartner von Fraunhofer Mitarbeiterinnen und Mitarbeitern zur Verfügung.

Die für Sie ausgestellten Zertifikate eignen sich auch für die Signatur von E-Mails. Die Empfänger einer solchen E-Mail können sich sicher sein, dass die Nachricht auch tatsächlich von Ihnen stammt und während der Übertragung nicht verändert wurde.

Es ist zu beachten, dass die Ausstellung von Zertifikaten der *PKI-Contacts* nur auf Initiative eines Mitarbeiters der Fraunhofer-Gesellschaft möglich ist.

Hinweis: Die in dieser Anleitung enthaltenen Screenshots wurden – sofern nicht anders angegeben – unter Verwendung von Mozilla Firefox in den Versionen 6 bis 9 unter Windows 7 erstellt. Je nach Betriebssystem bzw. verwendetem Browser kann das Erscheinungsbild einzelner Dialoge variieren. Auch können Browser-interne Abläufe insbesondere in Bezug auf die Auswahl von Zertifikaten oder die PIN-Eingabe der Smartcard je nach Produkt geringfügig unterschiedlich sein.

1 Zertifikat eines Fraunhofer Mitarbeiters erhalten

Um einem Fraunhofer Mitarbeiter eine verschlüsselte E-Mail zu senden, benötigen Sie dessen digitales Verschlüsselungszertifikat. Dieses Zertifikat können Sie per E-Mail erhalten oder über die Webseite https://contacts.pki.fraunhofer.de herunterladen.

1.1 Ein Zertifikat per E-Mail erhalten

Um das Verschlüsselungszertifikat des Fraunhofer Mitarbeiters über E-Mail zu beziehen, bitten Sie ihn, Ihnen eine signierte E-Mail zu senden. Sind die Wurzelzertifikate und die übrigen Zertifikate der Zertifikatsketten der PKI für Fraunhofer Mitarbeiter korrekt in Ihren E-Mail-Client eingebunden (siehe Abschnitt 4.1.2), so steht das Zertifikat des Fraunhofer Mitarbeiters nun zur sicheren Kommunikation über E-Mail zur Verfügung. Sie können direkt auf die E-Mail des Fraunhofer Mitarbeiters mit einer verschlüsselten E-Mail antworten.

Hinweis: Die Wurzelzertifikate und die zugehörigen Zertifikate der Zertifikatsketten der PKI für Fraunhofer Mitarbeiter müssen Sie nur einmalig in den Zertifikatspeicher Ihres E-Mail-Programms importieren.

1.2 Ein Zertifikat über die Website der *PKI-Contacts* herunterladen

Möchten Sie einem Fraunhofer Mitarbeiter eine verschlüsselte E-Mail senden, der bereits über ein gültiges Zertifikat der Fraunhofer-PKI verfügt – Sie aber noch nicht im Besitz dieses Zertifikats sind –, so kann dieses Zertifikat über die Seite https://contacts.pki.fraunhofer.de bezogen werden.

Öffnen Sie die den Link in Ihrem Browser und wählen Sie anschließend im Bereich **Für Kommunikationspartner** den Menüeintrag **Zertifikat eines Fraunhofer Mitarbeiters suchen** (vgl. Abbildung 1).

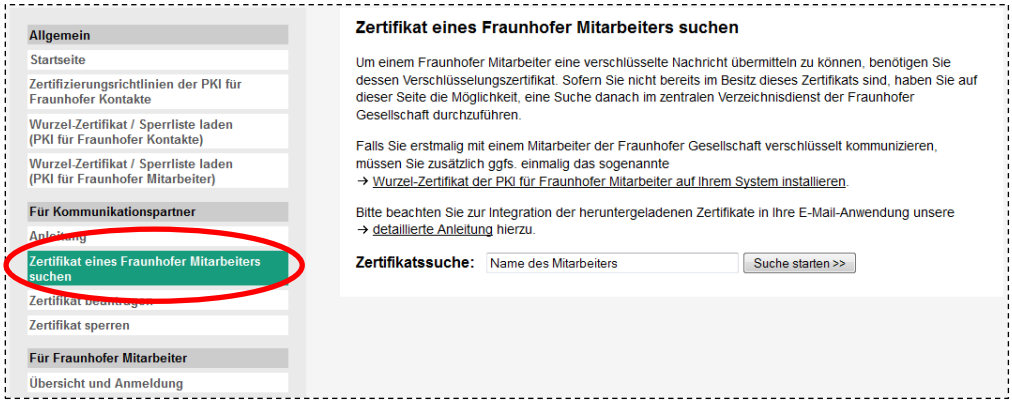


Abbildung 1: Eingabemaske zur Suche nach Zertifikaten von Fraunhofer Mitarbeitern

Geben Sie nun den Nachnamen des Fraunhofer Mitarbeiters ein, nach dessen Zertifikat Sie suchen wollen und klicken Sie auf die Schaltfläche **Suchen starten**.

Hinweis: Es ist auch möglich nur einen Teil des Namens anzugeben. Es werden dann im Suchergebnis Fraunhofer Mitarbeiter aufgelistet, deren Nachname den von Ihnen angegebenen Bestandteil enthalten.

Hinweis: Aus Datenschutzgründen ist die Anzahl der Treffer in der Ausgabe auf drei beschränkt. Sofern der von Ihnen gesuchte Fraunhofer Mitarbeiter in der Trefferliste nicht enthalten ist, ist es ggfs. sinnvoll den Suchausdruck spezieller zu gestalten, d. h. einen Suchausdruck zu verwenden, der mehr Zeichen umfasst.

Falls ein Fraunhofer Mitarbeiter gefunden wurde, der dem den von Ihnen eingegebenen Namen entspricht, erhalten Sie eine Anzeige der öffentlich verfügbaren Daten des Mitarbeiters wie in Abbildung 2 dargestellt. Sofern der Fraunhofer Mitarbeiter über ein Verschlüsselungszertifikat verfügt, sind Angaben hierzu im Abschnitt *Zertifikat* angegeben.

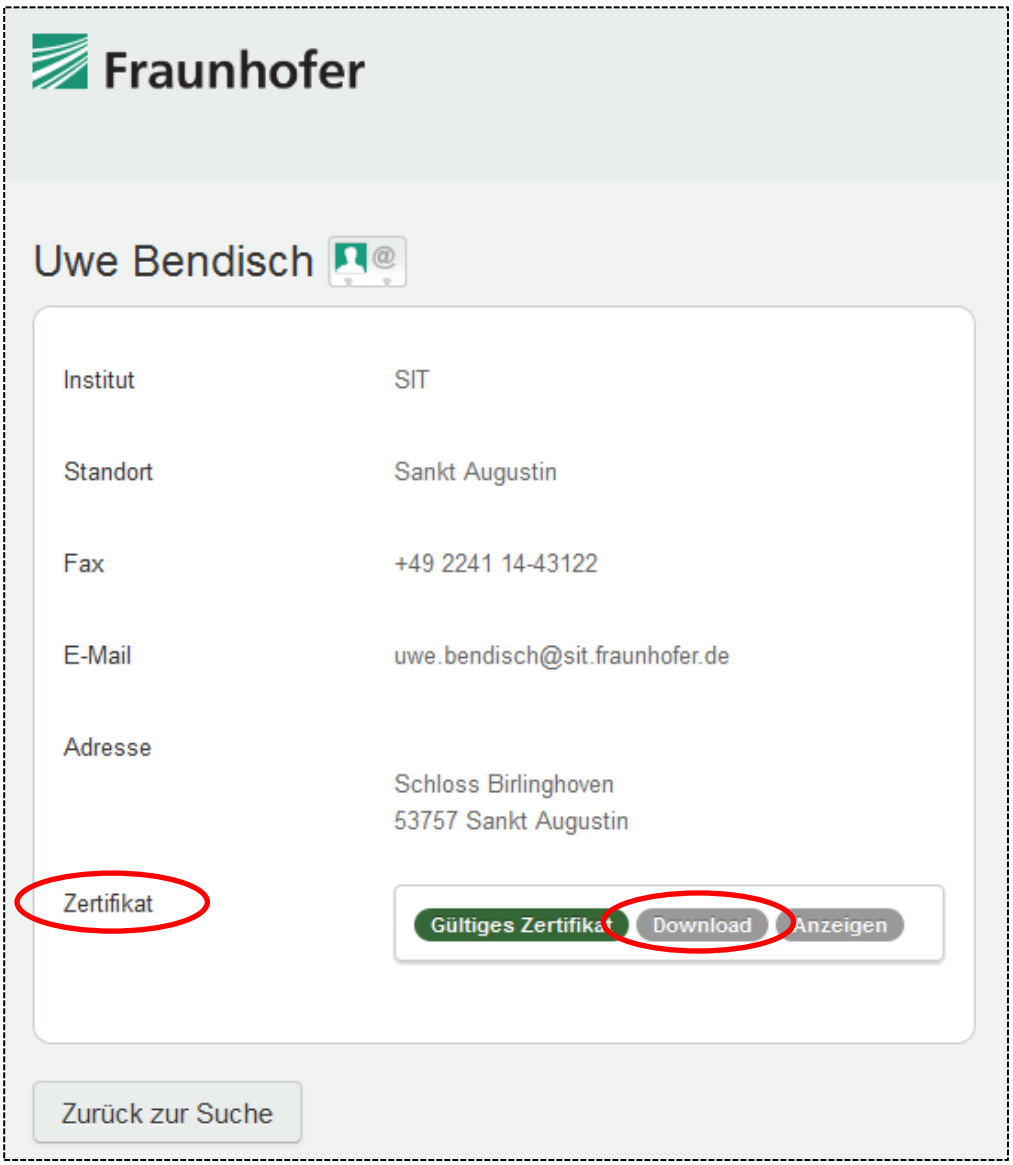


Abbildung 2: Ergebnis der Suche nach einem Zertifikat eines Fraunhofer Mitarbeiters

Um ein gültiges Zertifikat auf Ihrem Computer zu speichern, klicken auf die Schaltfläche **Download** und wählen Sie die Option **Datei speichern**.

Wechseln Sie nun zu dem Ordner, in dem das Zertifikat gespeichert werden soll und klicken Sie auf **Speichern**. Sie können den vorgeschlagenen Dateinamen ersetzen oder ändern, achten Sie jedoch darauf, dass die Dateiendung *.cer* erhalten bleibt (vgl. Abbildung 3).

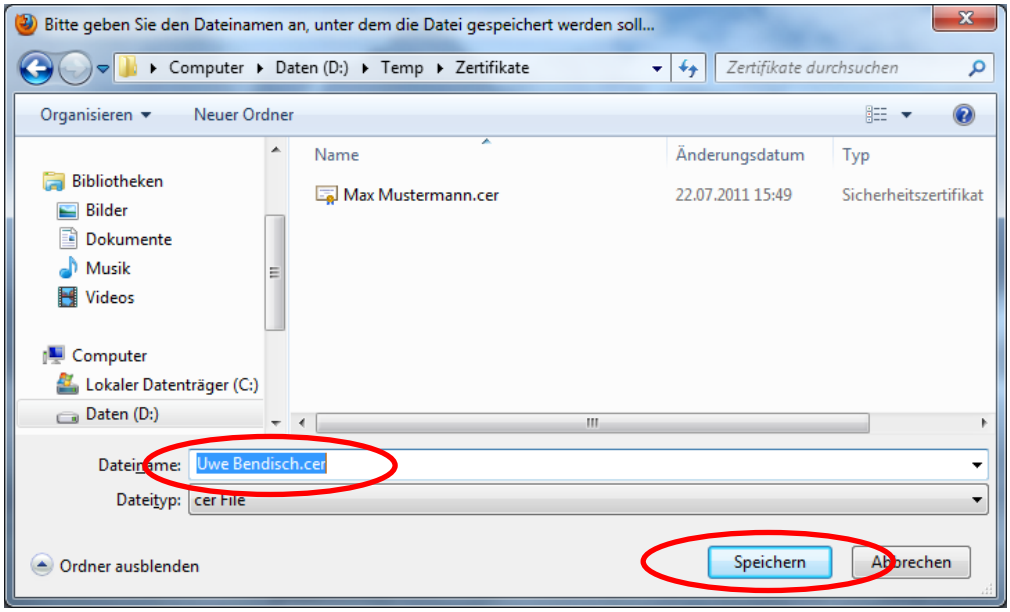


Abbildung 3: Speichern des Zertifikats eines Fraunhofer Mitarbeiters

Wie das Zertifikat in Ihren E-Mail-Client eingebunden werden kann, damit es zur sicheren Kommunikation verwendet werden kann, ist vom verwendeten E-Mail-Client abhängig und wird im Abschnitt 4.3 beschrieben.

2 Ein eigenes Zertifikat beantragen

Für die sichere E-Mail-Kommunikation mit Fraunhofer benötigen Sie ebenfalls ein Zertifikat, das für Ihre E-Mail-Adresse ausgestellt ist. Sofern Sie noch kein eigenes Zertifikat besitzen, können Sie ein kostenloses Zertifikat der PKI für Fraunhofer Kontakte (*PKI-Contacts*) erhalten.

Voraussetzung dafür ist, dass ein Fraunhofer Mitarbeiter, der Sie kennt, die Zertifikatsbeantragung für Sie initiiert. Bitten Sie also den Fraunhofer Mitarbeiter, mit dem Sie in Kontakt stehen, dies für Sie zu tun. Die eigentliche Schlüsselerzeugung und Zertifikatsbeantragung nehmen Sie dann im Anschluss selbst vor.

Auf der Webseite https://contacts.pki.fraunhofer.de gibt es hierzu einen zugangsgeschützten Bereich für Fraunhofer Mitarbeiter, über den diese die Ausstellung von Zertifikaten für Kommunikationspartner autorisieren können.

Im Laufe dieses Prozesses erhalten Sie dann eine automatisch erzeugte E-Mail mit einem Link (vgl. Abbildung 4), der Sie auf eine spezielle Webseite der *PKI-Contacts* leitet, die Sie durch die Zertifikatsbeantragung führt. Klicken Sie auf den in der E-Mail angegebenen Link oder kopieren Sie ihn in die Adressleiste Ihres Browsers.

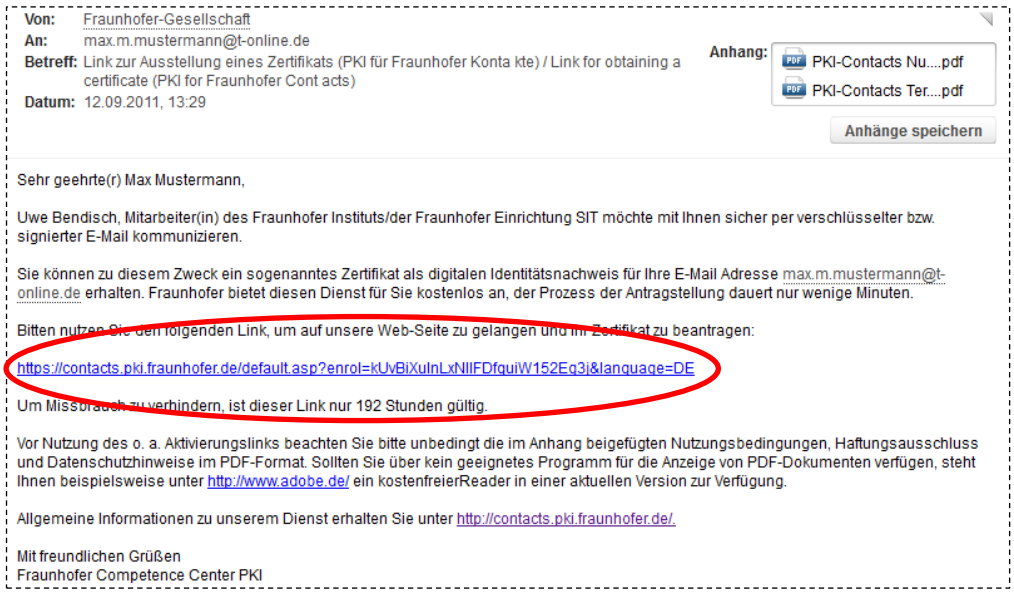


Abbildung 4: E-Mail mit Link zur Ausstellung eines Zertifikats

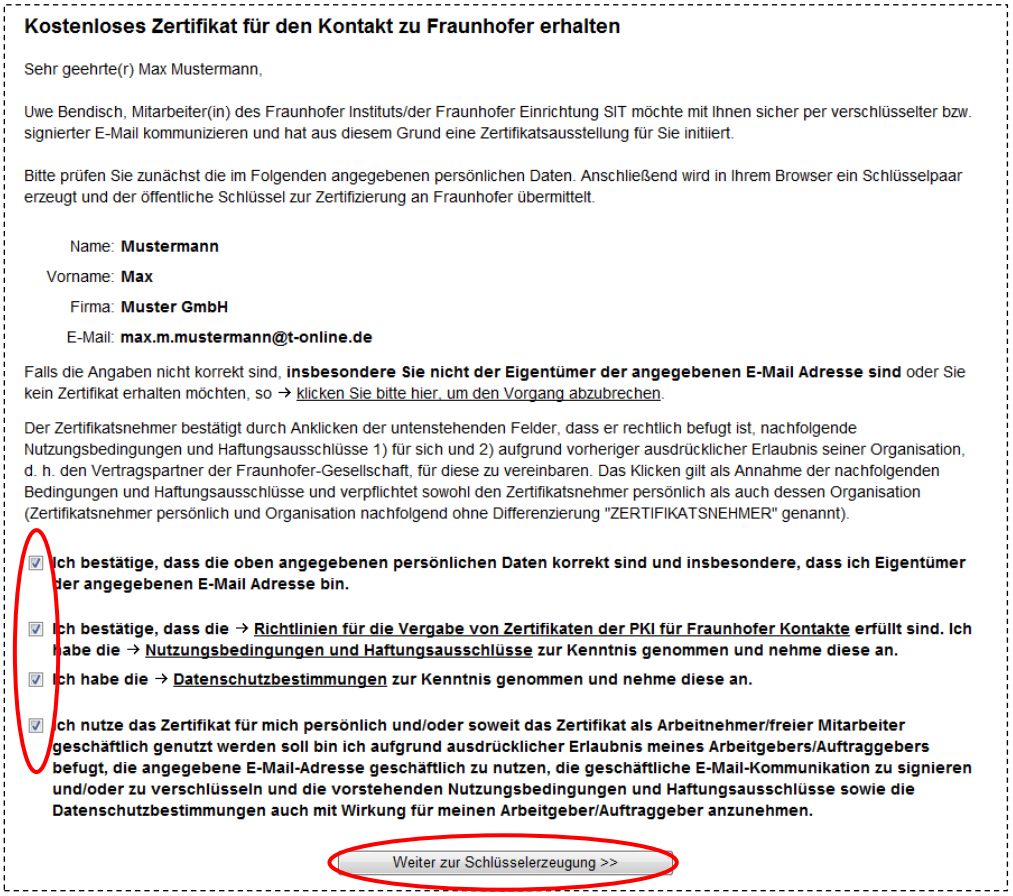
Hinweis: Bitte beachten Sie, dass der Link aus Sicherheitsgründen ein Identifikationsmerkmal erhält, das nur für Sie gültig ist. Ferner ist eine Nutzung des Links nur innerhalb von 192 Stunden nach Versand der E-Mail möglich. Sollten

Sie innerhalb dieser Frist keine Zertifikatsbeantragung durchführen, müssen Sie bei Ihrer Kontaktperson in der Fraunhofer-Gesellschaft eine erneute Autorisierung beantragen.

2.1 Ein eigenes Zertifikat mit dem Microsoft Internet Explorer beantragen

Hinweis: Die Screenshots wurden unter Verwendung des Microsoft Internet Explorers in der Version 9 angefertigt.

Der Link aus der automatisch erzeugten E-Mail leitet Sie auf eine Webseite, die Sie durch die Zertifikatsbeantragung führt (vgl. Abbildung 5).



Kostenloses Zertifikat für den Kontakt zu Fraunhofer erhalten

Sehr geehrte(r) Max Mustermann,

Uwe Bendisch, Mitarbeiter(in) des Fraunhofer Instituts/der Fraunhofer Einrichtung SIT möchte mit Ihnen sicher per verschlüsselter bzw. signierter E-Mail kommunizieren und hat aus diesem Grund eine Zertifikatsausstellung für Sie initiiert.

Bitte prüfen Sie zunächst die im Folgenden angegebenen persönlichen Daten. Anschließend wird in Ihrem Browser ein Schlüsselpaar erzeugt und der öffentliche Schlüssel zur Zertifizierung an Fraunhofer übermittelt.

Name: **Mustermann**
Vorname: **Max**
Firma: **Muster GmbH**
E-Mail: **max.m.mustermann@t-online.de**

Falls die Angaben nicht korrekt sind, **insbesondere Sie nicht der Eigentümer der angegebenen E-Mail Adresse sind** oder Sie kein Zertifikat erhalten möchten, so → klicken Sie bitte hier, um den Vorgang abzubrechen.

Der Zertifikatsnehmer bestätigt durch Anklicken der untenstehenden Felder, dass er rechtlich befugt ist, nachfolgende Nutzungsbedingungen und Haftungsausschlüsse 1) für sich und 2) aufgrund vorheriger ausdrücklicher Erlaubnis seiner Organisation, d. h. den Vertragspartner der Fraunhofer-Gesellschaft, für diese zu vereinbaren. Das Klicken gilt als Annahme der nachfolgenden Bedingungen und Haftungsausschlüsse und verpflichtet sowohl den Zertifikatsnehmer persönlich als auch dessen Organisation (Zertifikatsnehmer persönlich und Organisation nachfolgend ohne Differenzierung "ZERTIFIKATSNEHMER" genannt).

☑ **Ich bestätige, dass die oben angegebenen persönlichen Daten korrekt sind und insbesondere, dass ich Eigentümer der angegebenen E-Mail Adresse bin.**

☑ **Ich bestätige, dass die → Richtlinien für die Vergabe von Zertifikaten der PKI für Fraunhofer Kontakte erfüllt sind. Ich habe die → Nutzungsbedingungen und Haftungsausschlüsse zur Kenntnis genommen und nehme diese an.**

☑ **Ich habe die → Datenschutzbestimmungen zur Kenntnis genommen und nehme diese an.**

☑ **Ich nutze das Zertifikat für mich persönlich und/oder soweit das Zertifikat als Arbeitnehmer/freier Mitarbeiter geschäftlich genutzt werden soll bin ich aufgrund ausdrücklicher Erlaubnis meines Arbeitgebers/Auftraggebers befugt, die angegebene E-Mail-Adresse geschäftlich zu nutzen, die geschäftliche E-Mail-Kommunikation zu signieren und/oder zu verschlüsseln und die vorstehenden Nutzungsbedingungen und Haftungsausschlüsse sowie die Datenschutzbestimmungen auch mit Wirkung für meinen Arbeitgeber/Auftraggeber anzunehmen.**

Weiter zur Schlüsselerzeugung >>

Abbildung 5: Zertifikatsaustellung mit dem Internet Explorer – Prüfung der Daten und Bestätigung der Kenntnisnahme der Richtlinien für die Vergabe von Zertifikaten etc.

Prüfen und bestätigen Sie nun, dass Ihre persönlichen Daten korrekt sind und bestätigen Sie ferner die Kenntnisnahme und Einhaltung der übrigen aufgeführ-

ten Bedingungen und Haftungsausschlüsse, insbesondere dass Sie die Richtlinien für die Vergabe von Zertifikaten der PKI für Fraunhofer Kontakte zur Kenntnis genommen haben und erfüllen werden.

Wenn Sie die Schaltfläche **Weiter zur Schlüsselerzeugung** anklicken, werden Ihnen Ihre Eingaben und Bestätigungen nochmals in der Zusammenfassung angezeigt (vgl. Abbildung 6). Sie haben darüber hinaus die Möglichkeit, den Vorgang der Zertifikatserstellung noch abzubrechen. Sie erhalten dann kein Zertifikat.

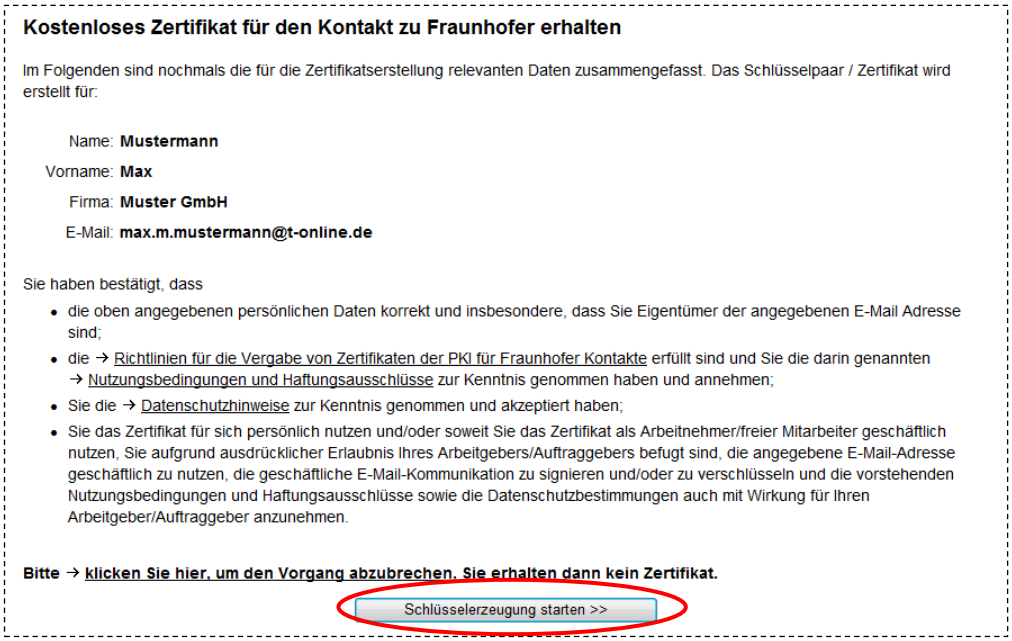


Abbildung 6: Zertifikatsaustellung mit dem Internet Explorer – Zusammenfassung der Eingaben und Bestätigungen der Kenntnisnahmen

Klicken Sie auf die Schaltfläche **Schlüsselerzeugung starten**, um in Ihrem Browser ein kryptografisches Schlüsselpaar zu generieren und dessen öffentlichen Schlüssel an den Webserver zu übermitteln, der daraus Ihr Zertifikat erzeugt. Da es sich hierbei um einen sicherheitskritischen Vorgang handelt, weist der Internet Explorer Sie auf diesen Vorgang explizit hin und fordert Ihre Zustimmung (vgl. Abbildung 7). Bestätigen Sie die Sicherheitsabfrage bitte mit **Ja** und warten Sie einen Moment bis die Schlüsselerzeugung abgeschlossen ist.

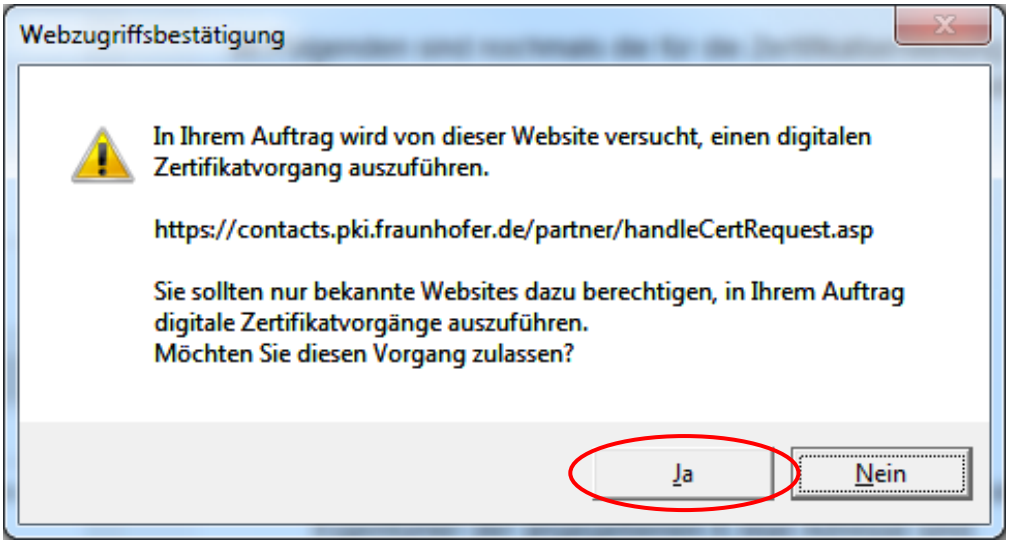


Abbildung 7: Zertifikatsaustellung mit dem Internet Explorer – Sicherheitsabfrage im Rahmen der Schlüsselerzeugung

War die Schlüsselgenerierung und Zertifikatserstellung erfolgreich, so erhalten Sie nun die Nachricht, dass das Zertifikat installiert werden kann. Klicken Sie dazu auf den Link **Ihr Zertifikat installieren** (vgl. Abbildung 8). Mittels dieses Vorgangs wird das Zertifikat im Zertifikatspeicher des Internet Explorers (Microsoft-Zertifikatspeicher) installiert.

Abbildung 8: Zertifikatsaustellung mit dem Internet Explorer – Bestätigung der erfolgreichen Zertifikatausstellung

Der Internet-Explorer weist Sie mit derselben Meldung wie sie in Abbildung 7 dargestellt ist, darauf hin, dass die Installation des Zertifikats ein mögliches Sicherheitsrisiko darstellen kann. Bestätigen Sie die Sicherheitsabfrage bitte mit der Schaltfläche **Ja**.

Sie erhalten nun die Meldung, dass das Zertifikat erfolgreich in Ihrem Browser installiert wurde (vgl. Abbildung 9).

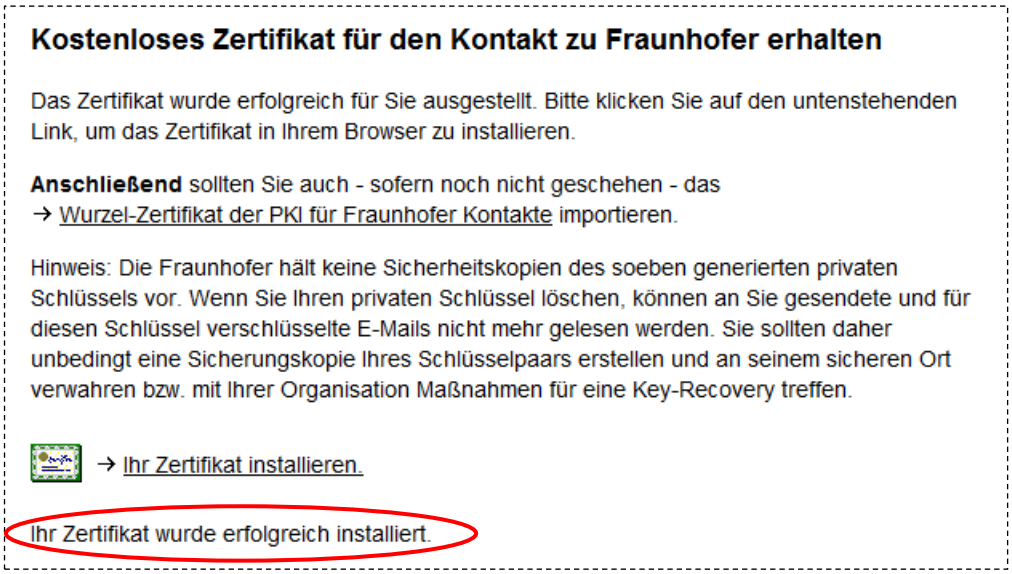


Abbildung 9: Zertifikatsaustellung mit dem Internet Explorer – Bestätigung der Zertifikatinstallation

Um das Zertifikat in Ihrem E-Mail-Client verwenden zu können, muss es nun ggfs. aus dem Browser exportiert und in Ihren E-Mail-Client importiert werden. Dieser Vorgang ist abhängig vom verwendeten Browser bzw. E-Mail-Client. Der Zertifikatexport aus dem Internet Explorer wird im Abschnitt 3.1 beschrieben und die Nutzung des persönlichen Zertifikats in verschiedenen E-Mail-Clients im Kapitel 4.

Hinweis: Bitte beachten Sie, dass ein Zertifikatexport aus dem Internet Explorer nicht notwendig ist, falls Sie Ihr Zertifikat mit einem E-Mail-Client nutzen, der ebenfalls auf den Microsoft Zertifikatspeicher zugreift (wie beispielsweise Microsoft Outlook). In diesen Fällen ist es ausreichend, das Zertifikat im E-Mail-Client zu konfigurieren (vgl. Kapitel 4)

2.2 Ein eigenes Zertifikat mit Mozilla Firefox beantragen

Der Link aus der automatisch erzeugten E-Mail leitet Sie auf eine Webseite, die Sie durch die Zertifikatsbeantragung führt (vgl. Abbildung 10).

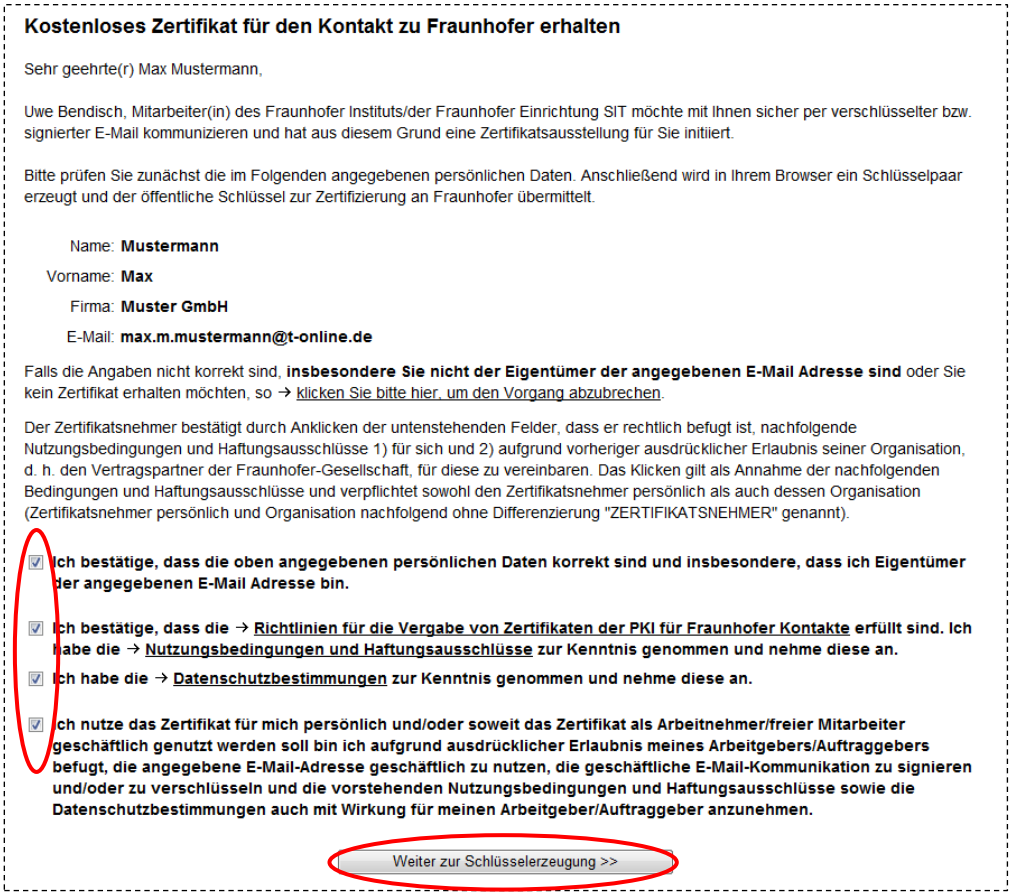


Abbildung 10: Zertifikatsaustellung mit Mozilla Firefox – Prüfung der Daten und Bestätigung der Kenntnisnahme der Richtlinien für die Vergabe von Zertifikaten etc.

Prüfen und bestätigen Sie nun, dass Ihre persönlichen Daten korrekt sind und bestätigen Sie ferner die Kenntnisnahme und Einhaltung der übrigen aufgeführten Bedingungen und Haftungsausschlüsse, insbesondere dass Sie die Richtlinien für die Vergabe von Zertifikaten der PKI für Fraunhofer Kontakte zur Kenntnis genommen haben und erfüllen werden.

Wenn Sie die Schaltfläche **Weiter zur Schlüsselerzeugung** anklicken, werden Ihnen Ihre Eingaben und Bestätigungen nochmals in der Zusammenfassung angezeigt (vgl. Abbildung 11). Sie haben darüber hinaus die Möglichkeit, den Vorgang der Zertifikatserstellung noch abzubrechen. Sie erhalten dann kein Zertifikat.

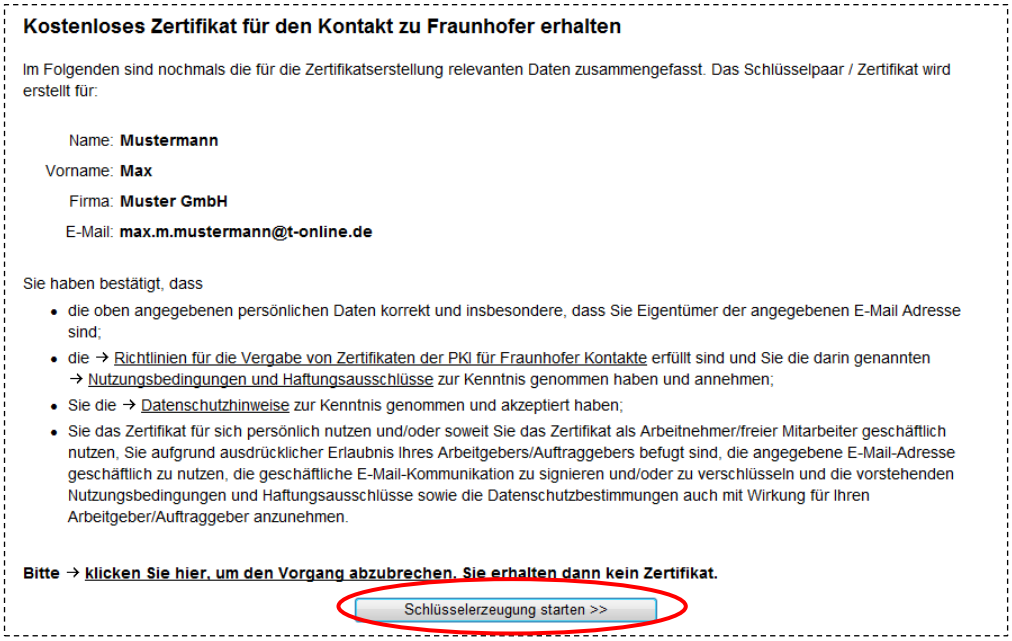


Abbildung 11: Zertifikatsaustellung mit Mozilla Firefox – Zusammenfassung der Eingaben und Bestätigungen der Kenntnisnahmen

Klicken Sie auf die Schaltfläche **Schlüsselerzeugung starten**, um in Ihrem Browser ein kryptografisches Schlüsselpaar zu generieren und dessen öffentlichen Schlüssel an den Webserver zu übermitteln, der daraus Ihr Zertifikat erzeugt.

Sofern an Ihrem Rechner ein Lesegerät für Smartcards angeschlossen und eine Karte gesteckt ist, müssen Sie zunächst im Token-Wahl-Dialog auswählen, wo das zu erstellende Schlüsselpaar bzw. Zertifikat abgelegt werden soll (vgl. Abbildung 12). Wählen Sie **Software-Sicherheitsmodul** und bestätigen Sie mit der Schaltfläche **OK**.

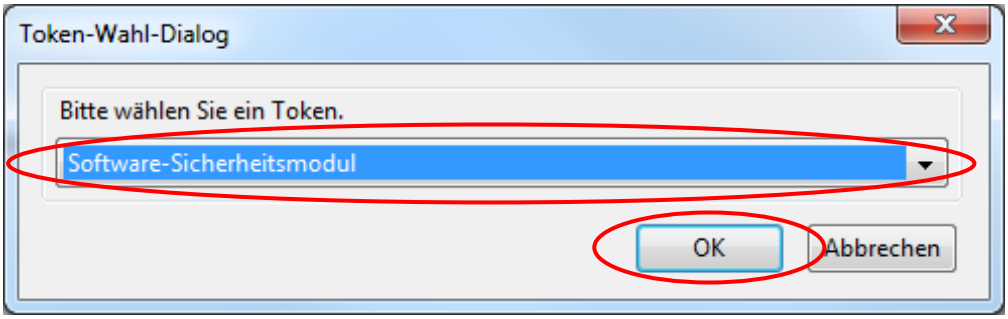


Abbildung 12: Zertifikatsaustellung mit Mozilla Firefox – Auswahl des Speicherorts für das Schlüsselpaar bzw. Zertifikat

Hinweis: Ist an Ihrem Rechner kein solches Lesegerät angeschlossen oder steckt keine geeignete Karte im Lesegerät wird der o. a. Dialog nicht angezeigt.

Hinweis: Falls Sie in Ihrem Browser die Verwendung des Master-Kennworts aktiviert haben, werden Sie nun aufgefordert, dieses Passwort für den Zugriff auf Ihr Software-Sicherheitsmodul anzugeben. Das Passwort wird benötigt, da Ihr persönliches Zertifikat im Zertifikatsspeicher des Browsers gespeichert wird.

Anschließend erhalten Sie die Meldung, dass Ihr Schlüssel generiert wird (vgl. Abbildung 13).

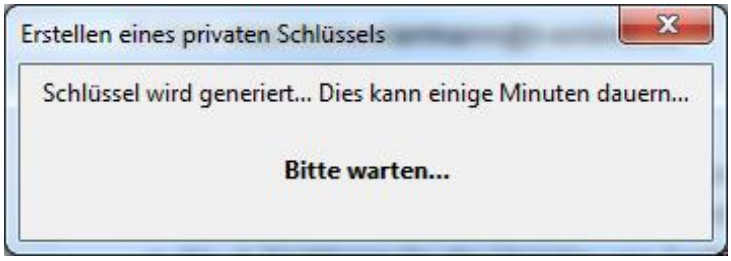


Abbildung 13: Zertifikatsaustellung mit Mozilla Firefox – Erstellung des Schlüsselpaars

War die Schlüsselgenerierung und Zertifikatserstellung erfolgreich, so erhalten Sie nun die Nachricht, dass das Zertifikat installiert werden kann. Klicken Sie dazu auf den Link **Ihr Zertifikat installieren** (vgl. Abbildung 14). Mittels dieses Vorgangs wird das Zertifikat im Firefox Zertifikatspeicher installiert.

Abbildung 14: Zertifikatsaustellung mit Mozilla Firefox – Bestätigung der erfolgreichen Zertifikatausstellung

Mozilla Firefox meldet die erfolgreiche Installation des Zertifikats in einem separaten Fenster (vgl. Abbildung 15). Sie werden explizit darauf hingewiesen, dass

Sie eine Sicherungskopie des Zertifikats anlegen sollten. Bestätigen Sie diesen Hinweis mit **OK**.

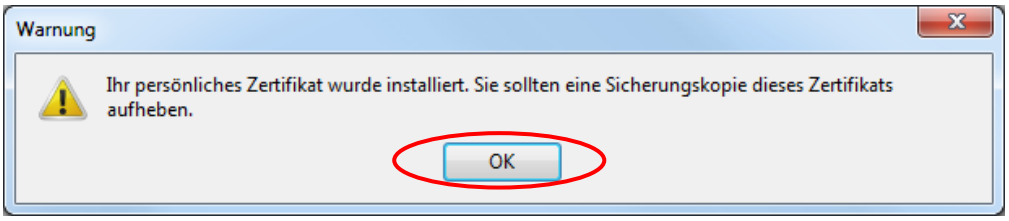


Abbildung 15: Zertifikatsaustellung mit Mozilla Firefox – Bestätigung der Zertifikatinstallation

Um das Zertifikat in Ihrem E-Mail-Client verwenden zu können, muss es nun aus dem Browser exportiert und in Ihren E-Mail-Client importiert werden. Dieser Vorgang ist abhängig vom verwendeten Browser bzw. E-Mail-Client. Der Zertifikatexport aus Mozilla Firefox wird im Abschnitt 3.2 beschrieben und die Nutzung des persönlichen Zertifikats in verschiedenen E-Mail-Clients im Kapitel 4.

3 Ein eigenes Zertifikat aus dem Browser exportieren

In diesem Kapitel wird beschrieben, wie eigene Zertifikate aus dem Browser exportiert werden können.

Ein Export der Zertifikate und zugehörigen privaten Schlüssel ist notwendig, um lokale Sicherungskopien der Zertifikate anzufertigen. Des Weiteren ist es bei einigen Kombinationen aus Browser und E-Mail-Client notwendig, die Zertifikate (und privaten Schlüssel) manuell in den jeweiligen E-Mail-Client zu integrieren. Auf die Besonderheiten der einzelnen Kombinationen wird in den folgenden Abschnitten hingewiesen.

3.1 Ein eigenes Zertifikat aus dem Microsoft Internet Explorer exportieren

Hinweis: Verwenden Sie den Internet Explorer in Kombination mit Microsoft Outlook oder einem anderen E-Mail-Programm, das auf den Microsoft-Zertifikatspeicher zugreift, ist für den sicheren E-Mail-Verkehr kein Export des persönlichen Zertifikats bzw. Schlüssels notwendig. Es wird jedoch empfohlen, dennoch eine Sicherungskopie des Zertifikats (und privaten Schlüssels) anzufertigen.

Öffnen Sie zunächst den Zertifikatspeicher von Microsoft, der aus dem Internet Explorer unter **Extras → Internetoptionen → Inhalte → Zertifikate** erreicht werden kann (vgl. Abbildung 16).

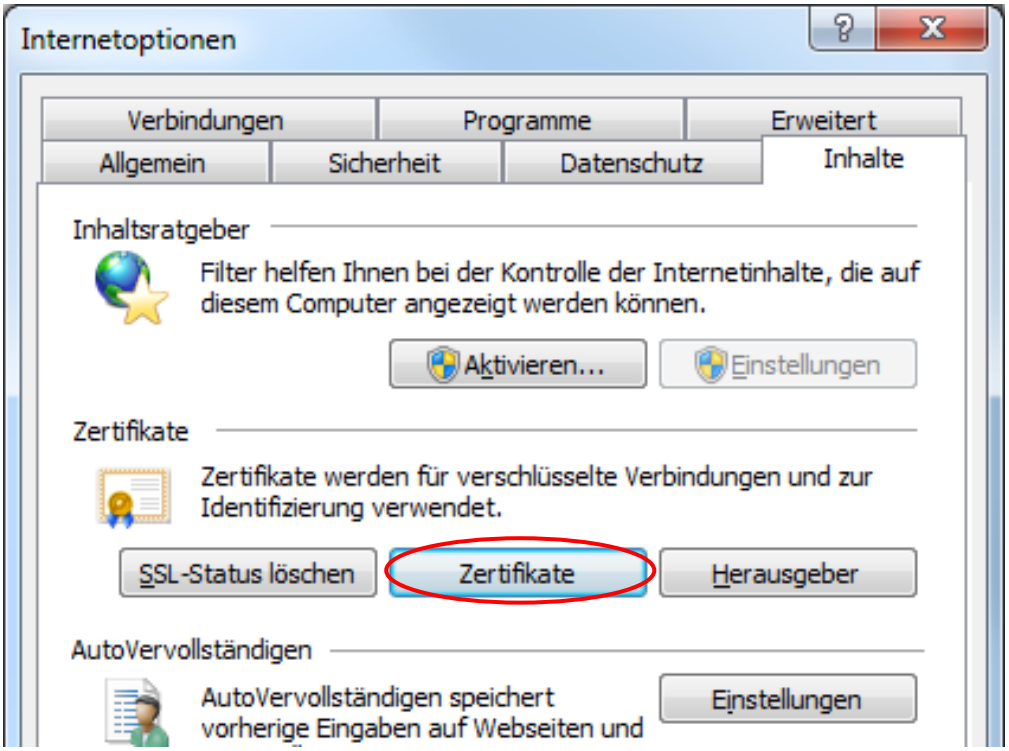


Abbildung 16: Öffnen des Microsoft-Zertifikatspeichers über den Microsoft Internet Explorer

Markieren Sie anschließend im Reiter **Eigene Zertifikate** das zu exportierende Zertifikat und klicken Sie auf die Schaltfläche **Exportieren** (vgl. Abbildung 17).

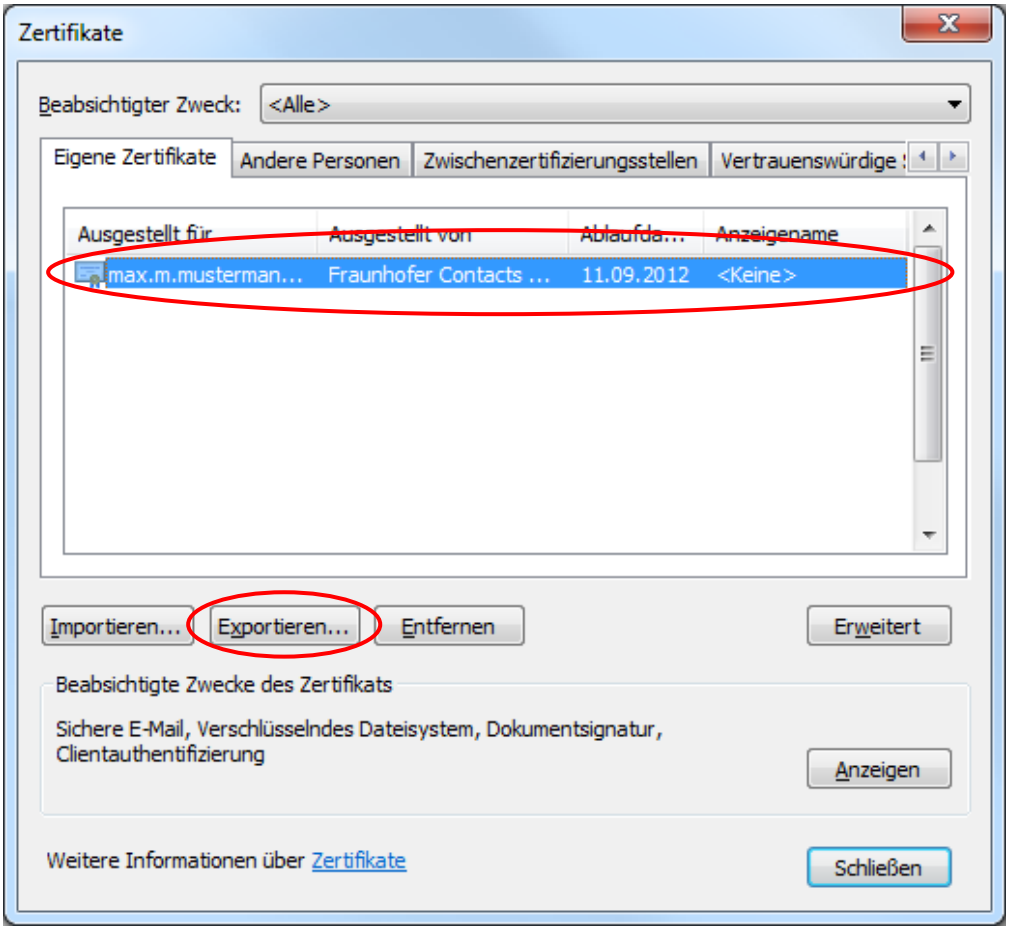


Abbildung 17: Auswahl des zu exportierenden Zertifikats im Microsoft-Zertifikatspeicher

Es wird nun der Microsoft Zertifikatexport-Assistent geöffnet, der Sie durch den Exportvorgang begleitet. Betätigen Sie die Schaltfläche **Weiter** (vgl. Abbildung 18).

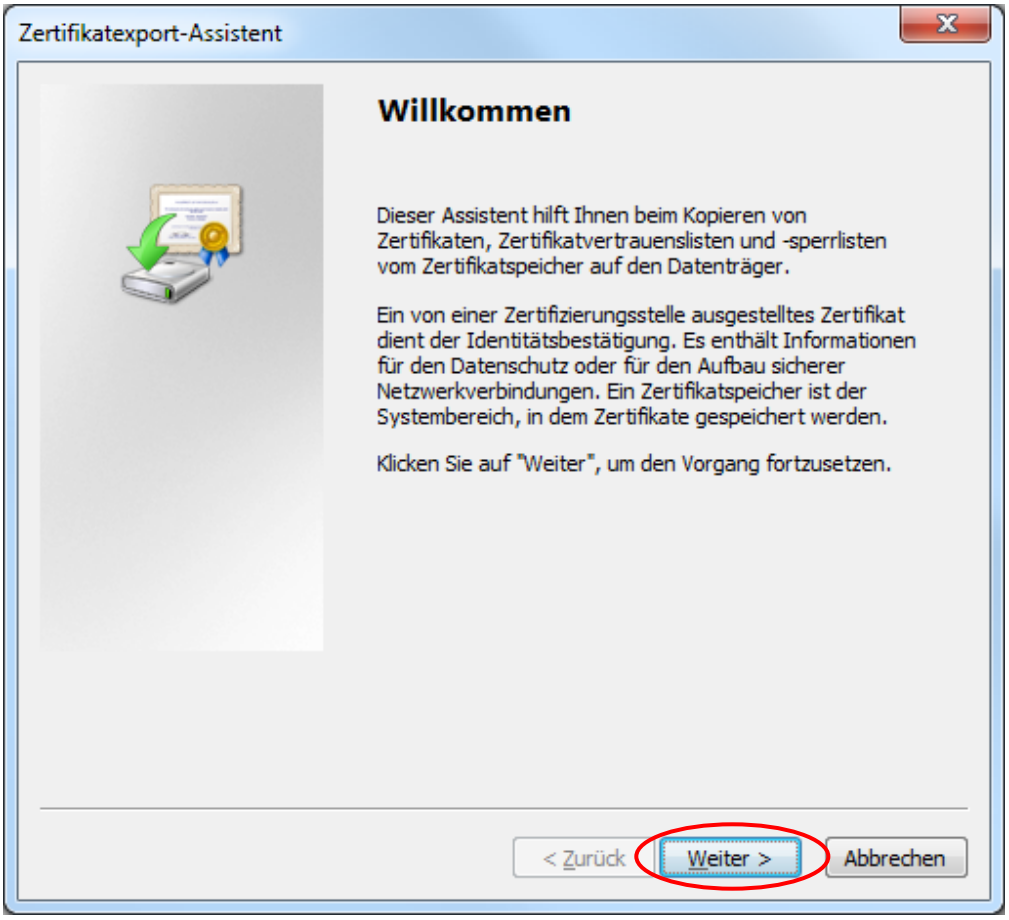


Abbildung 18: Microsoft Zertifikatexport-Assistent

Wählen Sie im folgenden Dialog die Option **Ja, privaten Schlüssel exportieren** und bestätigen Sie den Dialog durch die Schaltfläche **Weiter** (vgl. Abbildung 19).

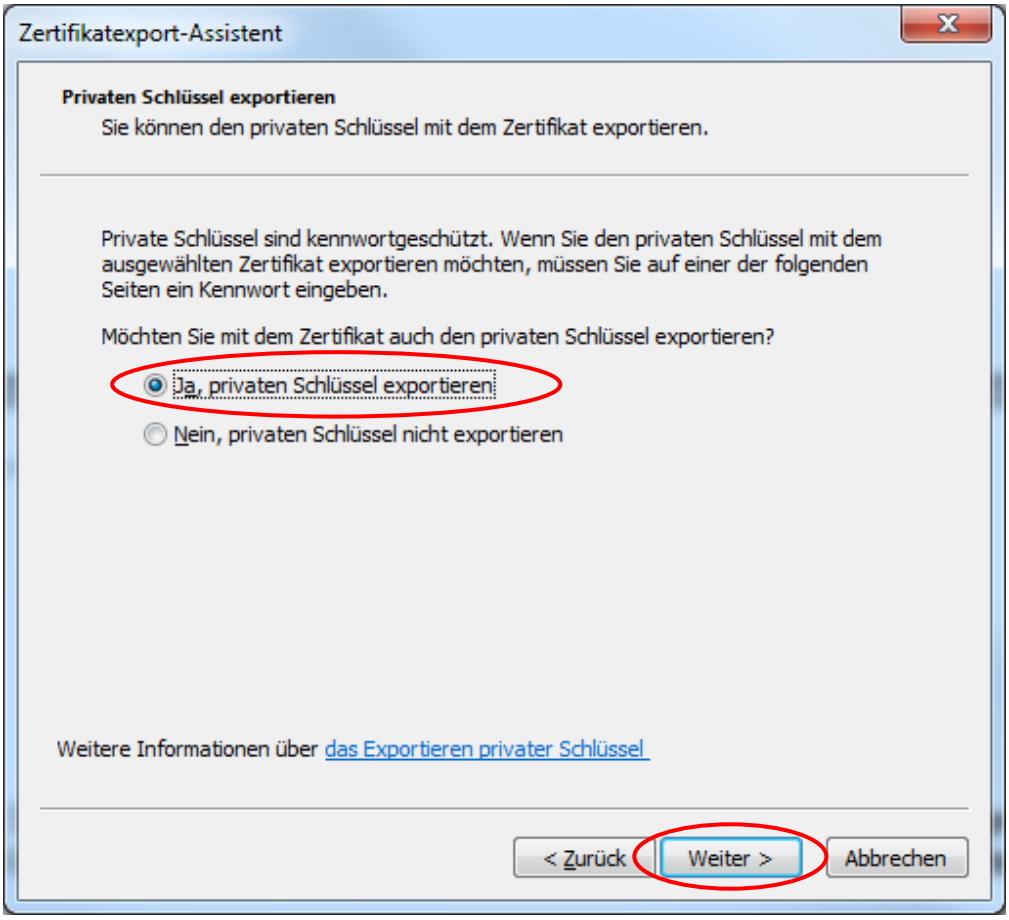


Abbildung 19: Microsoft Zertifikatexport-Assistent – Auswahl der Option des Exports des privaten Schlüssels

Im nun folgenden Dialog müssen Sie keine Änderungen vornehmen und können direkt mit der Schaltfläche **Weiter** bestätigen (vgl. Abbildung 20).

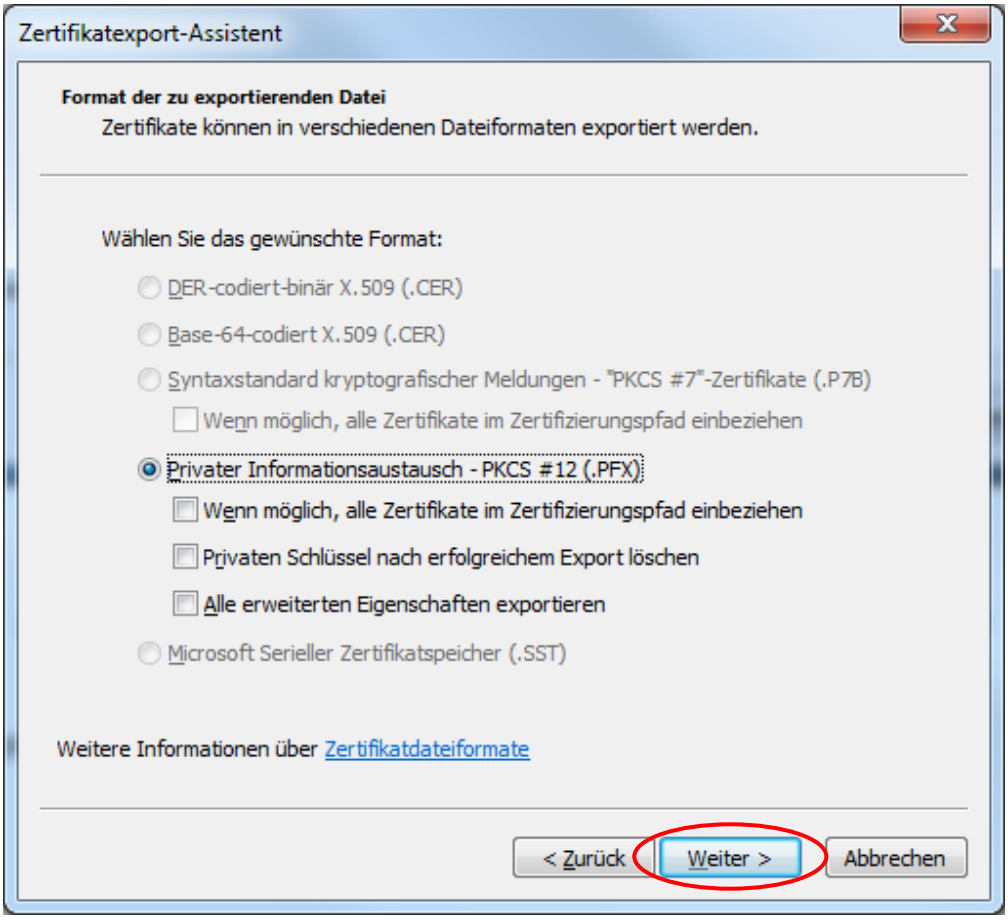


Abbildung 20: Microsoft Zertifikatexport-Assistent – Auswahl des Dateiexportformats

Geben Sie nun ein sicheres Kennwort[1] ein, das den privaten Schlüssel beim Export schützen soll (vgl. Abbildung 21). Das Kennwort wird immer dann benötigt, wenn Sie Ihr Zertifikat in ein Programm importieren möchten und dient als Sicherung vor unberechtigten Zugriffen. Bestätigen Sie diesen Dialog mit **Weiter**.

[1] Das Kennwort sollte mindestens eine Länge von zwölf Zeichen haben und neben Buchstaben in Klein- und Großschreibung, auch Ziffern und Sonderzeichen beinhalten.

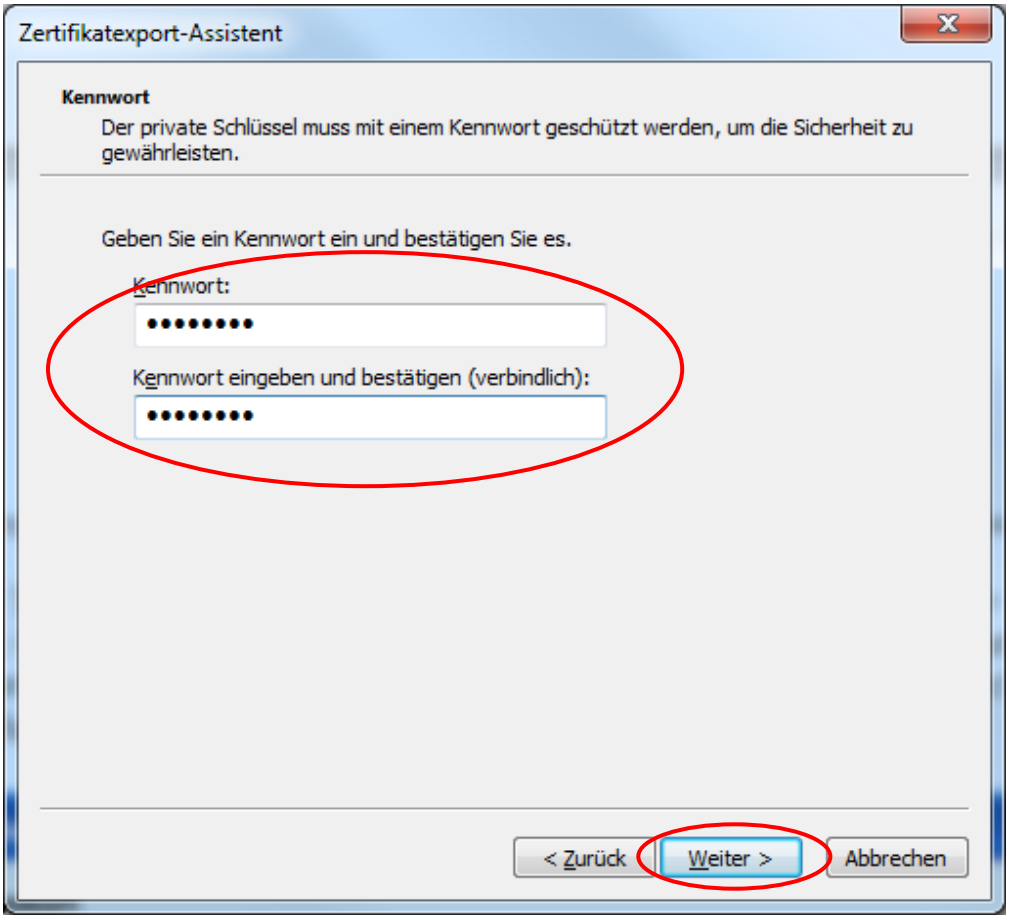


Abbildung 21: Microsoft Zertifikatexport-Assistent – Eingabe des Transport-Passworts für das Zertifikat-Backup

Klicken Sie nun auf **Durchsuchen** und wählen Sie einen Speicherort für das Zertifikat aus. Geben Sie einen „sprechenden" Namen für die Zertifikat- und Schlüsseldatei an, klicken Sie auf **Speichern** und bestätigen Sie den verbleibenden Dialog mit **Weiter** (vgl. Abbildung 22).

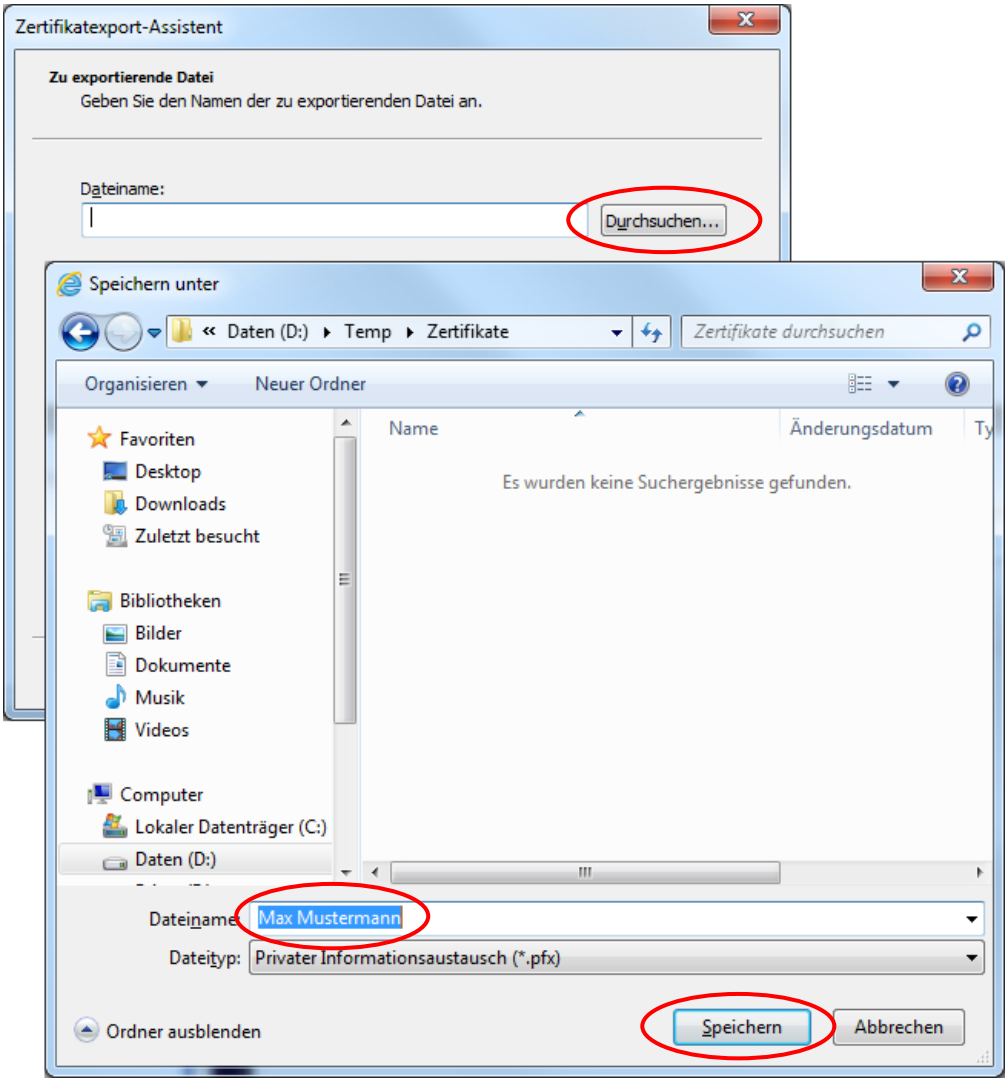


Abbildung 22: Microsoft Zertifikatexport-Assistent – Auswahl des Speicherorts für das Zertifikat-Backup

Der Zertifikatexport-Assistent zeigt Ihnen nun nochmals eine Zusammenfassung Ihrer Einstellungen an. Klicken Sie jetzt auf **Fertigstellen**, um den Exportvorgang tatsächlich durchzuführen und abzuschließen (vgl. Abbildung 23).

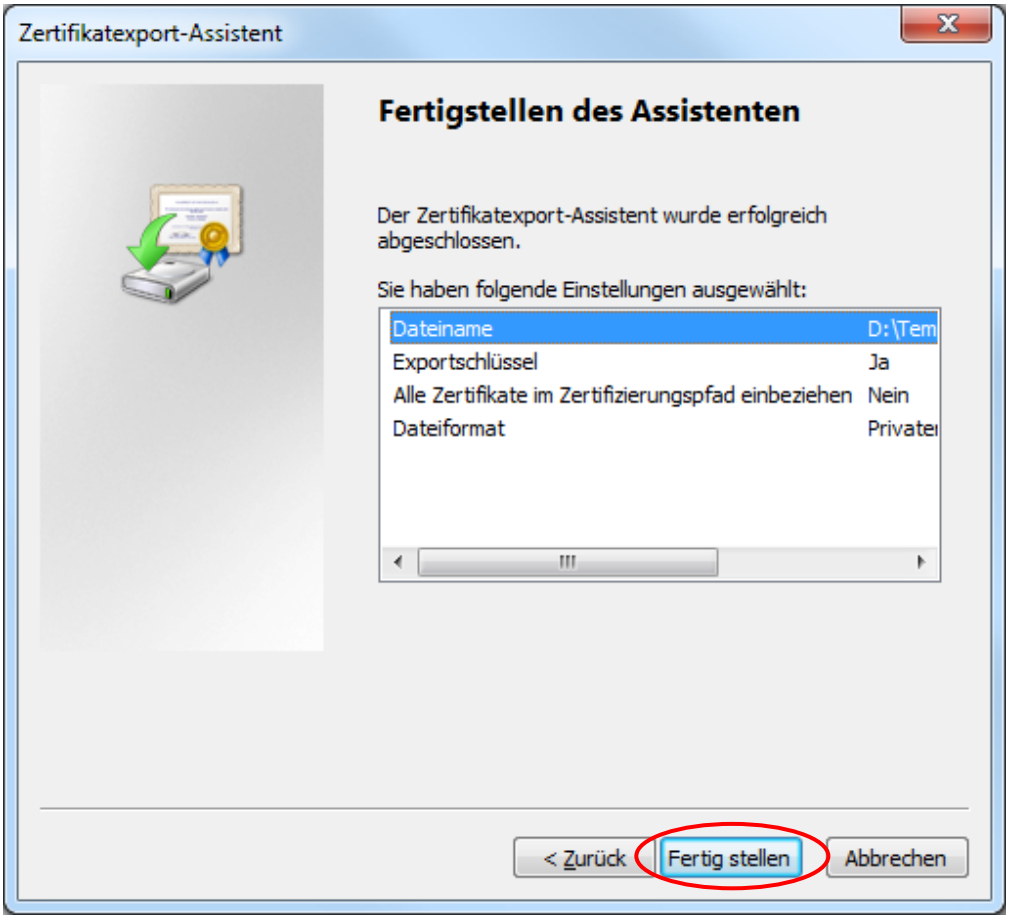


Abbildung 23: Microsoft Zertifikatexport-Assistent – Beenden des Assistenten

Es erfolgt eine Meldung, dass der Exportvorgang erfolgreich war. Diese kann mit **OK** bestätigt werden (vgl. Abbildung 24).

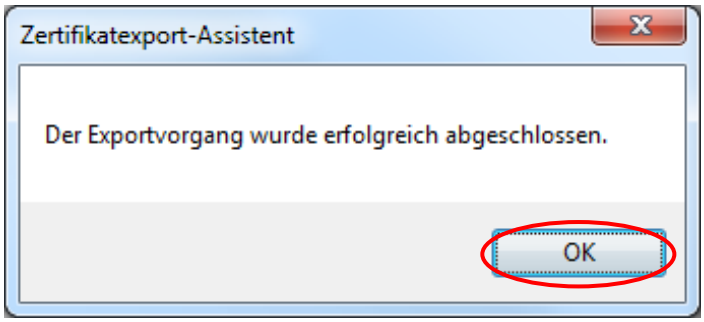


Abbildung 24: Microsoft Zertifikatexport-Assistent – Hinweis zum erfolgreichen Export des Zertifikats und privaten Schlüssels

3.2 Ein eigenes Zertifikat aus Mozilla Firefox exportieren

Hinweis: Unabhängig davon welches E-Mail-Programm Sie in Kombination mit Mozilla Firefox verwenden, ist für die Nutzung des sicheren E-Mail-Verkehr in jedem Fall ein Export des persönlichen Zertifikats bzw. Schlüssels aus dem Browser (und ein Import im jeweiligen E-Mail-Programm) notwendig. Der Zertifikatspeicher von Mozilla Firefox kann nur über den Browser selbst genutzt werden. Darüber hinaus ist ein Export auch sinnvoll, um eine Sicherungskopie des Zertifikats (und privaten Schlüssels) anzufertigen.

Öffnen Sie zunächst den Zertifikatspeicher von Mozilla Firefox, der sich unter **Extras → Einstellungen → Erweitert → Verschlüsselung → Zertifikate anzeigen** befindet (vgl. Abbildung 25).

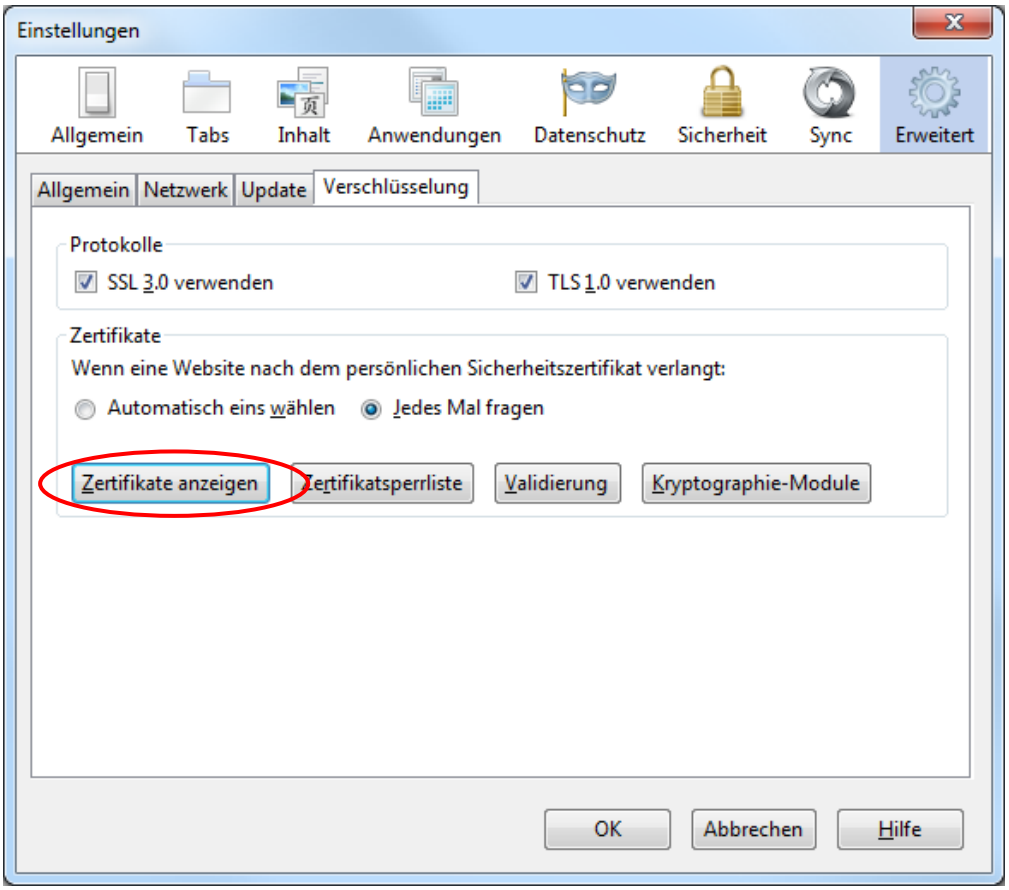


Abbildung 25: Öffnen des Zertifikatspeichers von Mozilla Firefox

Markieren Sie anschließend im Reiter **Ihre Zertifikate** das zu exportierende Zertifikat und klicken Sie auf die Schaltfläche **Sichern** (vgl. Abbildung 26).

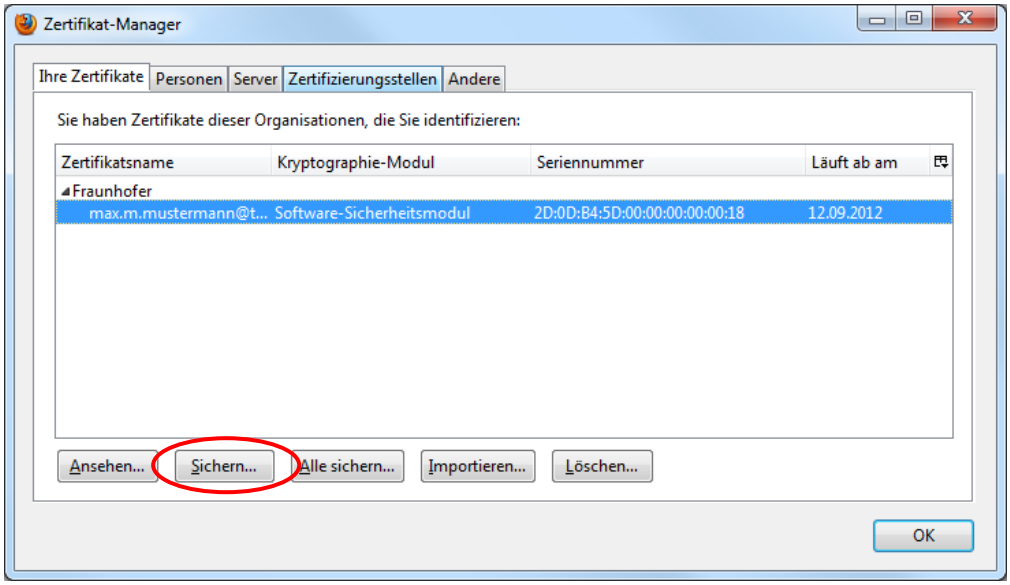


Abbildung 26: Auswahl des zu exportierenden Zertifikats im Zertifikatspeicher von Mozilla Firefox

Wählen Sie nun einen Speicherort für Ihr Zertifikat und geben Sie einen „sprechenden" Namen für die Zertifikat- und Schlüsseldatei an und klicken Sie anschließend auf **Speichern** (vgl. Abbildung 27).

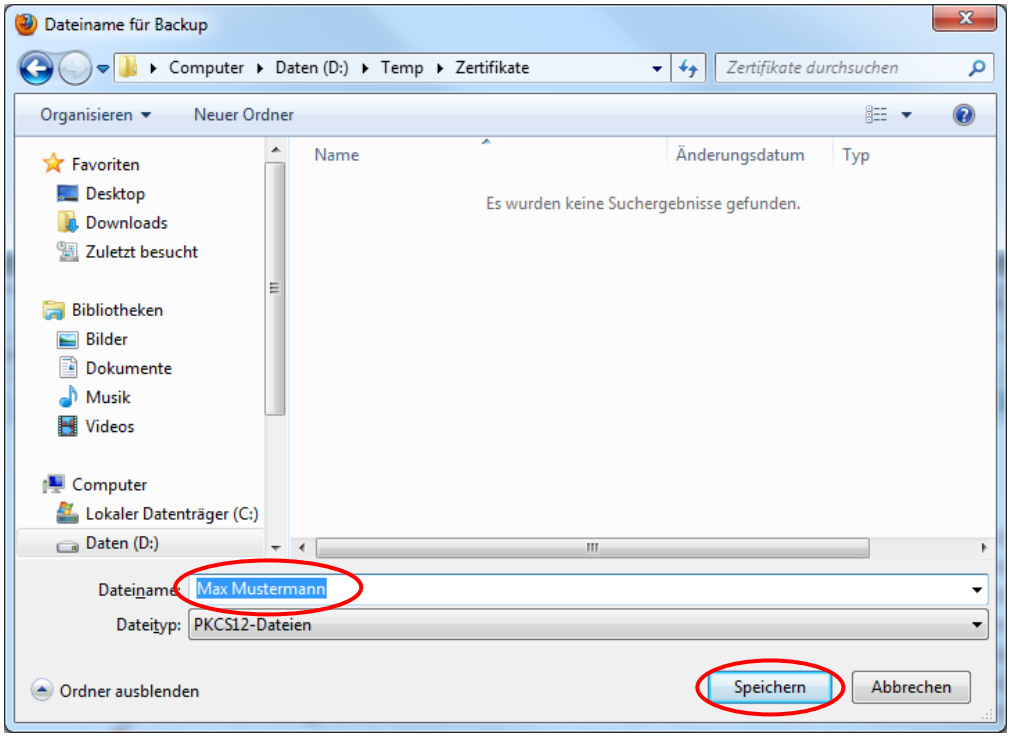


Abbildung 27: Auswahl des Speicherorts für das Zertifikat-Backup in Mozilla Firefox

Hinweis: Falls Sie in Ihrem Browser die Verwendung des Master-Kennworts aktiviert haben, werden Sie nun aufgefordert, dieses Passwort für den Zugriff auf Ihr Software-Sicherheitsmodul anzugeben. Das Passwort wird benötigt, da Ihr persönliches Zertifikat einschließlich des zugehörigen privaten Schlüssels aus dem Zertifikatsspeicher des Browsers exportiert wird.

Geben Sie nun ein sicheres Kennwort[2] ein, das den privaten Schlüssel beim Export schützen soll (vgl. Abbildung 28). Das Kennwort wird immer dann benötigt, wenn Sie Ihr Zertifikat in ein Programm importieren möchten und dient als Sicherung vor unberechtigten Zugriffen. Bestätigen Sie diesen Dialog mit **OK**.

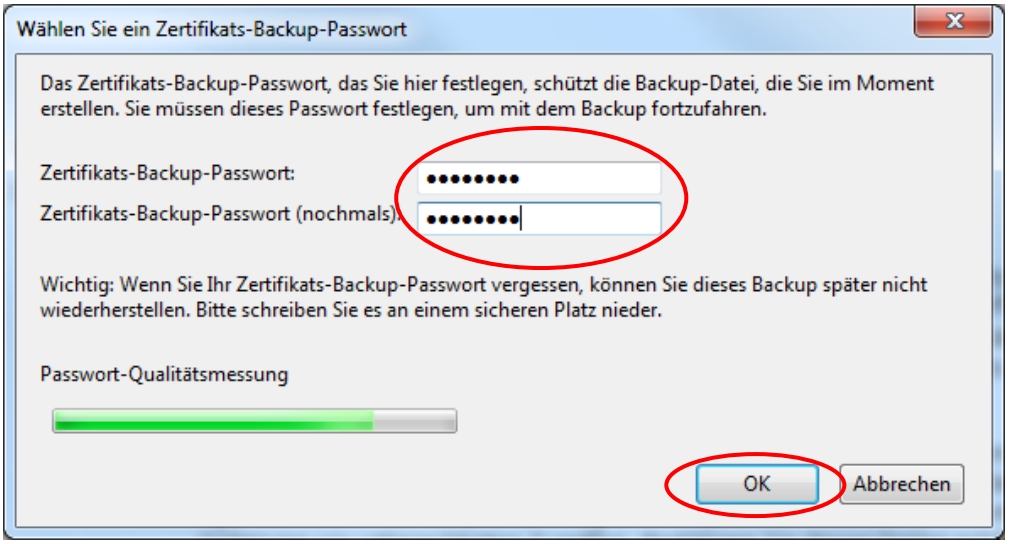


Abbildung 28: Eingabe des Transport-Passworts für das Zertifikat-Backup (Mozilla Firefox)

Es erfolgt eine Meldung, dass der Sicherungsvorgang erfolgreich war. Diese kann mit **OK** bestätigt werden (vgl. Abbildung 29).

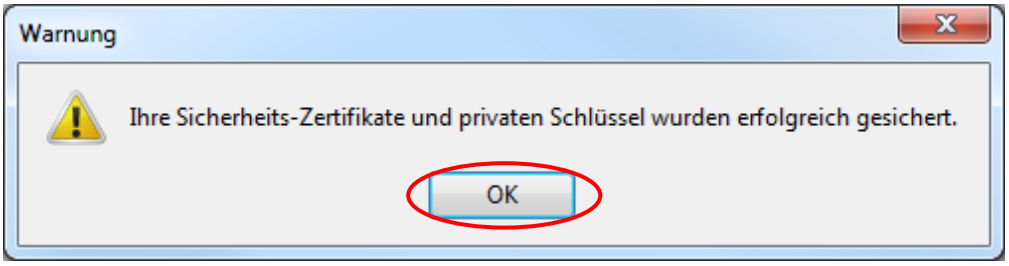


Abbildung 29: Hinweis zur erfolgreichen Sicherung des Zertifikats und privaten Schlüssels (Mozilla Firefox)

[2] Das Kennwort sollte mindestens eine Länge von zwölf Zeichen haben und neben Buchstaben in Klein- und Großschreibung, auch Ziffern und Sonderzeichen beinhalten.

4 Zertifikate im E-Mail-Client nutzen

In diesem Kapitel wird beschrieben, wie Sie Ihr eigenes Zertifikat zur sicheren E-Mail-Kommunikation mit einem Fraunhofer-Mitarbeiter nutzen können. Hierzu ist es zunächst erforderlich, das Wurzelzertifikat der PKI für Fraunhofer Kontakte sowie Ihr eigenes Zertifikat in Ihren E-Mail-Client zu integrieren.

Darüber hinaus ist es für eine verschlüsselte Kommunikation mit einem Fraunhofer-Mitarbeiter erforderlich, auch dessen Verschlüsselungszertifikat in Ihren E-Mail-Client aufzunehmen. Zusätzlich kann es weiterhin in Ausnahmefällen auch notwendig sein, die Wurzelzertifikate bzw. die Zertifikatsketten der PKI für Fraunhofer Mitarbeiter in den E-Mail-Client zu integrieren. Auch das hierzu erforderliche Vorgehen ist in diesem Kapitel beschrieben.

4.1 Den E-Mail-Client für die Zertifikatsnutzung vorbereiten

In Abhängigkeit von dem von Ihnen verwendeten E-Mail-Client ist die Vorbereitung des E-Mail-Clients unterschiedlich, so dass das entsprechende Vorgehen in diesem Abschnitt zum einen für Anwendungen beschrieben wird, die auf den Microsoft-Zertifikatspeicher zugreifen (beispielsweise Microsoft Outlook) als auch für solche, die einen eigenen Zertifikatspeicher verwenden (beispielsweise Mozilla Thunderbird).

4.1.1 Integration des Wurzelzertifikats der PKI für Fraunhofer Kontakte

Laden Sie zunächst das Wurzelzertifikat über die Seite https://contacts.pki.fraunhofer.de herunter. Klicken Sie dazu im Menü im Bereich **Allgemein** auf den Menüeintrag **Wurzel-Zertifikat / Sperrliste laden (PKI für Fraunhofer Kontakte)** und in der erscheinenden Seite dann mit der rechten Maustaste auf den Verweis **Wurzel-Zertifikat herunterladen Zertifizierungsstelle für Fraunhofer Kontakte** und wählen Sie im Kontextmenü **Ziel Speichern unter** (vgl. Abbildung 30).

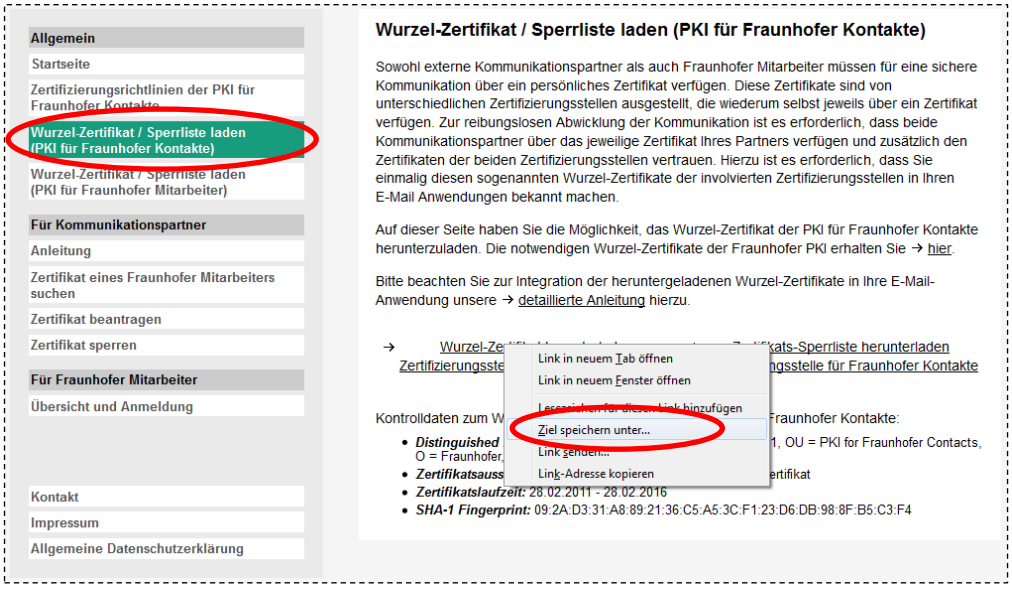


Abbildung 30: Herunterladen des Wurzelzertifikats der PKI für Fraunhofer Kontakte

Wechseln Sie nun zu dem Ordner, in dem das Zertifikat gespeichert werden soll und klicken Sie auf **Speichern** (vgl. Abbildung 31).

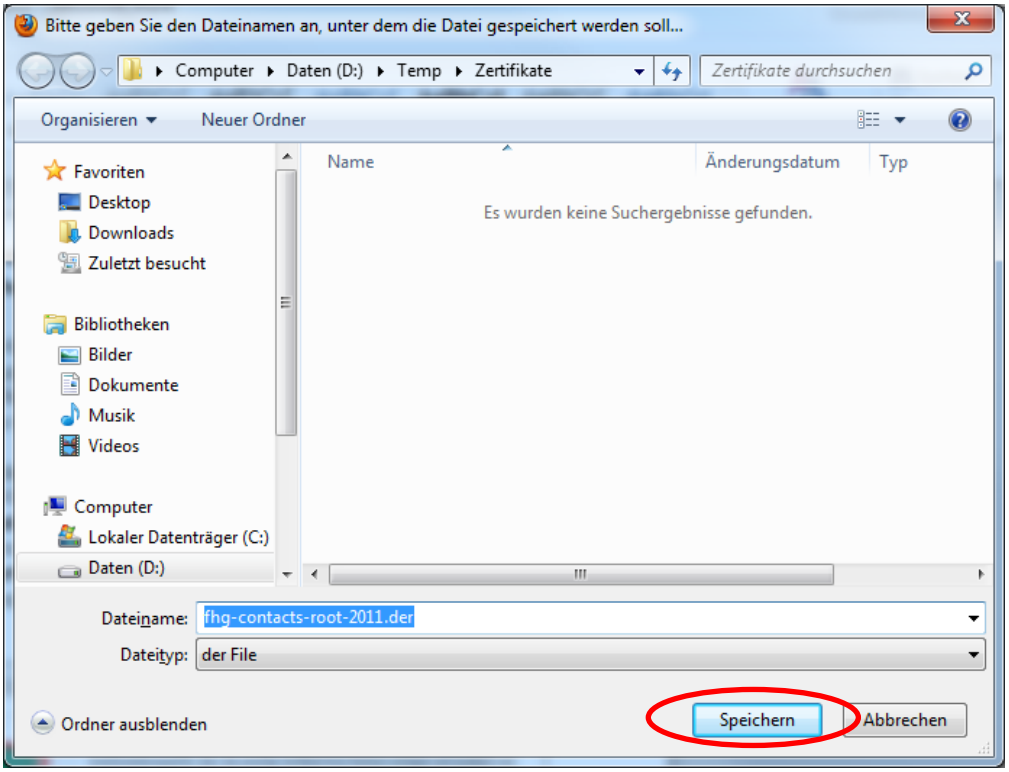


Abbildung 31: Speichern des Wurzelzertifikats der PKI für Fraunhofer Kontakte

4.1.1.1 Wurzelzertifikat der PKI für Fraunhofer Kontakte in den Microsoft-Zertifikatspeicher aufnehmen

Falls Sie Microsoft Outlook zur E-Mail-Kommunikation verwenden, muss das Wurzelzertifikat der PKI für Fraunhofer Kontakte in den Microsoft-Zertifikatspeicher importiert werden, auf den auch Microsoft Outlook zurückgreift.

Öffnen Sie hierzu den Zertifikatspeicher von Microsoft über **Start → Systemsteuerung → Netzwerk und Internet → Internetoptionen → Inhalte → Zertifikate** und aktivieren Sie den Reiter **Vertrauenswürdige Stammzertifizierungsstellen**. Klicken Sie auf die Schaltfläche **Importieren** (vgl. Abbildung 32).

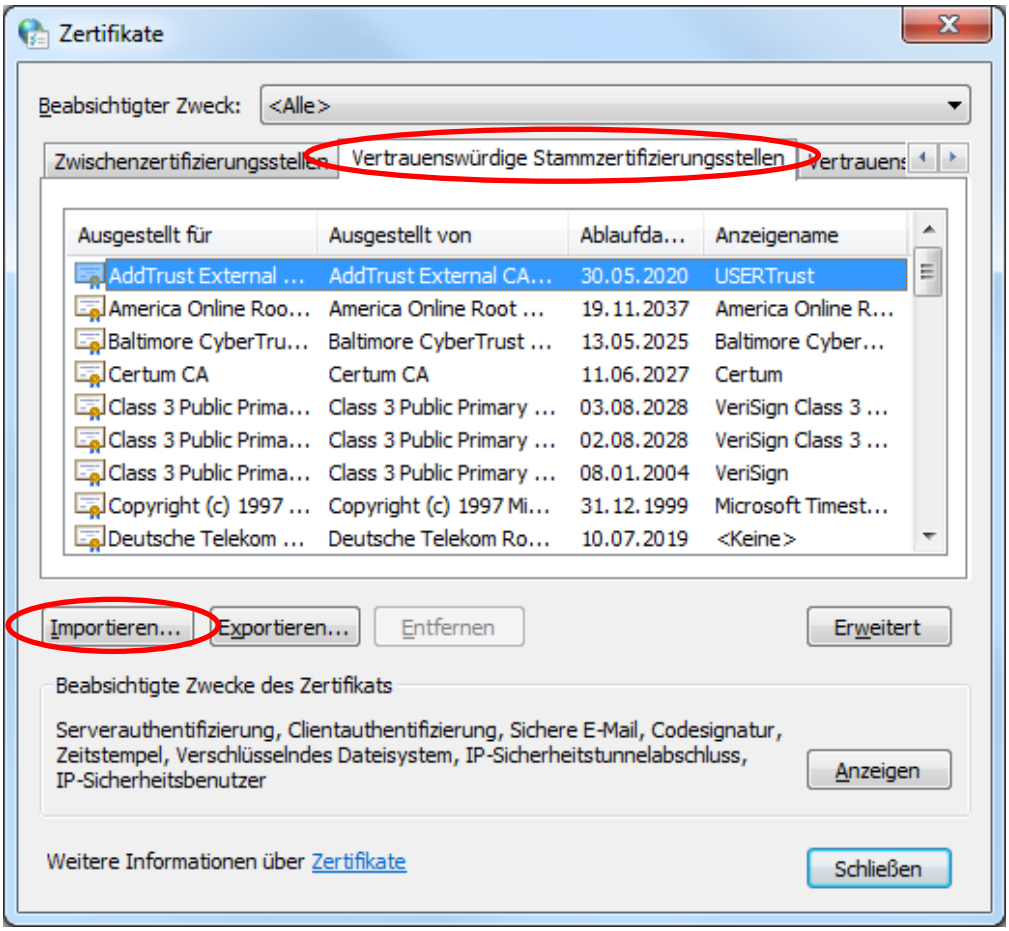


Abbildung 32: Ansicht des Microsoft-Zertifikatspeichers *Vertrauenswürdige Stammzertifizierungsstellen*

Es öffnet sich nun der Zertifikatimport-Assistent. Bestätigen Sie das erste Fenster mit **Weiter**. Klicken Sie nun auf die Schaltfläche **Durchsuchen** und wählen Sie das zuvor heruntergeladene Wurzelzertifikat aus. Bestätigen Sie den Dialog mit **Öffnen** und klicken Sie anschließend auf **Weiter** (vgl. Abbildung 33).

Hinweis: Falls Ihnen das Wurzelzertifikat der PKI für Fraunhofer Kontakte nicht im Öffnen-Dialog angezeigt wird, ist es erforderlich, den Filter der anzeigten Dateien von „X.509-Zertifikat (*.cer,*.crt)“ auf die Anzeige aller Dateien („Alle Dateien (*.*)“ umzustellen.

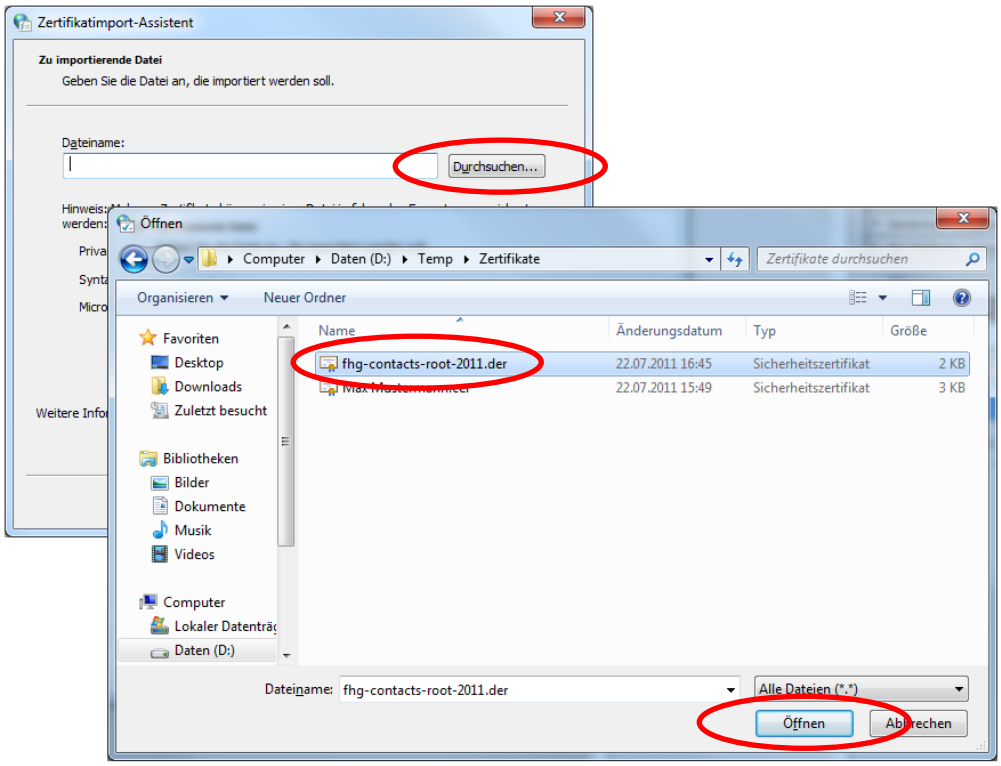


Abbildung 33: Auswahl des Wurzelzertifikats der PKI für Fraunhofer-Kontakte beim Import in den Microsoft-Zertifikatspeicher

In den folgenden Dialogen können Sie die Standardeinstellungen übernehmen und mit **Weiter** bestätigen. Beenden Sie den Zertifikatimport-Assistenten mit **Fertigstellen**. Zum Abschluss der Installation erhalten Sie eine Sicherheitswarnung (vgl. Abbildung 34), die Sie nach positiver Prüfung des Fingerabdrucks bitte mit **Ja** bestätigen. Vergleichen Sie hierzu bitte den in der Sicherheitswarnung angezeigten Fingerabdruck genau mit dem auf der Webseite angegebenen Fingerabdruck des Wurzelzertifikats und bestätigen Sie nur dann mit **Ja**, falls die Ziffern bzw. Buchstaben beider Werte zeichenweise identisch sind.

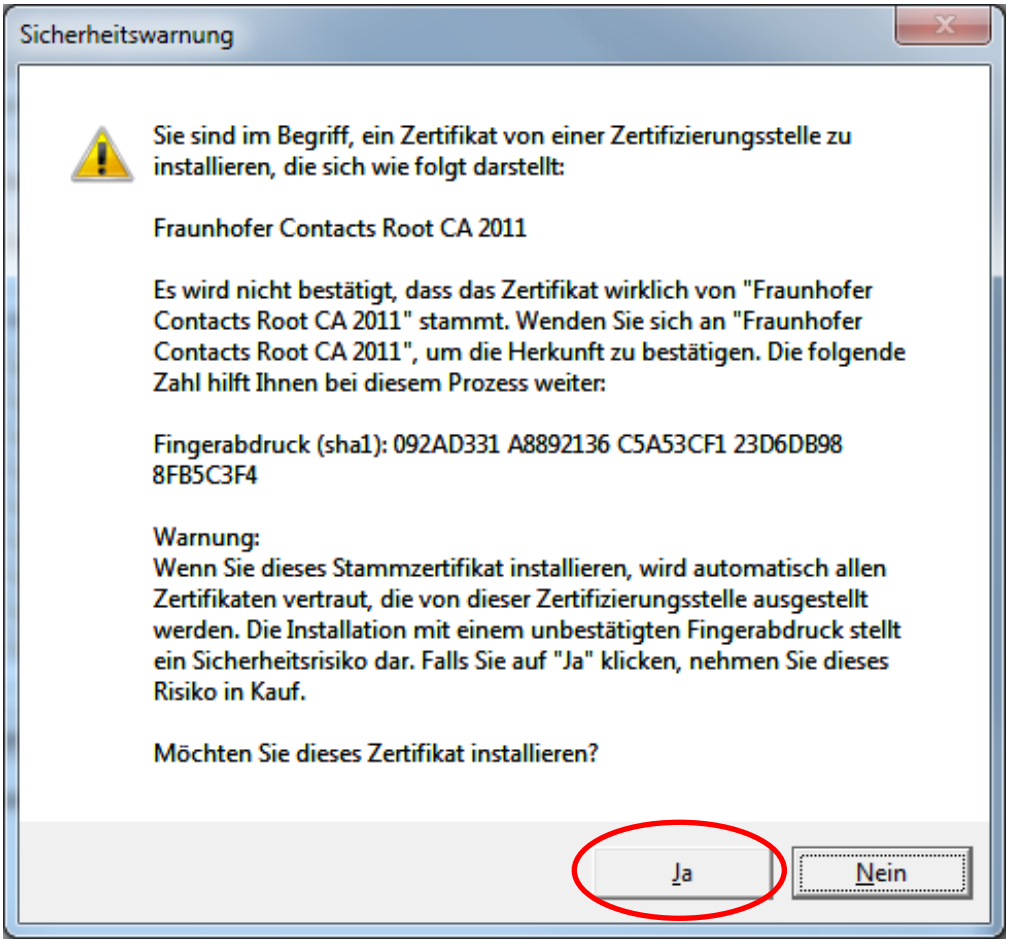


Abbildung 34: Sicherheitswarnung beim Import des Wurzelzertifikats der PKI für Fraunhofer Kontakte in den Microsoft-Zertifikatspeicher

Der erfolgreiche Abschluss des Imports wird nun mit einem Hinweis bestätigt. Schließen Sie das Fenster über die Schaltfläche **OK** (vgl. Abbildung 35).

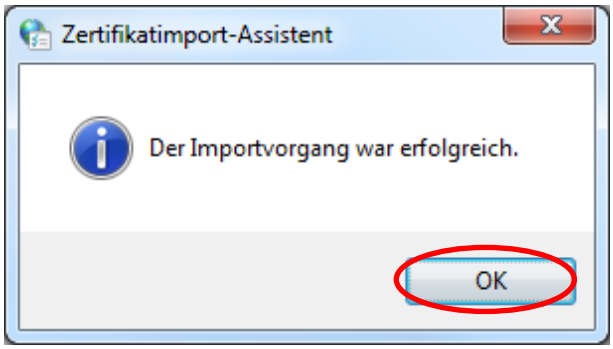


Abbildung 35: Erfolgreicher Abschluss des Imports des Wurzelzertifikats der PKI für Fraunhofer Kontakte in den Microsoft-Zertifikatspeicher

4.1.1.2 Wurzelzertifikat der PKI für Fraunhofer Kontakte in den Zertifikatspeicher von Mozilla Thunderbird aufnehmen

Hinweis: Die Screenshots wurden unter Verwendung von Mozilla Thunderbird in der Version 7 angefertigt.

Wenn Sie Mozilla Thunderbird zur E-Mail-Kommunikation verwenden, muss das Wurzelzertifikat der PKI für Fraunhofer Kontakte in den Zertifikatspeicher von Thunderbird importiert werden.

Hinweis: Mozilla Firefox und Mozilla Thunderbird verwenden jeweils eigene Zertifikatspeicher.

Um das Wurzelzertifikat in den Zertifikatspeicher von Thunderbird zu importieren, öffnen Sie dessen Zertifikatspeicher über **Extras → Einstellungen → Erweitert → Zertifikate → Zertifikate** und aktivieren Sie den Reiter **Zertifizierungsstellen**. Klicken Sie auf die Schaltfläche **Importieren** (vgl. Abbildung 36).

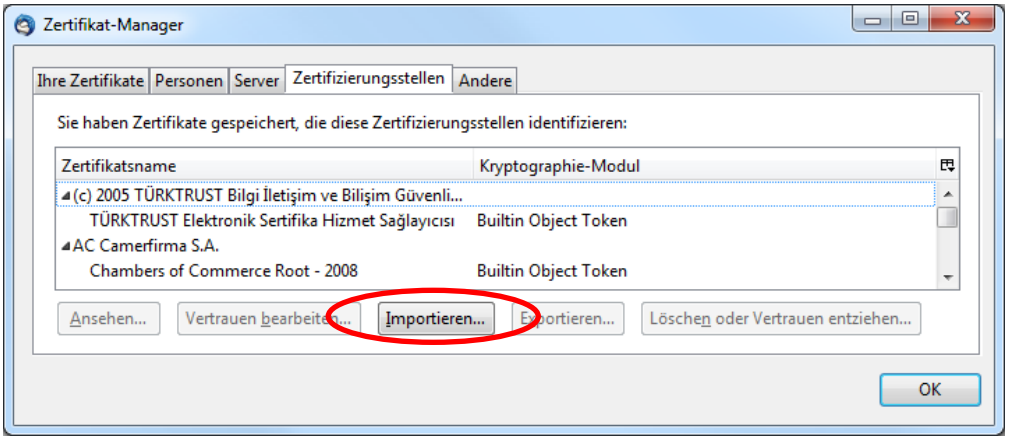


Abbildung 36: Ansicht des Thunderbird-Zertifikatspeichers *Zertifizierungsstellen*

Es öffnet sich nun ein Dateiauswahldialog. Navigieren Sie nun zum Ablageort an dem Sie das Wurzelzertifikat der PKI für Fraunhofer Kontakte abgelegt haben und wählen Sie das zuvor heruntergeladene Wurzelzertifikat aus. Schließen Sie den Dialog mit **Öffnen** (vgl. Abbildung 37).

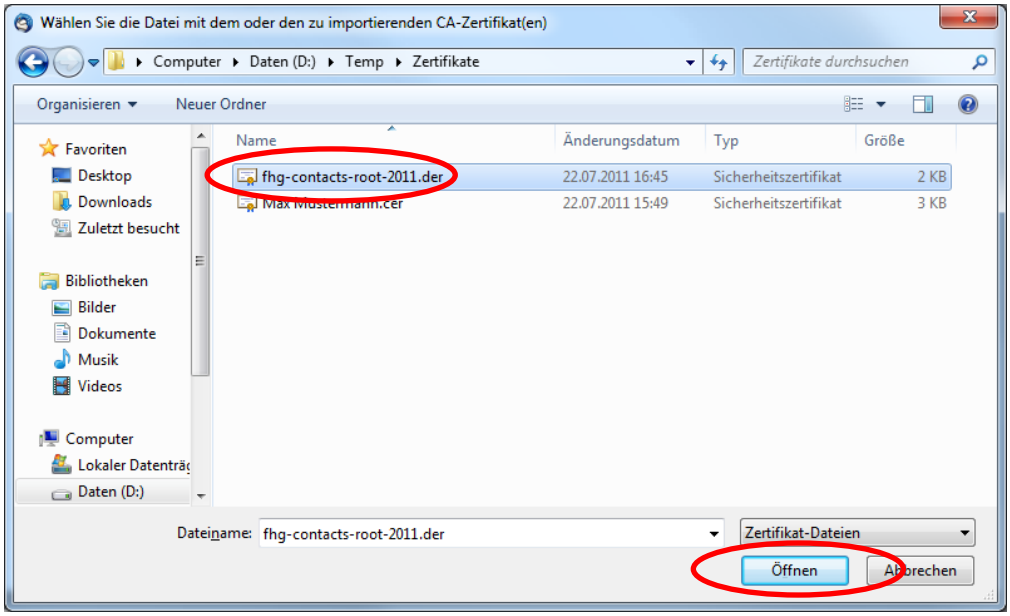


Abbildung 37: Auswahl des Wurzelzertifikats der PKI für Fraunhofer-Kontakte beim Import in den Thunderbird-Zertifikatspeicher

Bestätigen Sie nun, dass Sie dem Zertifikat mindestens für die Verwendungsart *Dieser CA vertrauen, um E-Mail-Nutzer zu identifizieren* vertrauen und schließen Sie den Dialog mit **OK**, nachdem Sie sich vergewissert haben, dass der SHA1-Fingerabdruck des Zertifikats genau mit dem auf der Web-Seite angegebenen Fingerabdruck des Wurzelzertifikats übereinstimmt (vgl. Abbildung 38). Zur Anzeige des Fingerabdrucks des zu importierenden Zertifikats wählen Sie bitte die Schaltfläche **Ansicht**. Der SHA1-Fingerabdruck ist auf dem Reiter **Allgemein** im unteren Bereich angegeben und die Ziffern bzw. Buchstaben müssen zeichenweise mit dem auf der Web-Seite angegebenen Wert übereinstimmen.

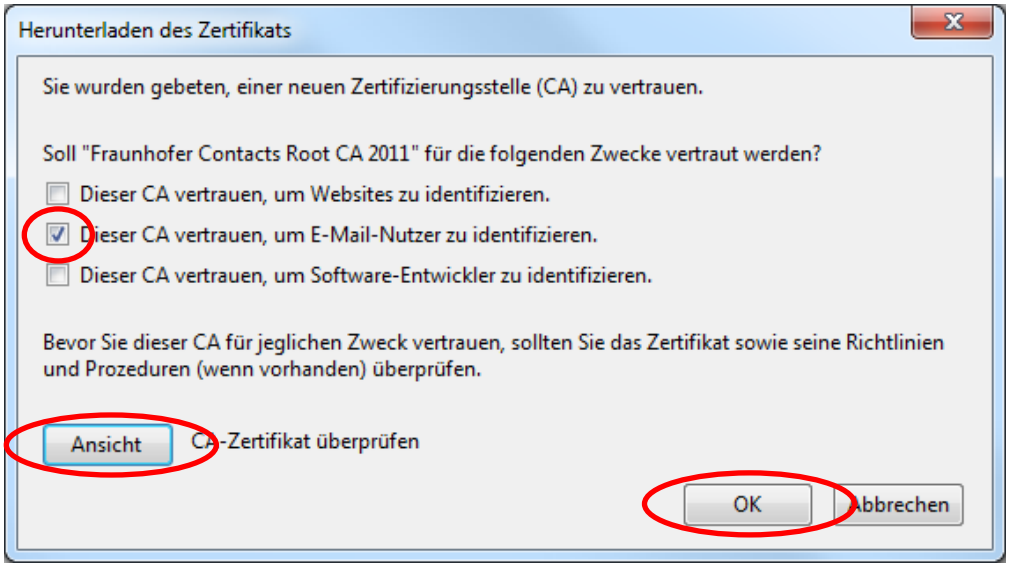


Abbildung 38: Vertrauensstellung des Wurzelzertifikats der PKI für Fraunhofer Kontakte beim Import in Mozilla-Thunderbird festlegen

Das Wurzelzertifikat der PKI für Fraunhofer-Kontakte ist jetzt im Zertifikatspeicher vorhanden und kann damit nun von Mozilla Thunderbird zur Verifikation der Benutzerzertifikate der PKI für Fraunhofer Kontakte verwendet werden.

4.1.2 Integration der Wurzelzertifikate / Zertifikatsketten der PKI für Fraunhofer Mitarbeiter

Um auch die Zertifikate von Fraunhofer Mitarbeitern korrekt überprüfen und verwenden zu können, ist es erforderlich, dass Sie auch denjenigen Zertifizierungsstellen vertrauen, die die Mitarbeiterzertifikate herausgegeben haben. Zertifikate für Fraunhofer Mitarbeiter werden derzeit aus zwei verschiedenen Public Key Infrastrukturen herausgegeben. Im Gegensatz zur PKI für Fraunhofer Kontakte handelt es sich bei den PKIs der Fraunhofer-Gesellschaft für ihre Mitarbeiter um jeweils zwei mehrstufige Hierarchien, an deren Spitze als Wurzelzertifikate das *Deutsche Telekom Root CA 2* Zertifikat bzw. das *T-TeleSec GlobalRoot Class 2* Zertifikat stehen.

Hinweis: In den allermeisten Fällen sind das *Deutsche Telekom Root CA 2* sowie das *T-TeleSec GlobalRoot Class 2* Zertifikat bereits standardmäßig im Lieferumfang der Betriebssysteme bzw. der Browser und E-Mail-Applikationen enthalten. Ein gesonderter Import ist also in der Regel nicht erforderlich. Führen Sie ihn nur dann durch, falls Sie Probleme bei der Verifikation bzw. Verwendung von Zertifikaten von Fraunhofer Mitarbeitern feststellen. Ein Einzelfällen kann es darüber hinaus auch notwendig sein, zusätzlich zu den beiden genannten Wurzelzertifikaten die übrigen Zertifikate der Zertifikatsketten der Fraunhofer PKI zu

importieren, namentlich das *DFN-Verein PCA Global - G01*, das *DFN-Verein Certification Authority 2*, das *Fraunhofer User CA – G01* sowie das *Fraunhofer User CA G02* Zertifikat.

Die Wurzelzertifikate der PKI für Fraunhofer Mitarbeiter sowie die übrigen Zertifikate der zugehörigen Zertifikatsketten können Sie über die Seite https://contacts.pki.fraunhofer.de herunterladen. Klicken Sie dazu im Menü im Bereich **Allgemein** auf den Menüeintrag **Wurzel-Zertifikat / Sperrliste laden (PKI für Fraunhofer Mitarbeiter)** und in der erscheinenden Seite dann mit der rechten Maustaste jeweils auf den Verweis **Zertifikat herunterladen**, der unterhalb des *Deutschen Telekom Root CA 2* bzw. des *T-TeleSec GlobalRoot Class 2* Zertifikats angegeben ist und wählen Sie im Kontextmenü **Ziel Speichern unter** (vgl. Abbildung 39).

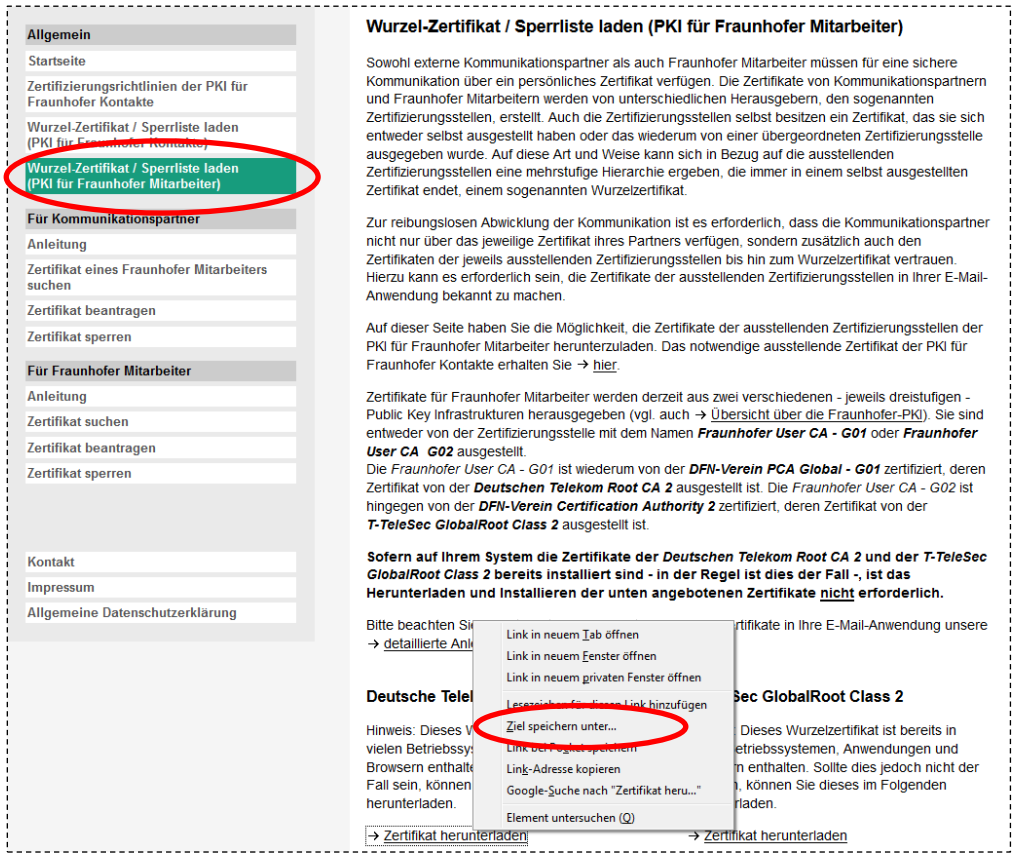


Abbildung 39: Herunterladen des *Deutschen Telekom Root CA 2* Wurzelzertifikats der PKI für Fraunhofer Mitarbeiter

Wechseln Sie nun zu dem Ordner, in dem das Zertifikat gespeichert werden soll und klicken Sie auf **Speichern** (vgl. Abbildung 40).

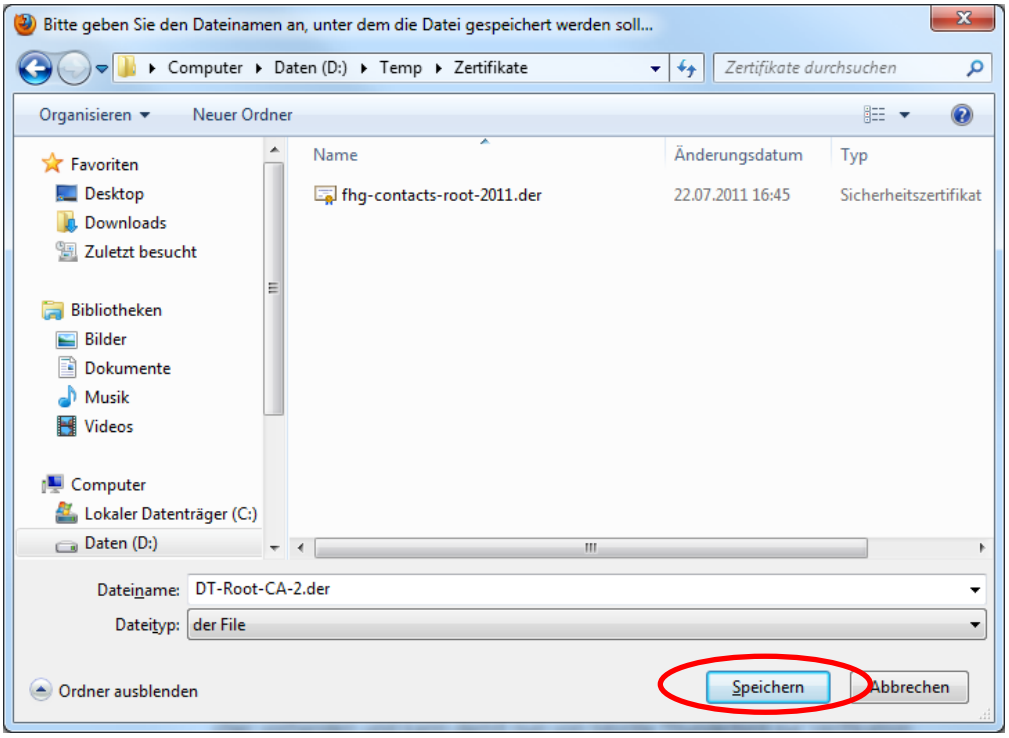


Abbildung 40: Speichern des Wurzelzertifikats der PKI für Fraunhofer Mitarbeiter

Hinweis: Das Herunterladen der Zertifikate der Zwischenzertifizierungsstellen der PKI für Fraunhofer Mitarbeiter (*DFN-Verein PCA Global - G01*, *DFN-Verein Certification Authority 2*, *Fraunhofer User CA – G01* sowie *Fraunhofer User CA G02* Zertifikat) erfolgt vollkommen analog.

4.1.2.1 Wurzelzertifikate / Zertifikatsketten der PKI für Fraunhofer Mitarbeiter in den Microsoft-Zertifikatspeicher aufnehmen

Das Vorgehen zur Integration der Wurzelzertifikate der PKI für Fraunhofer Mitarbeiter (*Deutsche Telekom Root CA 2* und *T-TeleSec GlobalRoot Class 2* Zertifikat) in den Microsoft-Zertifikatspeicher erfolgt vollkommen analog zum im Abschnitt 4.1.1.1 beschriebenen Verfahren.

Sofern auch der Import der Zertifikate der Zwischenzertifizierungsstellen der PKI für Fraunhofer Mitarbeiter vorgenommen wird, sind diese Zertifikate – namentlich das *DFN-Verein PCA Global - G01*, das *DFN-Verein Certification Authority 2*, das *Fraunhofer User CA – G01* sowie das *Fraunhofer User CA G02* Zertifikat – statt in den Zertifikatspeicher *Vertrauenswürdige Stammzertifizierungsstellen* in den Zertifikatspeicher *Zwischenzertifizierungsstellen* zu importieren. Ansonsten verläuft auch die Integration dieser Zertifikate entsprechend dem in Abschnitt 4.1.1.1 beschriebenen Verfahren.

4.1.2.2 Wurzelzertifikate / Zertifikatsketten der PKI für Fraunhofer Mitarbeiter in den Zertifikatspeicher von Mozilla Thunderbird aufnehmen

Das Vorgehen zur Integration der Wurzelzertifikate der PKI für Fraunhofer Mitarbeiter (*Deutsche Telekom Root CA 2* und *T-TeleSec GlobalRoot Class 2* Zertifikat) bzw. der Zertifikate der Zwischenzertifizierungsstellen der PKI für Fraunhofer Mitarbeiter – namentlich des *DFN-Verein PCA Global - G01*, des *DFN-Verein Certification Authority 2*, des *Fraunhofer User CA – G01* sowie des *Fraunhofer User CA G02* Zertifikats – in den Zertifikatspeicher von Mozilla Thunderbird erfolgt vollkommen analog zum im Abschnitt 4.1.1.2 beschriebenen Verfahren.

4.2 Ein eigenes Zertifikat in den E-Mail-Client aufnehmen

In diesem Abschnitt wird beschrieben, wie Sie Ihr eigenes Zertifikat in Ihren E-Mail-Client aufnehmen und konfigurieren können, so dass Sie signierte E-Mails versenden können. In Abhängigkeit von dem von Ihnen verwendeten E-Mail-Client verläuft die Aufnahme und Konfiguration des eigenen Zertifikats in Ihrem E-Mail-Client unterschiedlich, so dass das entsprechende Vorgehen zum einen für Anwendungen beschrieben wird, die auf den Microsoft-Zertifikatspeicher zugreifen (beispielsweise Microsoft Outlook) als auch für solche, die einen eigenen Zertifikatspeicher verwenden (beispielsweise Mozilla Thunderbird).

4.2.1 Ein eigenes Zertifikat in den Microsoft-Zertifikatspeicher aufnehmen

Falls Sie Microsoft Outlook zur E-Mail-Kommunikation verwenden, muss das eigene Zertifikat in den Microsoft-Zertifikatspeicher importiert werden, auf den auch die verschiedenen Versionen von Microsoft Outlook zurückgreifen.

Hinweis: Sofern Sie den Internet Explorer auf Ihrem System genutzt haben, um das eigene Zertifikat zu beantragen, ist eine Aufnahme des eigenen Zertifikats in den Microsoft Zertifikatspeicher nicht mehr erforderlich. Es ist im Rahmen des Beantragungsprozesses (vgl. Abschnitt 2.1) bereits diesem hinzugefügt worden. Es ist in diesem Fall nur noch erforderlich, das Zertifikat beispielsweise in Microsoft Outlook zu konfigurieren. Das hierzu notwendige Vorgehen ist in den Abschnitten 4.2.1.1ff. beschrieben.

Öffnen Sie hierzu den Zertifikatspeicher von Microsoft über **Start → Systemsteuerung → Netzwerk und Internet → Internetoptionen → Inhalte → Zertifikate** und aktivieren Sie den Reiter **Eigene Zertifikate**. Klicken Sie auf die Schaltfläche **Importieren** (vgl. Abbildung 41).

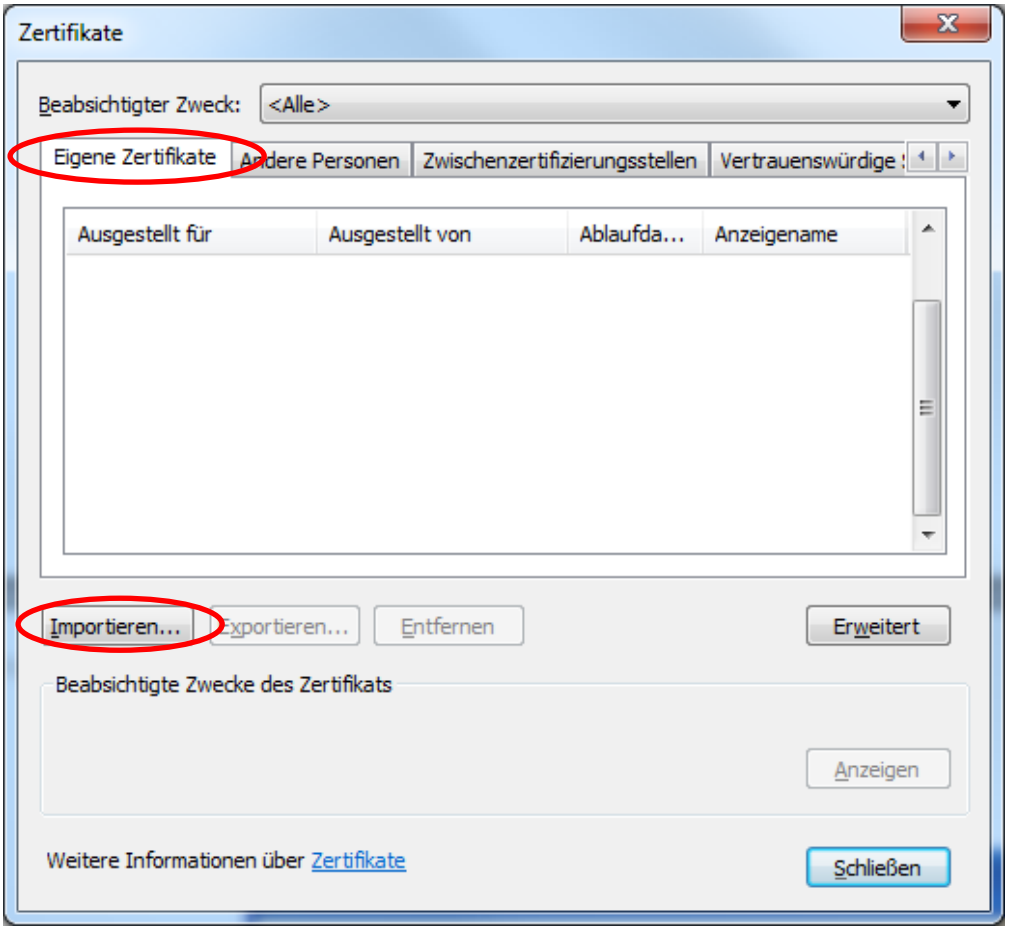


Abbildung 41: Ansicht des Microsoft-Zertifikatspeichers *Eigene Zertifikate*

Es öffnet sich nun der Zertifikatimport-Assistent. Bestätigen Sie das erste Fenster mit **Weiter**. Klicken Sie nun auf die Schaltfläche **Durchsuchen** und wählen Sie Ihr eigenes Zertifikat aus. Bestätigen Sie den Dialog mit **Öffnen** und klicken Sie anschließend auf **Weiter** (vgl. Abbildung 42).

Hinweis: Damit Ihnen Ihr eigenes Zertifikat im Auswahldialog angezeigt wird, ist es erforderlich, den Dateityp der angezeigten Dateien von „X.509-Zertifikat (*.cer,*.crt)“ auf „Privater Informationsaustausch (*.pfx,*.p12)“ zu ändern. Nur dann werden Ihnen auch solche Dateien angezeigt, die neben einem Zertifikat auch einen zugehörigen privaten Schlüssel beinhalten.

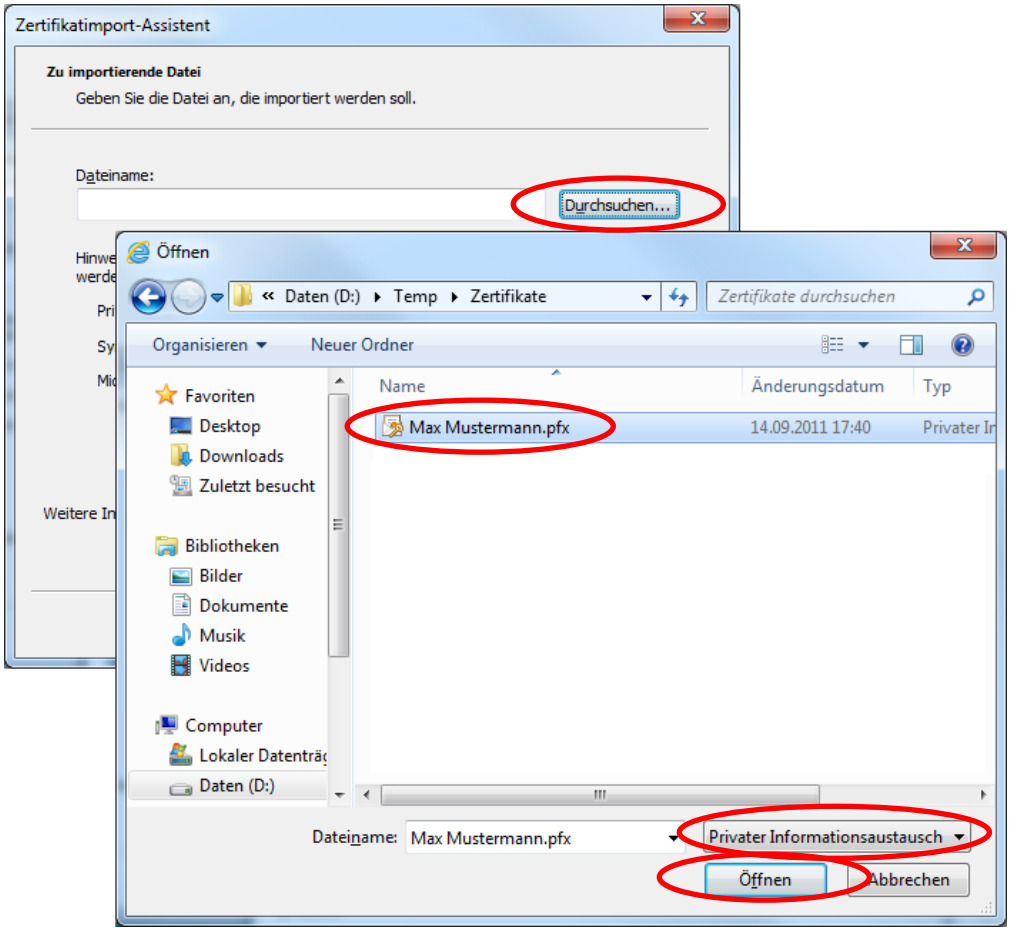


Abbildung 42: Auswahl des eigenen Zertifikats beim Import in den Microsoft-Zertifikatspeicher

Geben Sie nun das Kennwort ein, das Sie beim Speichern des Zertifikats einschließlich des privaten Schlüssels zum Schutz vor unberechtigtem Zugriff vergeben haben. Selektieren Sie außerdem zusätzlich zu der bereits standardmäßig aktivierten Option **Alle erweiterten Eigenschaften mit einbeziehen** die Optionen **Schlüssel als exportierbar markieren**, um ggfs. zu einem späteren Zeitpunkt das Zertifikat und den privaten Schlüssel erneut exportieren zu können sowie ggfls. die Option **Hohe Sicherheit für den privaten Schlüssel aktivieren** (vgl. Abbildung 43). Klicken Sie nun auf **Weiter**.

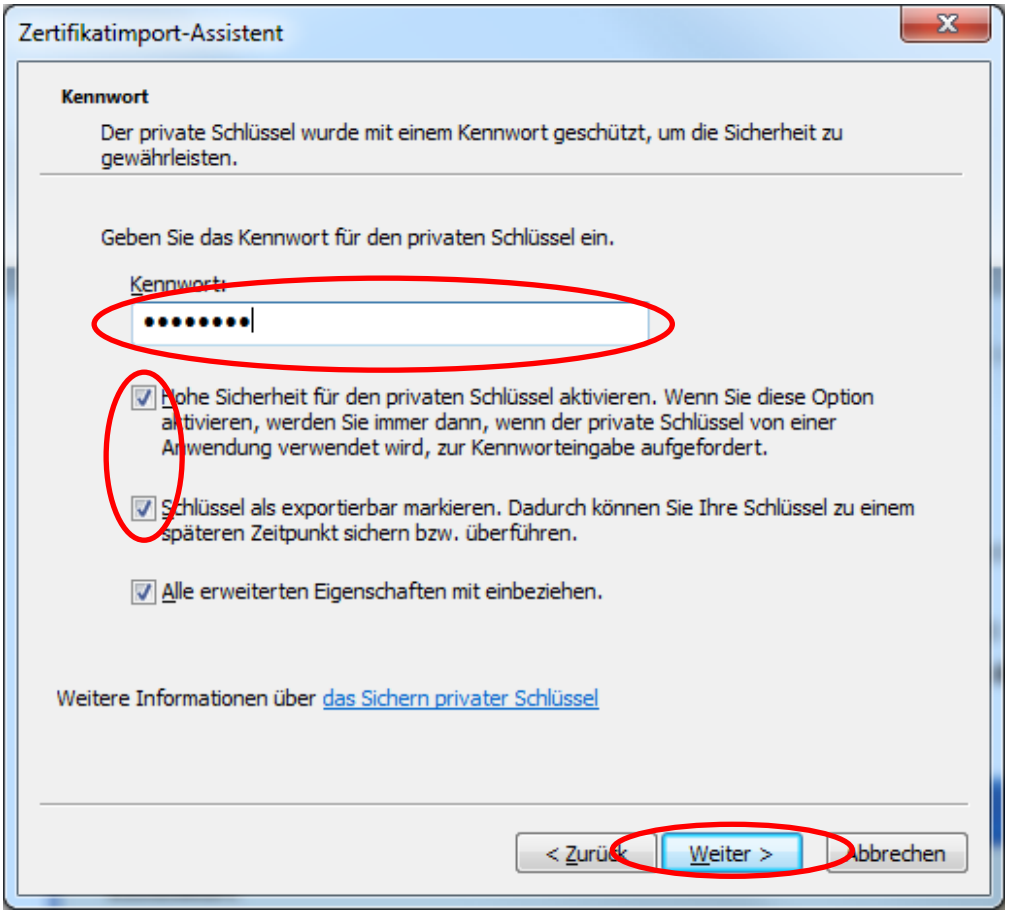


Abbildung 43: Eingabe des Kennworts und Festlegung der Import-Optionen beim Import des eigenen Zertifikats in den Microsoft-Zertifikatspeicher

Im folgenden Dialog können Sie die Vorgabewerte übernehmen und mit **Weiter** bestätigen (vgl. Abbildung 44).

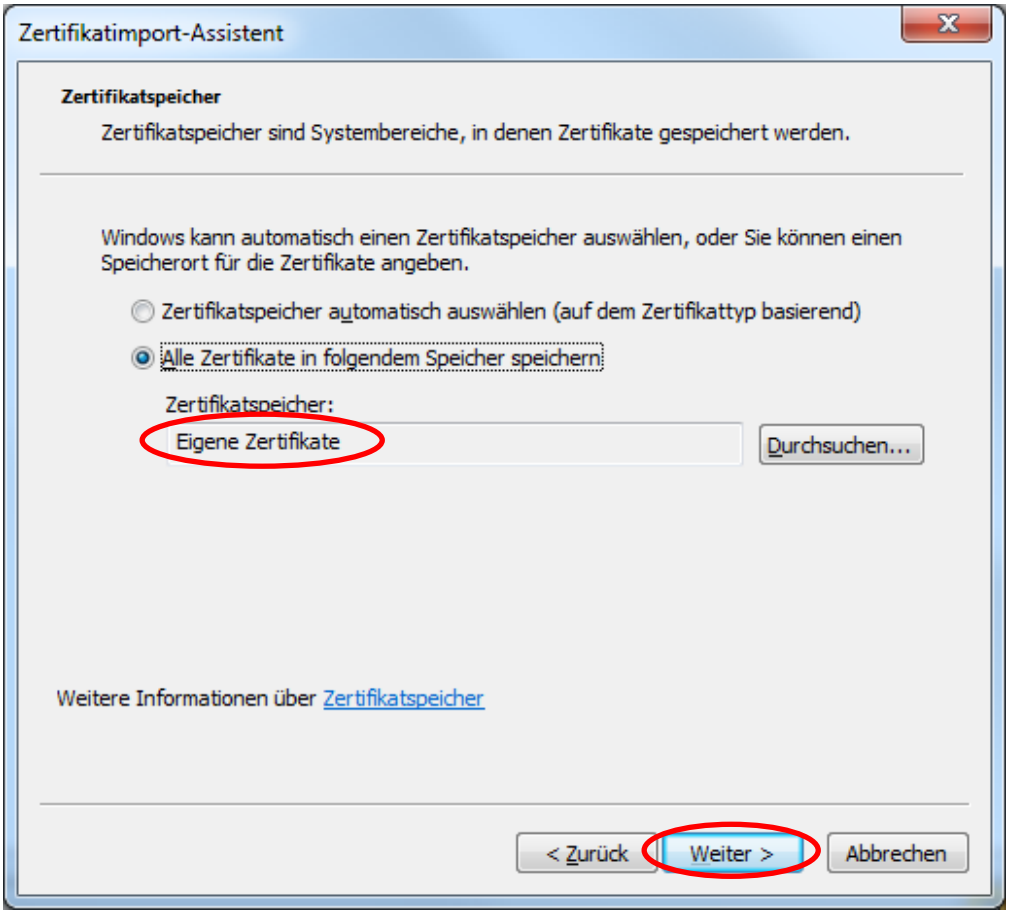


Abbildung 44: Auswahl des Zertifikatspeichers beim Import des eigenen Zertifikats in den Microsoft-Zertifikatspeicher

Es wird Ihnen nun der Dialog **Fertigstellen des Assistenten** angezeigt, der nochmals eine Zusammenfassung Ihrer Eingaben darstellt. Über die Schaltfläche **Fertig stellen** veranlassen Sie schließlich die Aufnahme Ihres eigenen Zertifikats in den Microsoft-Zertifikatspeicher. Falls Sie die Option **Hohe Sicherheit für den privaten Schlüssel aktivieren** (vgl. Abbildung 43) selektiert haben, werden Sie nun mit Hilfe von mehreren Dialogen aufgefordert, ein Kennwort für den Fall der Verwendung des privaten Schlüssels zu vergeben. Dieses Kennwort müssen Sie später beispielsweise immer beim Signieren bzw. beim Entschlüsseln von E-Mails angeben. Wählen Sie hierzu zunächst in dem in Abbildung 45 dargestellten Dialog die Schaltfläche **Sicherheitsstufe …**.

Hinweis: Falls Sie die Option **Hohe Sicherheit für den privaten Schlüssel aktivieren** (vgl. Abbildung 43) nicht selektiert haben, entfallen die im Folgenden dargestellten vier Dialoge.

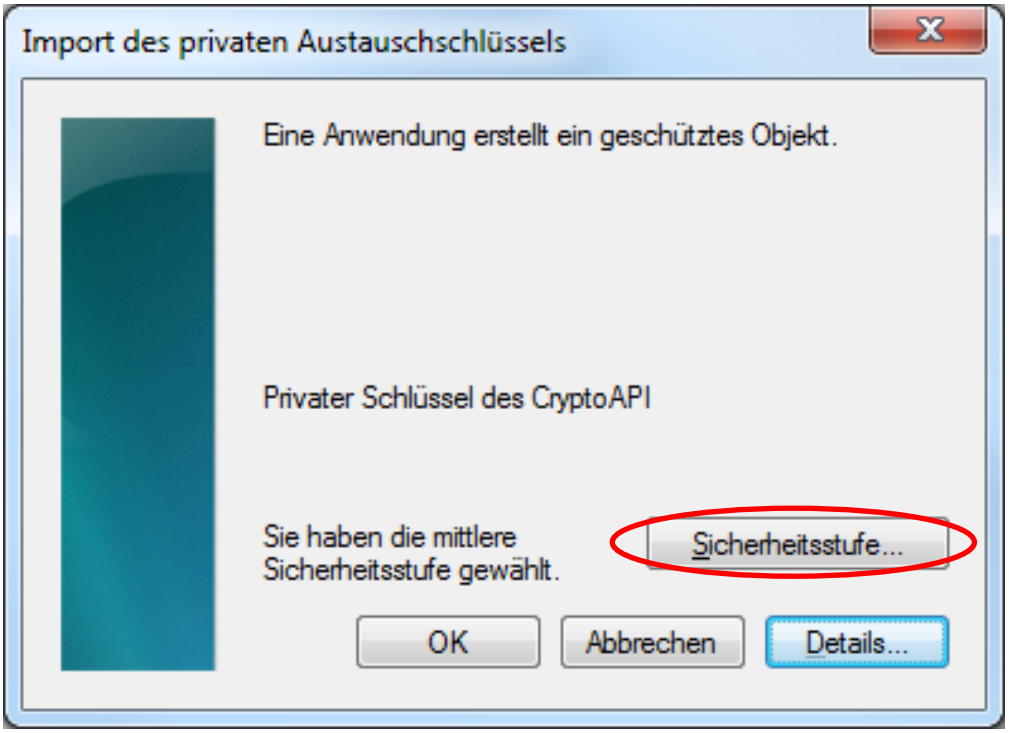


Abbildung 45: Anpassung der Sicherheitsstufe für den späteren Zugriff auf den eigenen privaten Schlüssel beim Import des eigenen Zertifikats in den Microsoft-Zertifikatspeicher

Zunächst ist erneut festzulegen, dass Sie bei Verwendung des zu Ihrem Zertifikat gehörenden privaten Schlüssels, um die Eingabe eines Kennworts gebeten werden wollen. Stellen Sie zu diesem Zweck die Sicherheitsstufe für den privaten Schlüssel von **Mittel** auf **Hoch** und verlassen Sie den Dialog anschließend über die Schaltfläche **Weiter** (vgl. Abbildung 46).

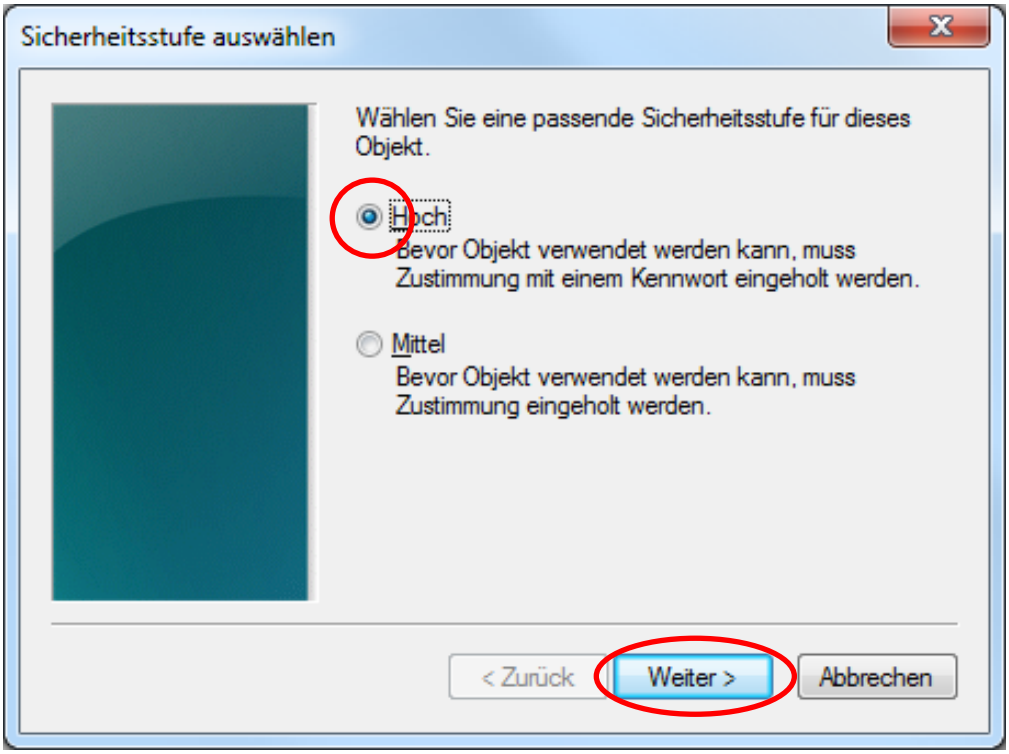


Abbildung 46: Änderung der Sicherheitsstufe, so dass beim späteren Zugriff auf den eigenen privaten Schlüssel ein Kennwort angefordert wird

Sie werden nun aufgefordert, das Kennwort festzulegen, das bei Verwendung des privaten Schlüssels angefordert werden soll. Aus Sicherheitsgründen muss die Eingabe zweifach erfolgen. Beenden Sie den Dialog über die Schaltfläche **Fertig stellen** (vgl. Abbildung 47).

Hinweis: Das Kennwort das Sie an dieser Stelle vergeben, wird immer dann angefordert, falls eine Anwendung den Zugriff auf Ihren privaten Schlüssel benötigt (beispielsweise beim Signieren oder Entschlüsseln von E-Mails). Es kann sich (muss sich aber nicht) vom Transportkennwort der Schlüssel- und Zertifikatsdatei unterscheiden, das Sie in Abbildung 43 eingeben haben. Sofern Sie ein anderes Kennwort vergeben, wählen Sie bitte ein sicheres Kennwort[3].

[3] Das Kennwort sollte mindestens eine Länge von zwölf Zeichen haben und neben Buchstaben in Klein- und Großschreibung, auch Ziffern und Sonderzeichen beinhalten.

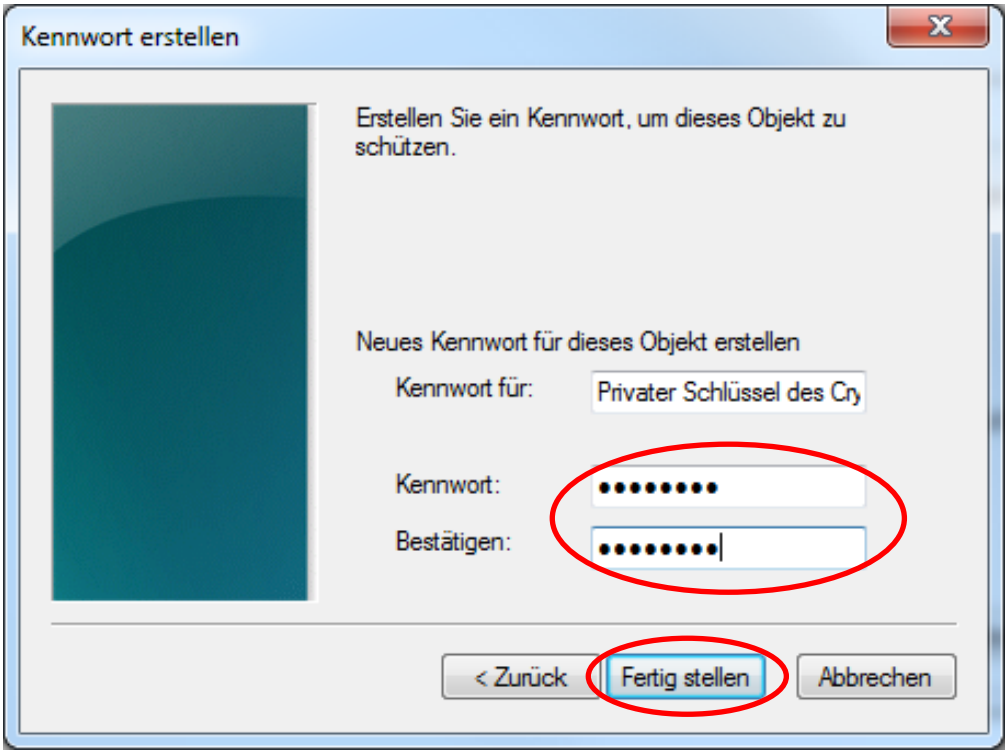


Abbildung 47: Festlegung des Kennworts, das beim späteren Zugriff auf den eigenen privaten Schlüssel angefordert werden soll

Sie kehren zurück zu dem bereits aus Abbildung 45 bekannten Dialog. Die Sicherheitsstufe ist jedoch nun entsprechend Ihrer Auswahl angepasst (vgl. Abbildung 48). Nach Betätigung der Schaltfläche **OK** wird nun der Import Ihres eigenes Zertifikats und zugehörigen privaten Schlüssels in den Microsoft-Zertifikatspeicher abschließend vorgenommen und der erfolgreiche Import durch die in Abbildung 49 dargestellte Meldung bestätigt. Bestätigen Sie auch diesen Dialog mit **OK**.

Ihr eigenes Zertifikat ist nun im Microsoft-Zertifikatspeicher verfügbar und kann für den sicheren E-Mail-Verkehr beispielsweise in Outlook konfiguriert werden (vgl. Abschnitte 4.2.1.1ff.).

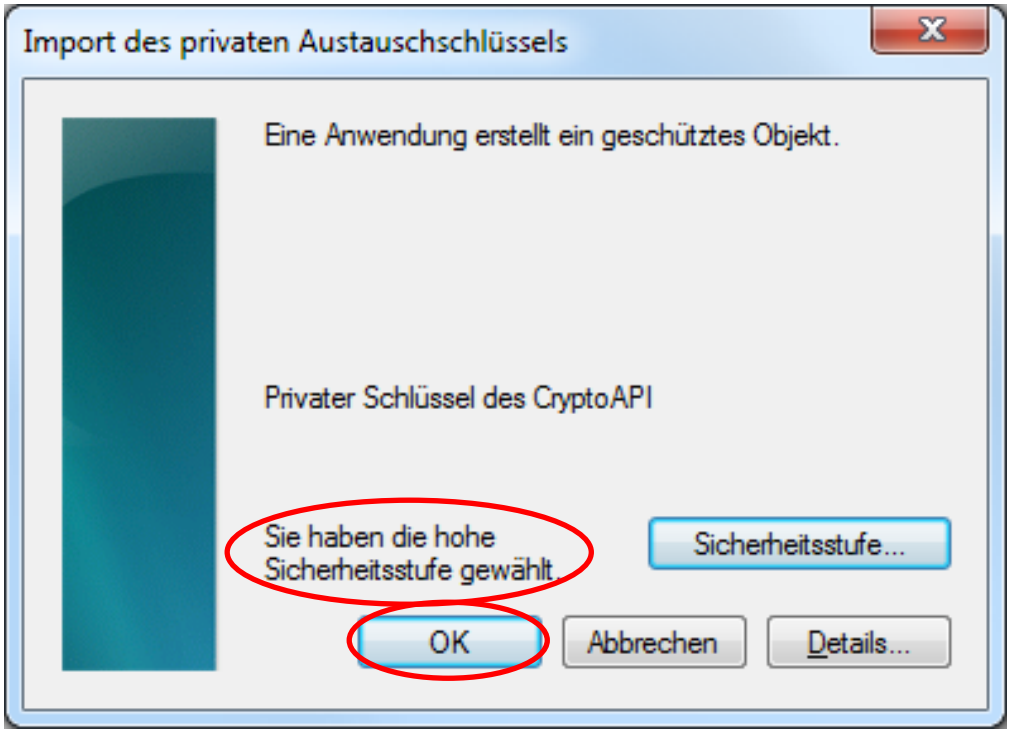


Abbildung 48: Angepasste Sicherheitsstufe für den späteren Zugriff auf den eigenen privaten Schlüssel beim Import des eigenen Zertifikats in den Microsoft-Zertifikatspeicher

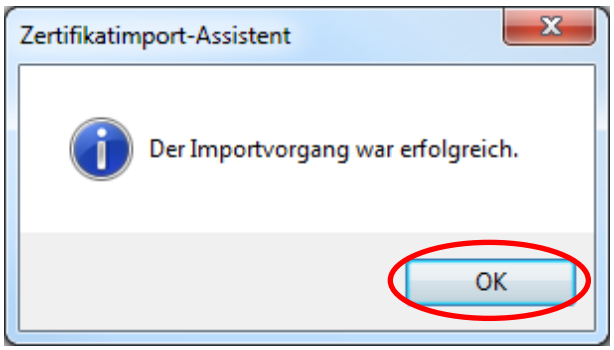


Abbildung 49: Erfolgreicher Abschluss des Imports des eigenen Zertifikats und privaten Schlüssels in den Microsoft-Zertifikatspeicher

4.2.1.1 Ein eigenes Zertifikat in Microsoft Outlook 2010 konfigurieren

Um Microsoft Outlook 2010 das eigene Zertifikat und den privaten Schlüssel bekannt zu machen, das Outlook zum Signieren bzw. Entschlüsseln von E-Mails verwenden soll, muss das Zertifikat im E-Mail-Client konfiguriert werden.

Öffnen Sie hierzu zunächst das **Sicherheitscenter** über **Datei → Optionen → Sicherheitscenter → Einstellungen für das Sicherheitscenter … → E-Mail-Sicherheit**. Nun wählen Sie in der Rubrik „Verschlüsselte E-Mail-Nachrichten" die Schaltfläche **Einstellungen** (vgl. Abbildung 50).

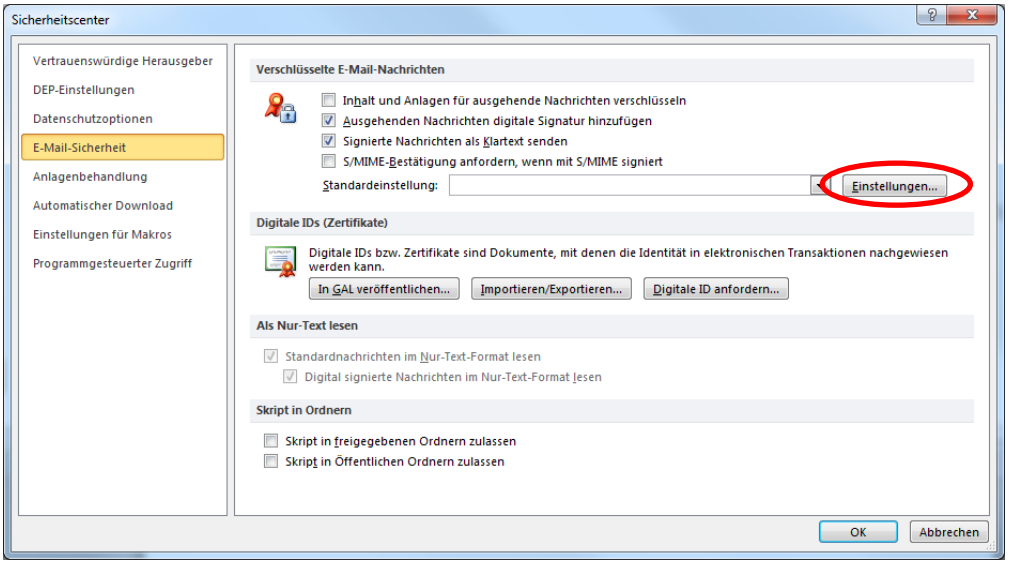


Abbildung 50: Outlook 2010 – Sicherheitscenter

Es öffnet sich der Dialog „Sicherheitseinstellungen ändern" (vgl. Abbildung 51). Passen Sie ggfs. den unter **Namen der Sicherheitseinstellung** angegebenen Namen Ihren Bedürfnissen entsprechend an und klicken Sie auf die obere der beiden Schaltflächen **Auswählen**, um das Signaturzertifikat festzulegen. Es wird Ihnen eine Liste aller Zertifikate angezeigt, die über den Zweck „digitale Signatur" verfügen und zu denen Sie einen privaten Schlüssel besitzen (in der Regel ist nur ein solches Zertifikat auf Ihrem System vorhanden). Wählen Sie Ihr eigenes Zertifikat der PKI für Fraunhofer Kontakte aus. Das ausgewählte Zertifikat wird automatisch – da es auch über den Zweck Verschlüsselung verfügt – auch als Verschlüsselungszertifikat eingetragen. Schließen Sie nun alle geöffneten Dialoge über die Schaltfläche **OK**.

Damit ist die Konfiguration Ihres eigenen Zertifikats in Microsoft Outlook 2010 abgeschlossen und Sie in der Lage digital signierte E-Mails zu versenden bzw. für Ihre E-Mail-Adresse verschlüsselte E-Mails zu entschlüsseln.

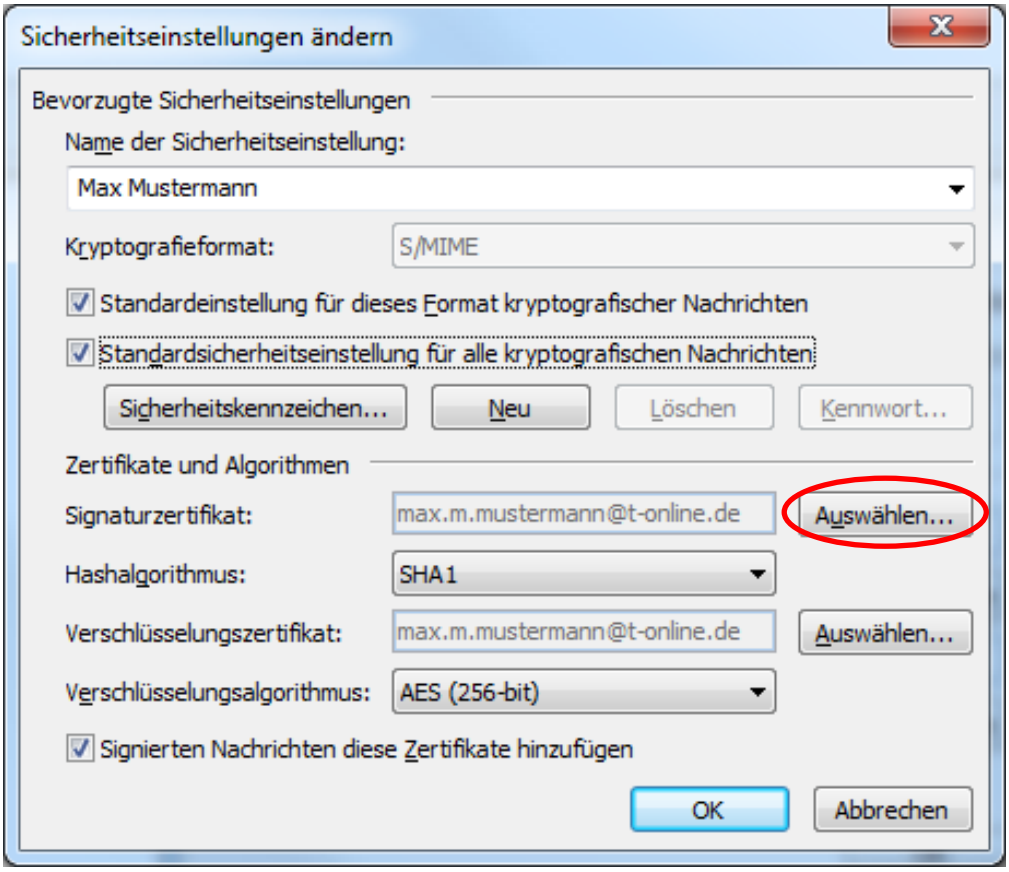


Abbildung 51: Outlook 2010 – Eigenes Zertifikat konfigurieren

4.2.1.2 Ein eigenes Zertifikat in Microsoft Outlook 2007 konfigurieren

Um Microsoft Outlook 2007 das eigene Zertifikat und den privaten Schlüssel bekannt zu machen, das Outlook zum Signieren bzw. Entschlüsseln von E-Mails verwenden soll, muss das Zertifikat im E-Mail-Client konfiguriert werden.

Öffnen Sie hierzu zunächst das **Vertrauensstellungcenter** über **Extras → Vertrauensstellungscenter → E-Mail-Sicherheit**. Nun wählen Sie in der Rubrik „Verschlüsselte E-Mail-Nachrichten" die Schaltfläche **Einstellungen** (vgl. Abbildung 52).

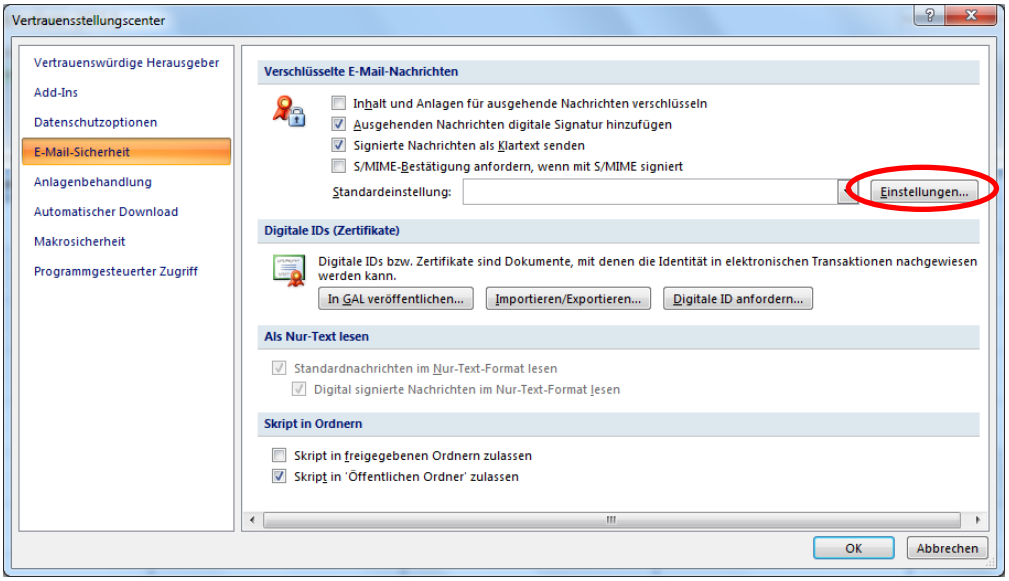


Abbildung 52: Outlook 2007 – Vertrauensstellungscenter

Es öffnet sich der Dialog „Sicherheitseinstellungen ändern“ (vgl. Abbildung 53). Passen Sie ggfls. den unter **Namen der Sicherheitseinstellung** angegebenen Namen Ihren Bedürfnissen entsprechend an bzw. legen Sie diesen fest und klicken Sie auf die obere der beiden Schaltflächen **Auswählen**, um das Signaturzertifikat festzulegen. Es wird Ihnen eine Liste aller Zertifikate angezeigt, die über den Zweck „digitale Signatur“ verfügen und zu denen Sie einen privaten Schlüssel besitzen (in der Regel ist nur ein solches Zertifikat auf Ihrem System vorhanden). Wählen Sie Ihr eigenes Zertifikat der PKI für Fraunhofer Kontakte aus. Das ausgewählte Zertifikat wird automatisch – da es auch über den Zweck Verschlüsselung verfügt – auch als Verschlüsselungszertifikat eingetragen. Selektieren Sie – sofern nicht bereits standardmäßig von Outlook vorgenommen – auch die Optionen **Standardeinstellung für dieses Format kryptografischer Nachrichten**, **Standardsicherheitseinstellung für alle kryptografischen** Nachrichten sowie **Signierten Nachrichten diese Zertifikate hinzufügen.** Schließen Sie nun alle geöffneten Dialoge über die Schaltfläche **OK**.

Damit ist die Konfiguration Ihres eigenen Zertifikats in Microsoft Outlook 2007 abgeschlossen und Sie in der Lage digital signierte E-Mails zu versenden bzw. für Ihre E-Mail-Adresse verschlüsselte E-Mails zu entschlüsseln.

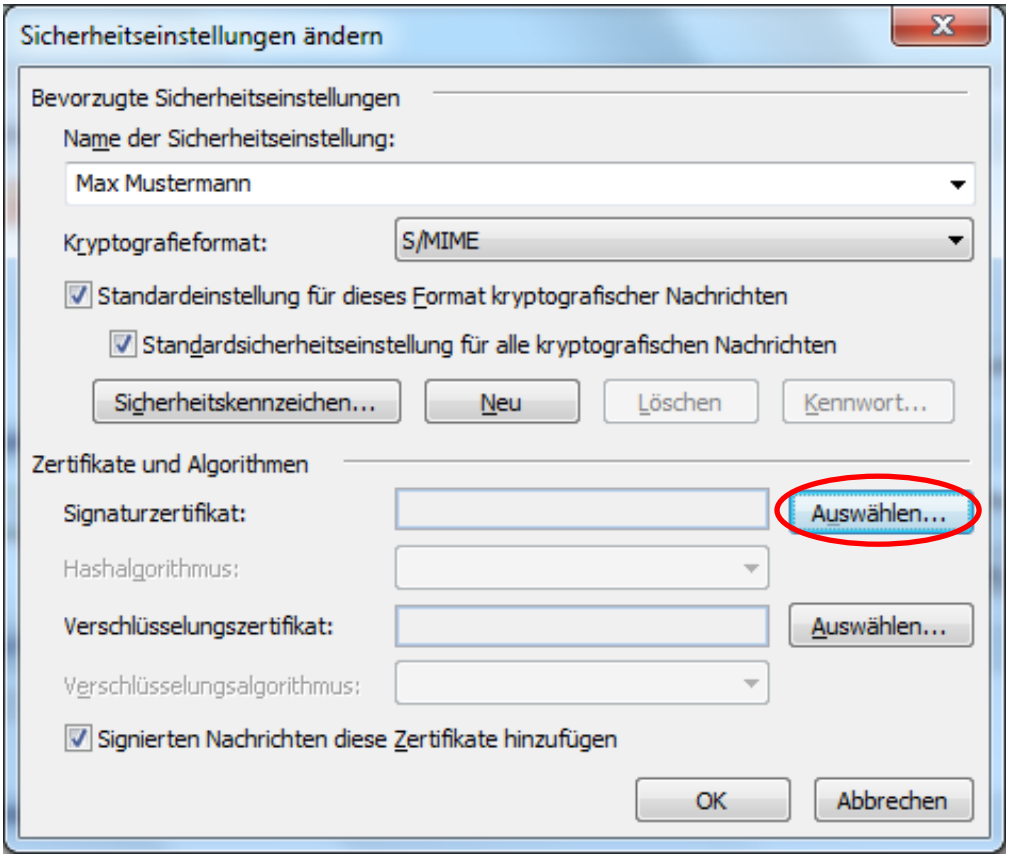


Abbildung 53: Outlook 2007 – Eigenes Zertifikat konfigurieren

4.2.1.3 Ein eigenes Zertifikat in Microsoft Outlook 2003 konfigurieren

Um Microsoft Outlook 2003 das eigene Zertifikat und den privaten Schlüssel bekannt zu machen, das Outlook zum Signieren bzw. Entschlüsseln von E-Mails verwenden soll, muss das Zertifikat im E-Mail-Client konfiguriert werden.

Öffnen Sie hierzu zunächst die Outlook **S/MIME-Optionen** über **Extras → Optionen**. Nun wählen Sie den Reiter **Sicherheit** und dort in der Rubrik „Verschlüsselte E-Mail-Nachrichten" die Schaltfläche **Einstellungen** (vgl. Abbildung 54).

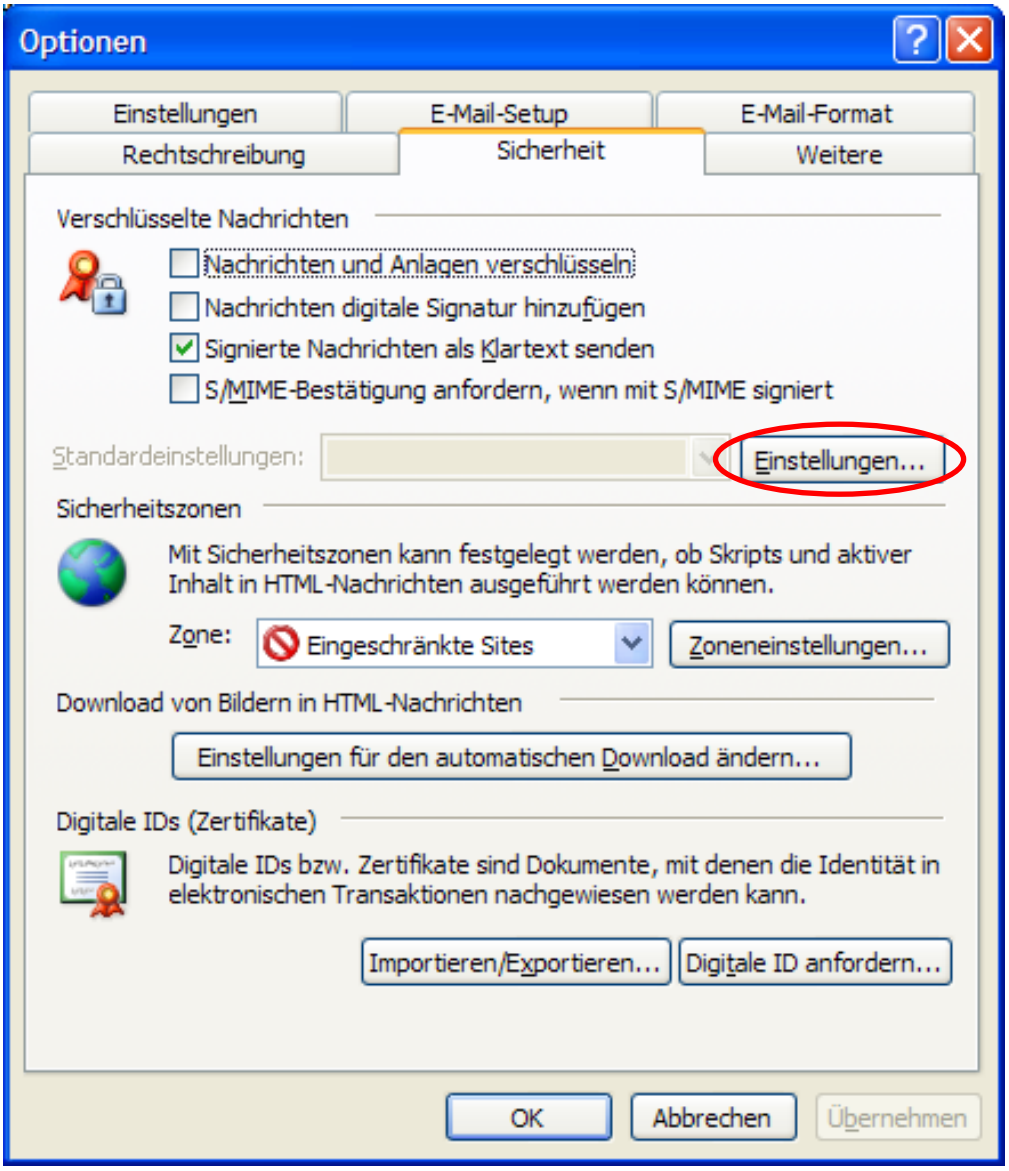


Abbildung 54: Outlook 2003 – S/MIME Optionen

Es öffnet sich der Dialog „Sicherheitseinstellungen ändern“ (vgl. Abbildung 55). Passen Sie ggfls. den unter **Namen der Sicherheitseinstellung** angegebenen Namen Ihren Bedürfnissen entsprechend an bzw. legen Sie diesen fest und klicken Sie auf die obere der beiden Schaltflächen **Auswählen**, um das Signaturzertifikat festzulegen. Es wird Ihnen eine Liste aller Zertifikate angezeigt, die über den Zweck „digitale Signatur“ verfügen und zu denen Sie einen privaten Schlüssel besitzen (in der Regel ist nur ein solches Zertifikat auf Ihrem System vorhanden). Wählen Sie Ihr eigenes Zertifikat der PKI für Fraunhofer Kontakte aus. Das ausgewählte Zertifikat wird automatisch – da es auch über den Zweck Verschlüsselung verfügt – auch als Verschlüsselungszertifikat eingetragen. Selektieren Sie – sofern nicht bereits standardmäßig von Outlook vorgenommen –

auch die Optionen **Standardeinstellung für dieses Format kryptografischer Nachrichten**, **Standardsicherheitseinstellung für alle kryptografischen** Nachrichten sowie **Signierten Nachrichten diese Zertifikate hinzufügen.** Schließen Sie nun alle geöffneten Dialoge über die Schaltfläche **OK**.

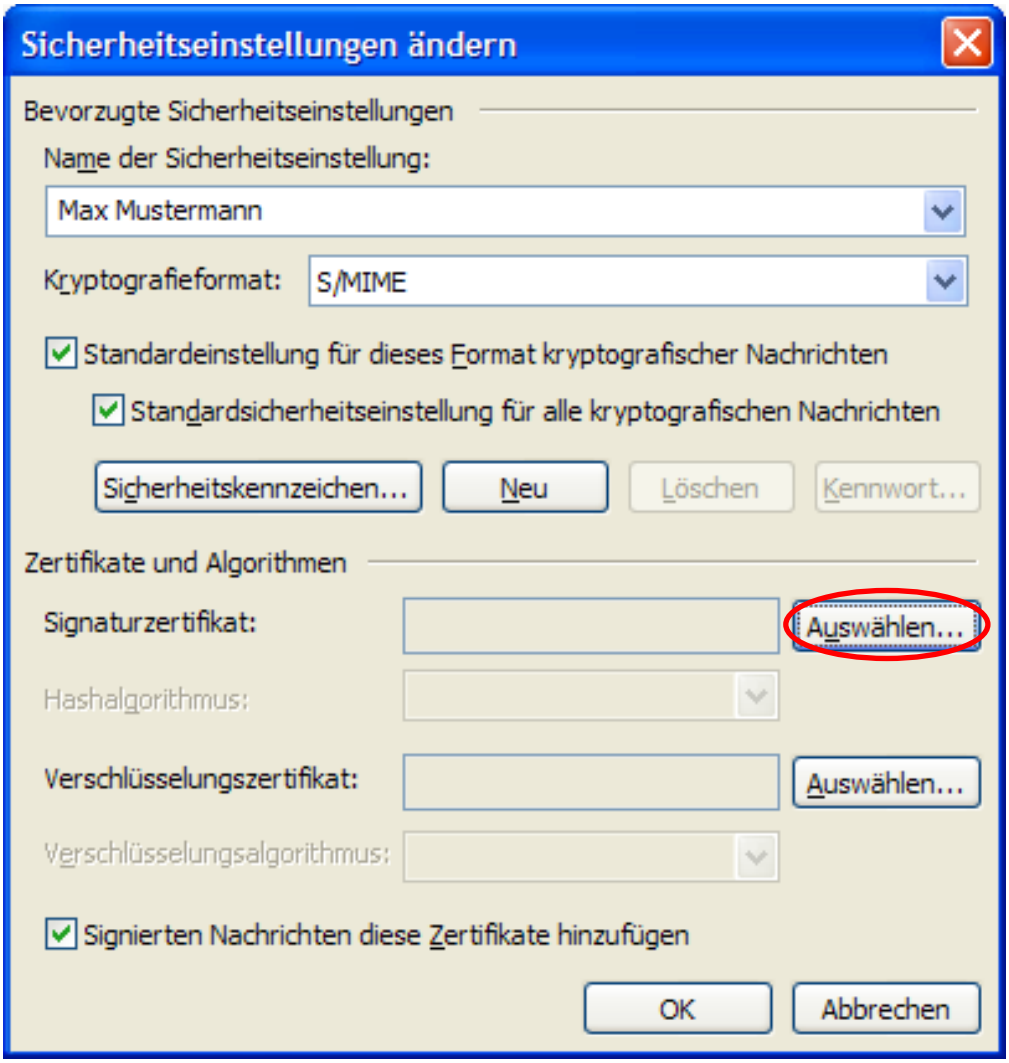


Abbildung 55: Outlook 2003 – Eigenes Zertifikat konfigurieren

Damit ist die Konfiguration Ihres eigenen Zertifikats in Microsoft Outlook 2003 abgeschlossen und Sie in der Lage digital signierte E-Mails zu versenden bzw. für Ihre E-Mail-Adresse verschlüsselte E-Mails zu entschlüsseln.

4.2.2 Ein eigenes Zertifikat in Mozilla Thunderbird aufnehmen und konfigurieren

Hinweis: Die Screenshots wurden unter Verwendung von Mozilla Thunderbird in der Version 7 angefertigt.

Falls Sie Mozilla Thunderbird zur E-Mail-Kommunikation verwenden, muss das eigene Zertifikat in den Zertifikatspeicher von Mozilla Thunderbird importiert werden.

Um Ihr eigenes Zertifikat in den Zertifikatspeicher von Thunderbird zu importieren, öffnen Sie dessen Zertifikatspeicher über **Extras → Einstellungen → Erweitert → Zertifikate → Zertifikate** und aktivieren Sie den Reiter **Ihre Zertifikate**. Klicken Sie auf die Schaltfläche **Importieren** (vgl. Abbildung 56).

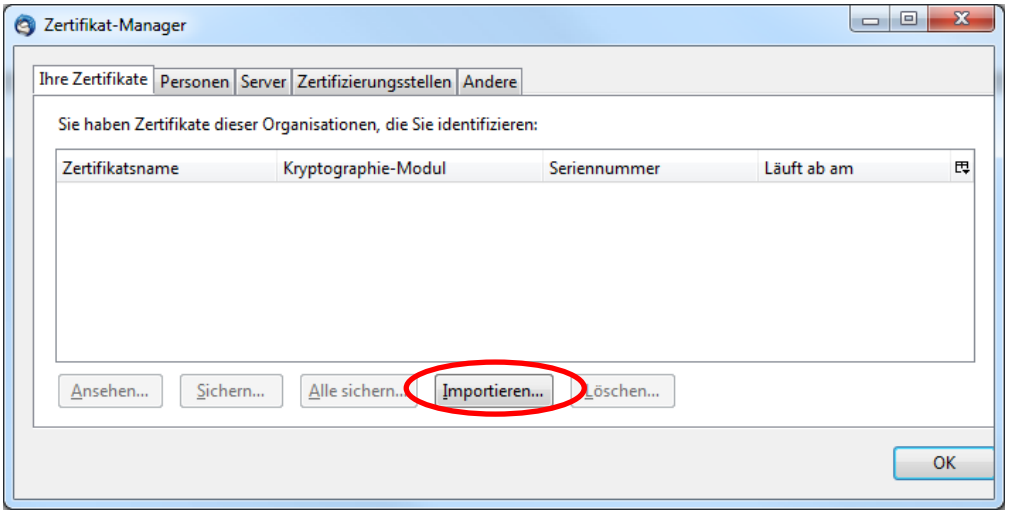


Abbildung 56: Ansicht des Thunderbird-Zertifikatspeichers *Ihre Zertifikate*

Es öffnet sich nun ein Dateiauswahldialog. Navigieren Sie nun zum Ablageort an dem Sie Ihr eigenes Zertifikat der PKI für Fraunhofer Kontakte abgelegt haben und wählen Sie dieses aus. Schließen Sie den Dialog mit **Öffnen** (vgl. Abbildung 57).

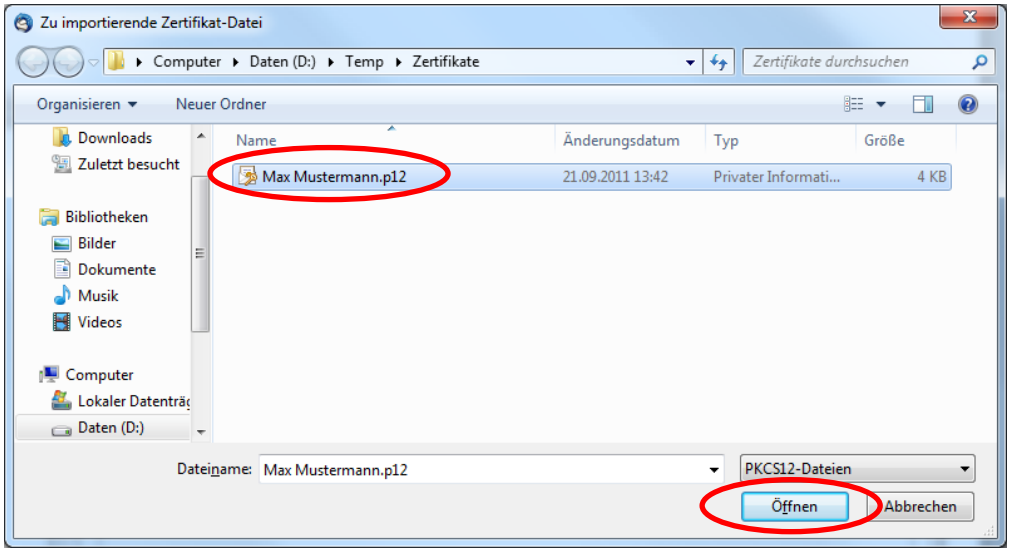


Abbildung 57: Auswahl des eigenen Zertifikats der PKI für Fraunhofer-Kontakte beim Import in den Thunderbird-Zertifikatspeicher

Geben Sie nun das Kennwort ein, das Sie beim Speichern des Zertifikats einschließlich des privaten Schlüssels zum Schutz vor unberechtigtem Zugriff vergeben haben. Klicken Sie anschließend auf **OK** (vgl. Abbildung 58).

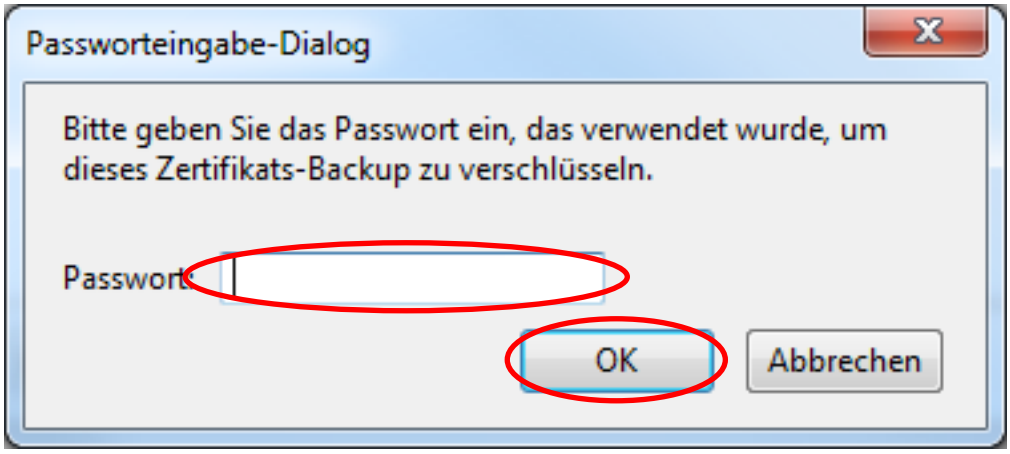


Abbildung 58: Eingabe des Kennworts des eigenen Zertifikats der PKI für Fraunhofer-Kontakte beim Import in den Thunderbird-Zertifikatspeicher

Nachdem der Import Ihres Zertifikats und privaten Schlüssels erfolgreich durchgeführt wurde, wird Ihnen dies entsprechend bestätigt (vgl. Abbildung 59). Klicken Sie auf die Schaltfläche **OK**. Der Import-Vorgang Ihres eigenen Zertifikats in den Zertifikatspeicher von Mozilla-Thunderbird ist damit beendet und Sie können das Zertifikat jetzt für den sicheren E-Mail-Verkehr konfigurieren, so

dass Sie anschließend in der Lage sind, E-Mails zu signieren bzw. zu entschlüsseln.

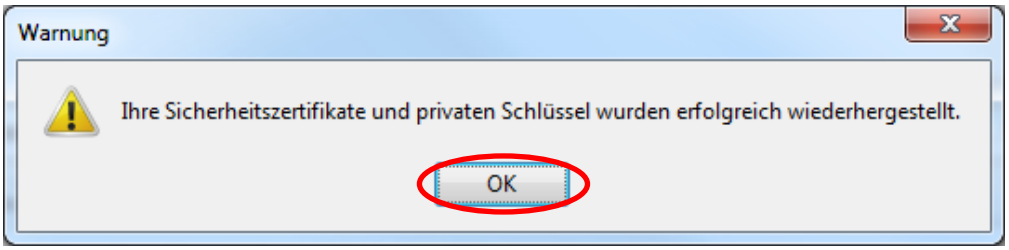


Abbildung 59: Erfolgreicher Abschluss des Imports des eigenen Zertifikats und privaten Schlüssels in den Thunderbird-Zertifikatspeicher

Öffnen Sie hierzu zunächst die **S/MIME-Sicherheit** über **Extras → Konten-Einstellungen → S/MIME-Sicherheit** (vgl. Abbildung 60). Klicken Sie auf die obere der beiden Schaltflächen **Auswählen**, um zunächst das Signaturzertifikat festzulegen.

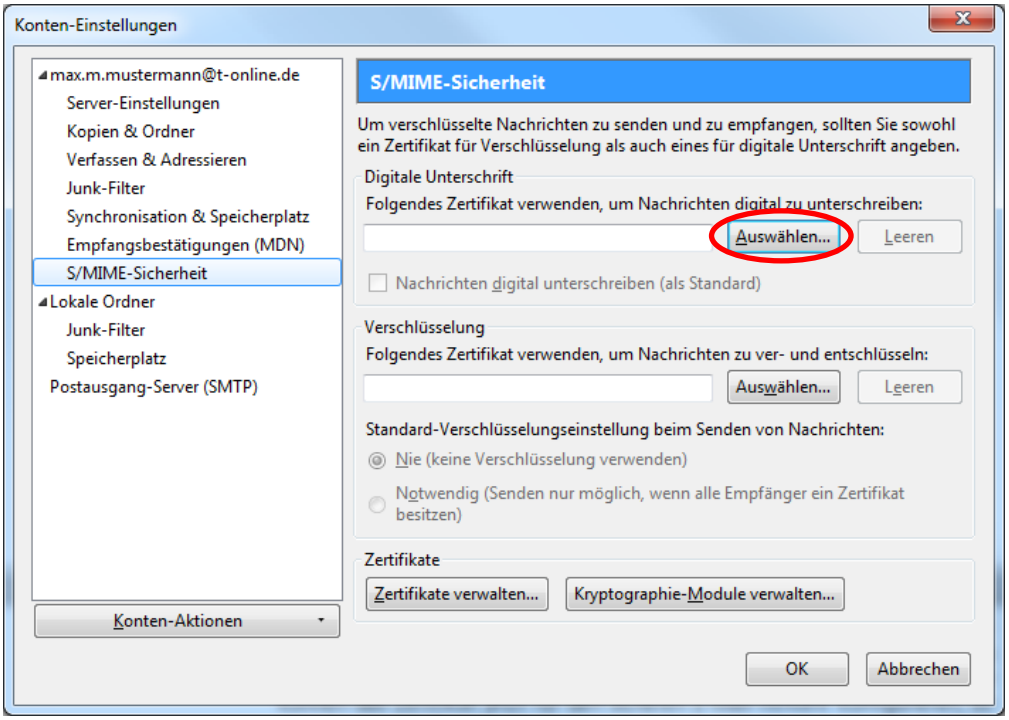


Abbildung 60: Mozilla-Thunderbird – Festlegung der S/MIME-Einstellungen

Es werden Ihnen in einer Listbox alle Zertifikate angezeigt, die über den Zweck „digitale Signatur“ verfügen und zu denen Sie einen privaten Schlüssel besitzen (in der Regel ist nur ein solches Zertifikat auf Ihrem System vorhanden). Wählen Sie Ihr eigenes Zertifikat der PKI für Fraunhofer Kontakte aus und beenden Sie den Dialog über die Schaltfläche **OK** (vgl. Abbildung 61).

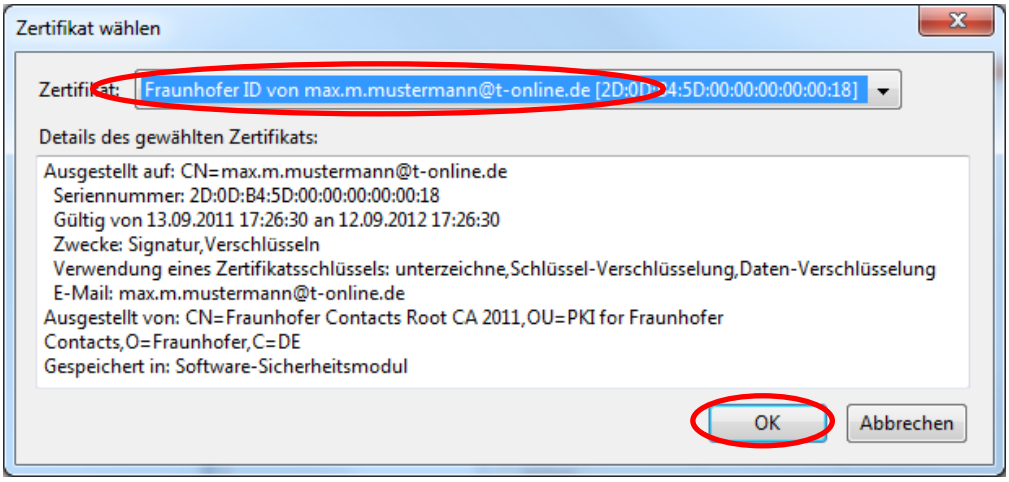


Abbildung 61: Mozilla-Thunderbird – Festlegung des Signaturzertifikats

Im Anschluss werden Sie nun gefragt, ob Sie dieses Zertifikat auch zur Entschlüsselung von E-Mails einsetzen möchten. Bestätigen Sie dies durch Anklicken der Schaltfläche **Ja** (vgl. Abbildung 62).

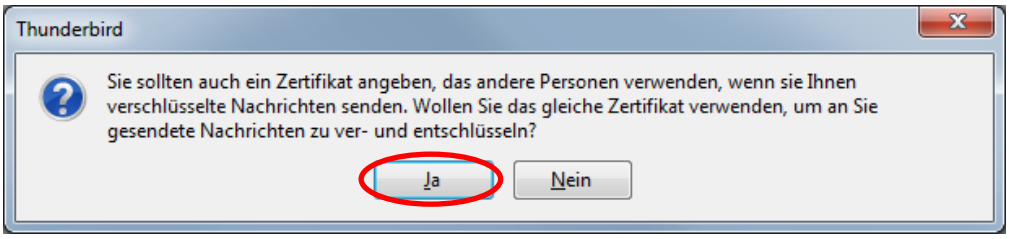


Abbildung 62: Mozilla-Thunderbird – Festlegung des Signaturzertifikats

Schließen Sie nun alle geöffneten Dialoge über die Schaltfläche **OK**. Damit ist die Konfiguration Ihres eigenen Zertifikats in Mozilla Thunderbird abgeschlossen und Sie in der Lage digital signierte E-Mails zu versenden bzw. für Ihre E-Mail-Adresse verschlüsselte E-Mails zu entschlüsseln.

4.3 Ein Zertifikat eines Fraunhofer Mitarbeiters in den E-Mail-Client aufnehmen

Hinweis: Die Aufnahme eines Zertifikats eines Fraunhofer Mitarbeiters in den E-Mail-Client ist in der Regel nicht notwendig, da diese automatisch vorgenommen wird, sobald Sie eine von einem Fraunhofer Mitarbeiter signierte E-Mail erhalten und Sie diese beantworten. Haben Sie das Zertifikat jedoch auf anderem Wege erhalten, können Sie es wie in den folgenden Unterabschnitten beschrieben in den jeweiligen E-Mail-Client importieren.

4.3.1 Ein Zertifikat eines Fraunhofer Mitarbeiters in Microsoft Outlook 2010 aufnehmen

Öffnen Sie zunächst auf dem Reiter **Start** eine neue E-Mail über die Schaltfläche **Neue E-Mail-Nachricht** und geben Sie die E-Mail Adresse des Fraunhofer Mitarbeiters als Empfänger ein. Klicken Sie dann mit der rechten Maustaste auf die eingegebene E-Mail-Adresse und wählen Sie im Kontextmenü die Option **Zu Outlook-Kontakten hinzufügen** (vgl. Abbildung 63).

Hinweis: Ist der Fraunhofer Mitarbeiter bereits in Ihren Kontakten enthalten, so öffnen Sie dessen Kontaktdaten über den Kontextmenüeintrag **Outlook-Kontakt nachschlagen**.

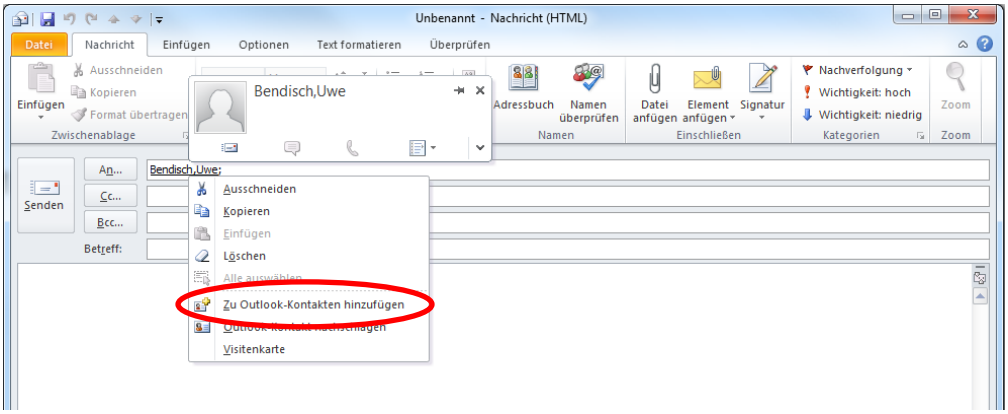


Abbildung 63: Hinzufügen eines Fraunhofer Mitarbeiters als Kontakt in Outlook 2010

Ihnen wird nun der Kontakteintrag angezeigt. Aktivieren Sie die Schaltfläche **Zertifikate** im Reiter **Kontakt** und klicken Sie dann auf die Schaltfläche **Importieren** (vgl. Abbildung 64).

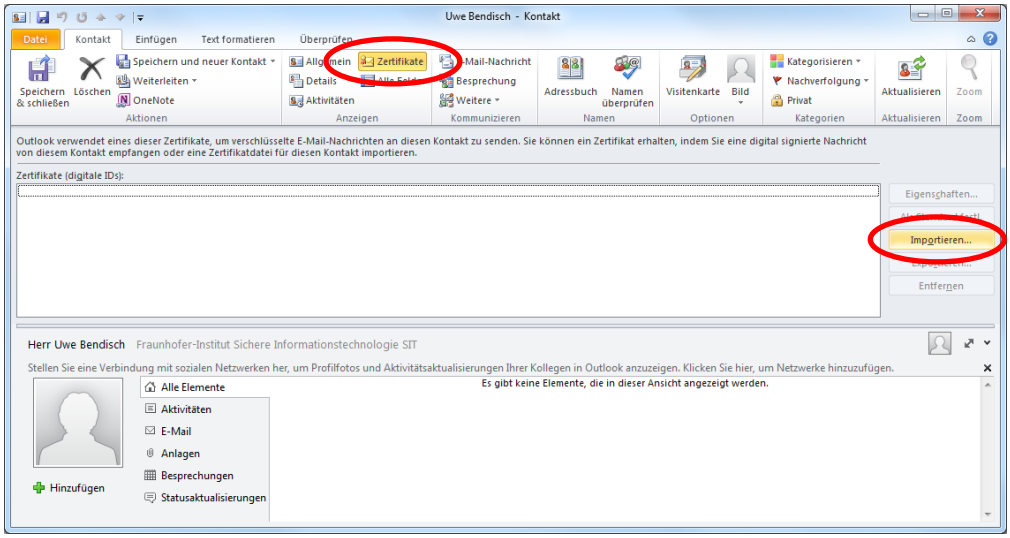


Abbildung 64: Importieren des Zertifikats des Fraunhofer Mitarbeiters in Outlook 2010

Wechseln Sie nun zu dem Verzeichnis, in dem Sie das Zertifikat des Fraunhofer Mitarbeiters abgelegt haben und wählen Sie das Zertifikat aus. Klicken Sie auf **Öffnen** (vgl. Abbildung 65).

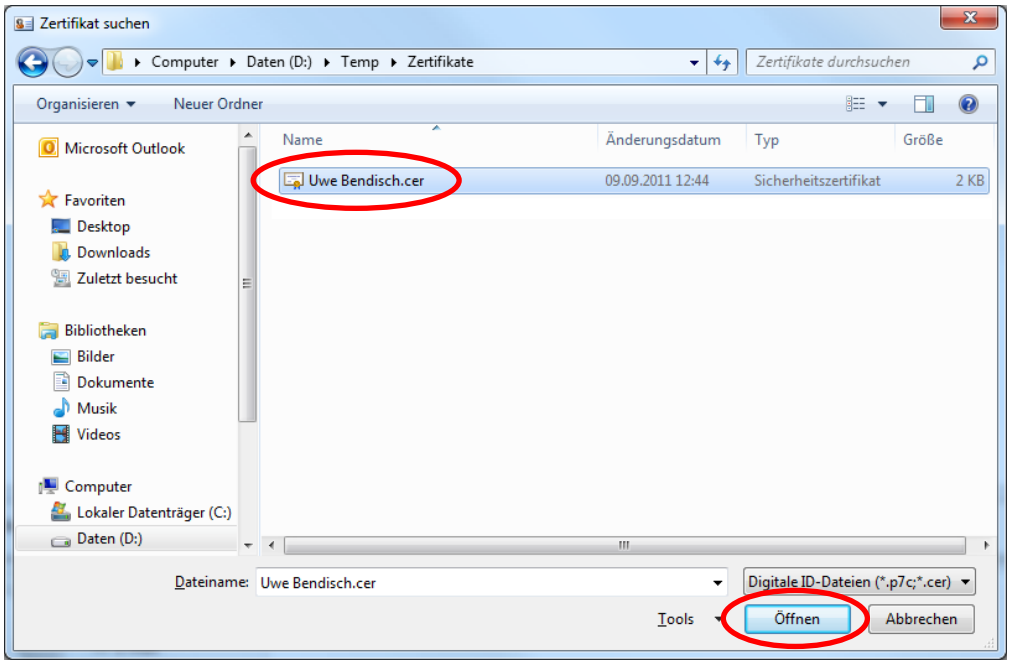


Abbildung 65: Auswahl des Zertifikats des Fraunhofer Mitarbeiters

Das Zertifikat ist nun dem Zertifikatspeicher hinzugefügt. Klicken Sie nun auf **Speichern & schließen** (vgl. Abbildung 66).

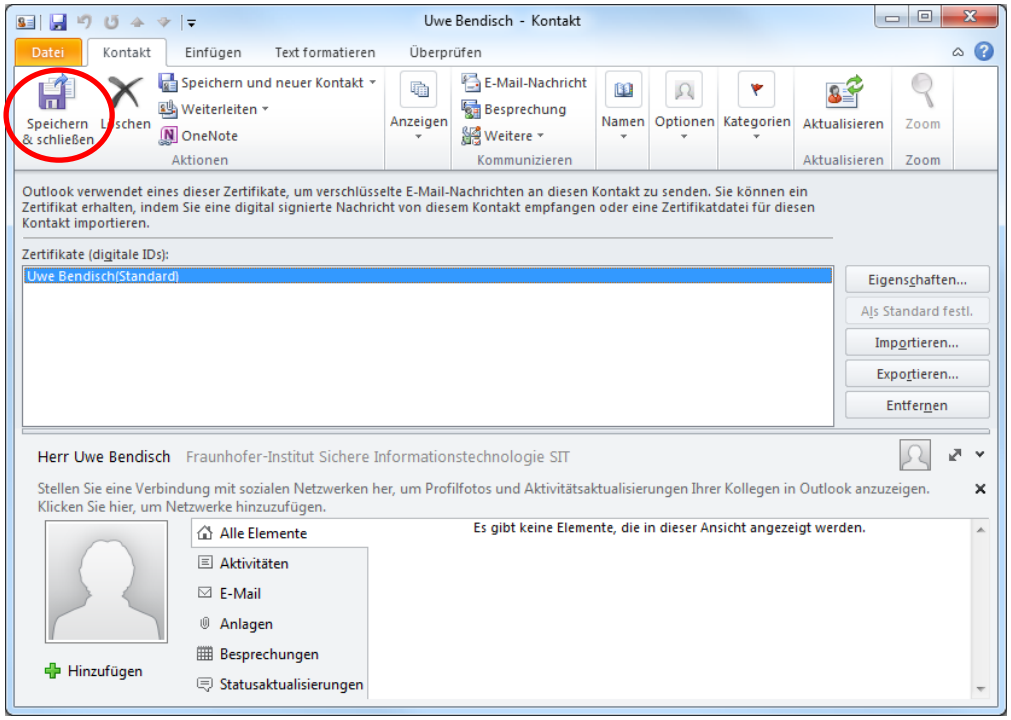


Abbildung 66: Speichern der Zertifikatszuordnung in Outlook 2010

Damit ist die Integration des Zertifikats des Fraunhofer Mitarbeiters in Outlook 2010 abgeschlossen und das Zertifikat kann für den sicheren E-Mail-Verkehr verwendet werden.

4.3.2 Ein Zertifikat eines Fraunhofer Mitarbeiters in Microsoft Outlook 2007 aufnehmen

Öffnen Sie zunächst eine neue E-Mail und geben Sie die E-Mail Adresse des Fraunhofer Mitarbeiters als Empfänger ein. Klicken Sie dann mit der rechten Maustaste auf die eingegebene E-Mail-Adresse und wählen Sie im Kontextmenü die Option **Zu Outlook-Kontakten hinzufügen** (vgl. Abbildung 67).

Hinweis: Ist der Fraunhofer Mitarbeiter bereits in Ihren Kontakten enthalten, so öffnen Sie dessen Kontaktdaten über den Kontextmenüeintrag **Outlook-Kontakt nachschlagen**.

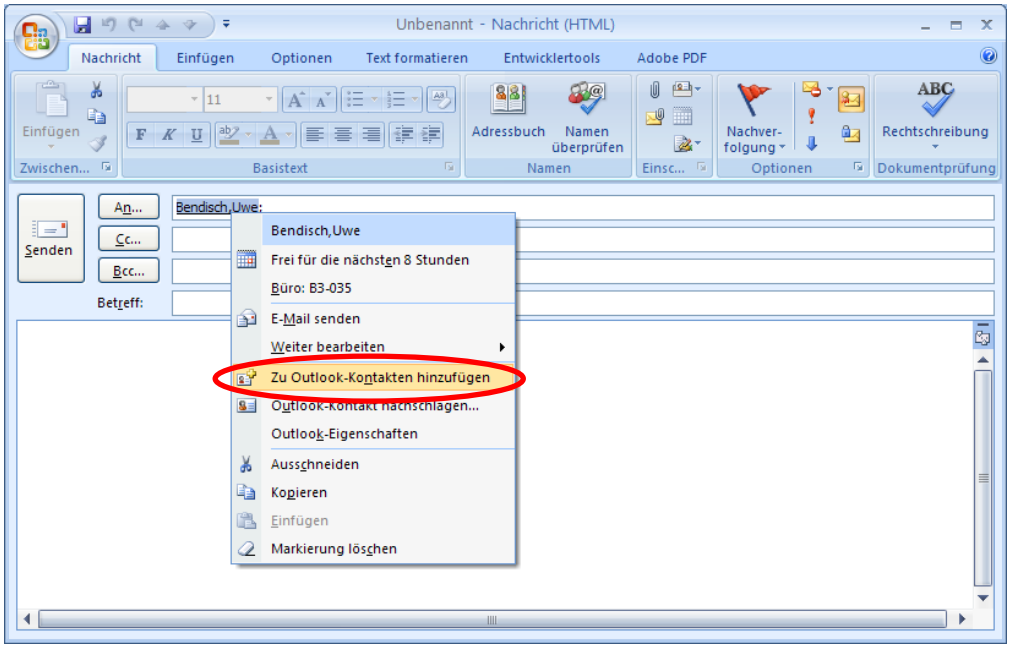


Abbildung 67: Hinzufügen eines Fraunhofer Mitarbeiters als Kontakt in Outlook 2007

Ihnen wird nun der Kontakteintrag angezeigt. Aktivieren Sie die Schaltfläche **Zertifikate** im Reiter **Kontakt** und klicken Sie dann auf die Schaltfläche **Importieren** (vgl. Abbildung 68).

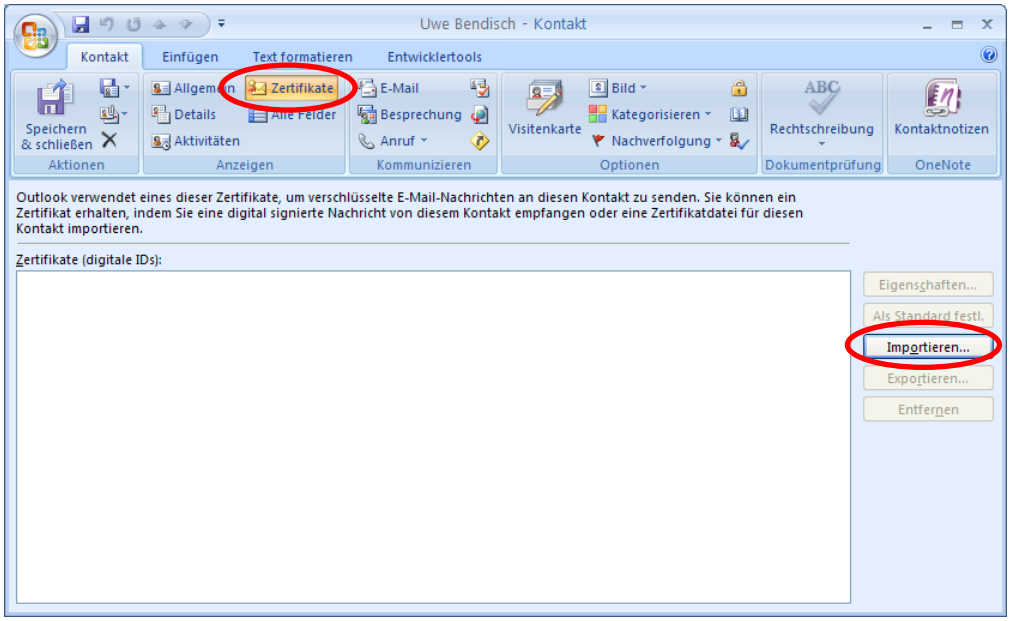


Abbildung 68: Importieren des Zertifikats des Fraunhofer Mitarbeiters in Outlook 2007

Wechseln Sie nun zu dem Verzeichnis, in dem Sie das Zertifikat des Fraunhofer Mitarbeiters abgelegt haben und wählen Sie das Zertifikat aus. Klicken Sie auf **Öffnen** (vgl. Abbildung 69).

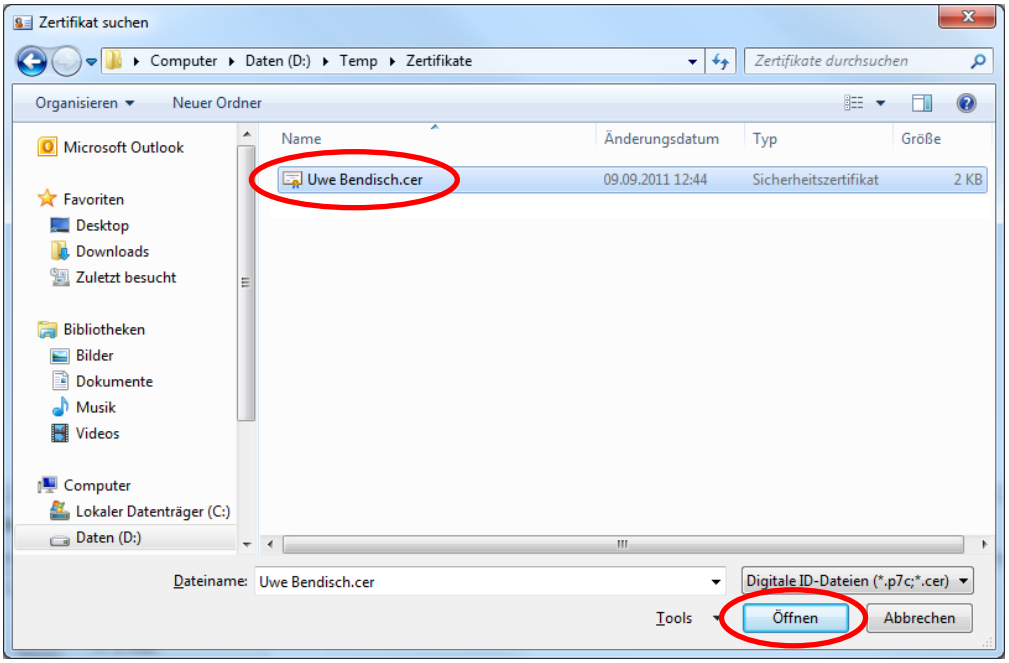


Abbildung 69: Auswahl des Zertifikats des Fraunhofer Mitarbeiters

Das Zertifikat ist nun dem Zertifikatspeicher hinzugefügt. Klicken Sie nun auf **Speichern & schließen** (vgl. Abbildung 70).

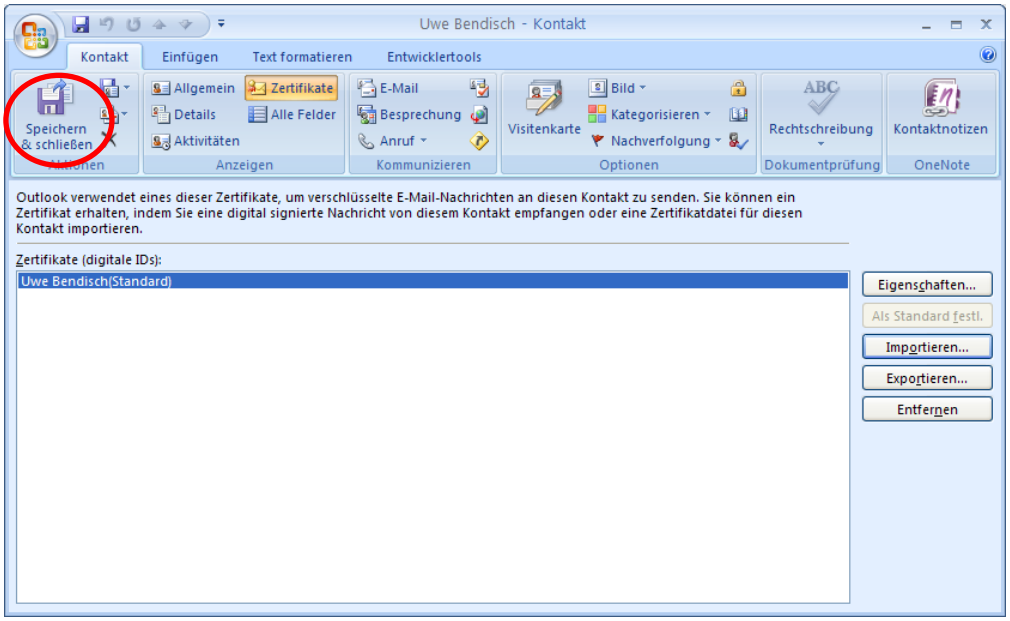


Abbildung 70: Speichern der Zertifikatszuordnung in Outlook 2007

Damit ist die Integration des Zertifikats des Fraunhofer Mitarbeiters in Outlook 2007 abgeschlossen und das Zertifikat kann für den sicheren E-Mail-Verkehr verwendet werden.

4.3.3 Ein Zertifikat eines Fraunhofer Mitarbeiters in Microsoft Outlook 2003 aufnehmen

Öffnen Sie zunächst eine neue E-Mail und geben Sie die E-Mail Adresse des Fraunhofer Mitarbeiters als Empfänger ein. Klicken Sie dann mit der rechten Maustaste auf die eingegebene E-Mail-Adresse und wählen Sie im Kontextmenü die Option **Zu Outlook-Kontakten hinzufügen** (vgl. Abbildung 71).

Hinweis: Ist der Fraunhofer Mitarbeiter bereits in Ihren Kontakten enthalten, so öffnen Sie dessen Kontaktdaten über den Kontextmenüeintrag **Outlook-Kontakt nachschlagen**.

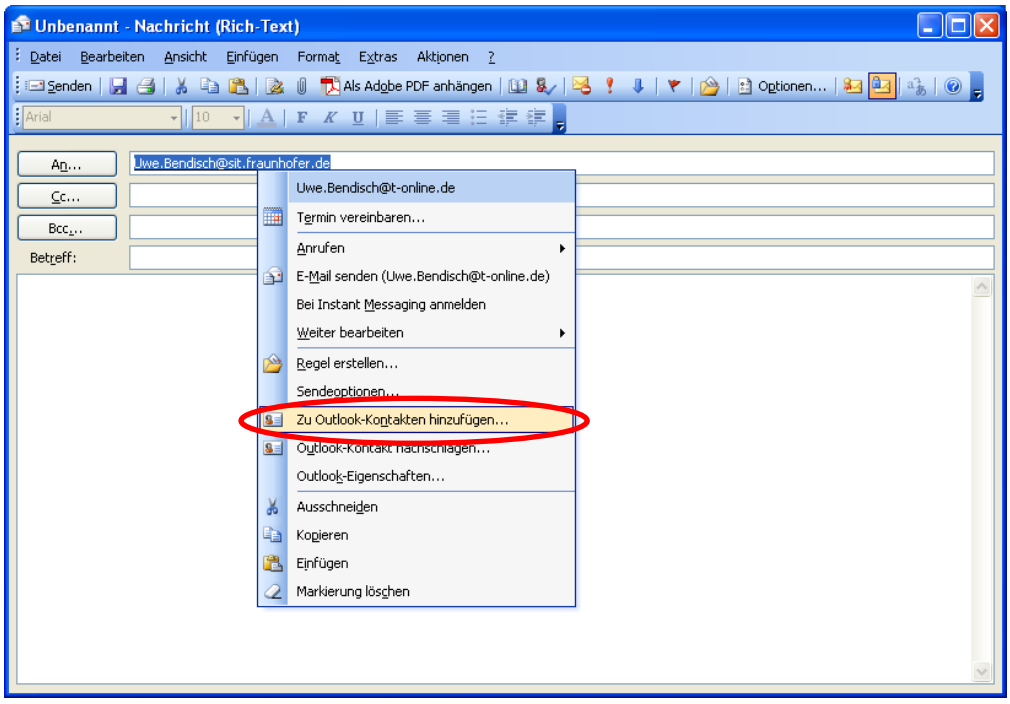


Abbildung 71: Hinzufügen eines Fraunhofer Mitarbeiters als Kontakt in Outlook 2003

Ihnen wird nun der Kontakteintrag angezeigt. Aktivieren Sie den Reiter **Zertifikate** und klicken Sie dann auf die Schaltfläche **Importieren** (vgl. Abbildung 72).

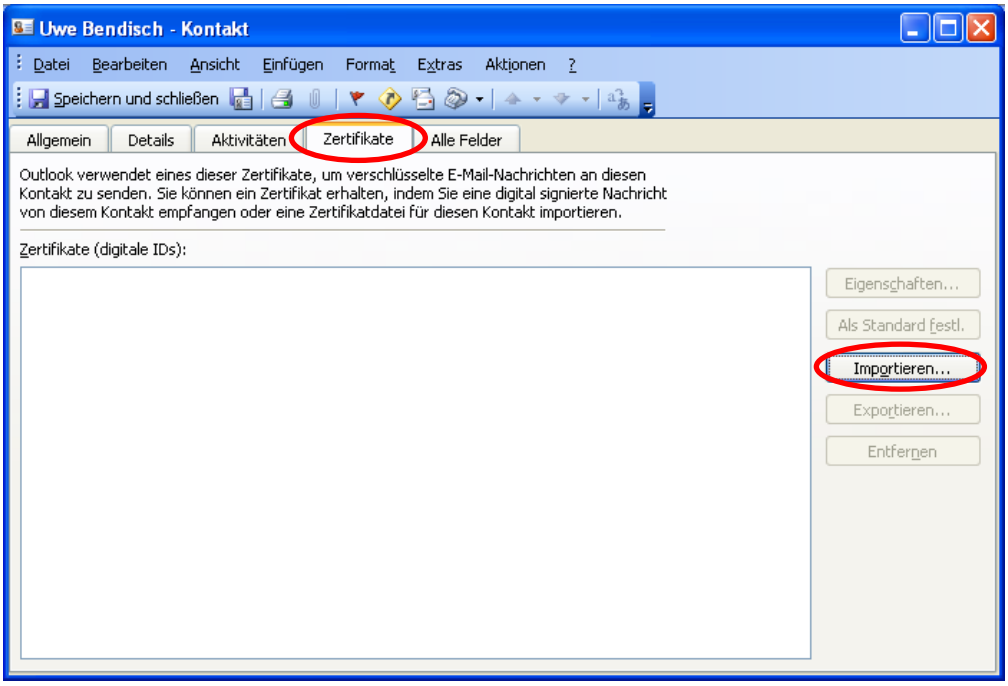


Abbildung 72: Importieren des Zertifikats des Fraunhofer Mitarbeiters in Outlook 2003

Wechseln Sie nun zu dem Verzeichnis, in dem Sie das Zertifikat des Fraunhofer Mitarbeiters abgelegt haben und wählen Sie das Zertifikat aus. Klicken Sie auf **Öffnen** (vgl. Abbildung 73).

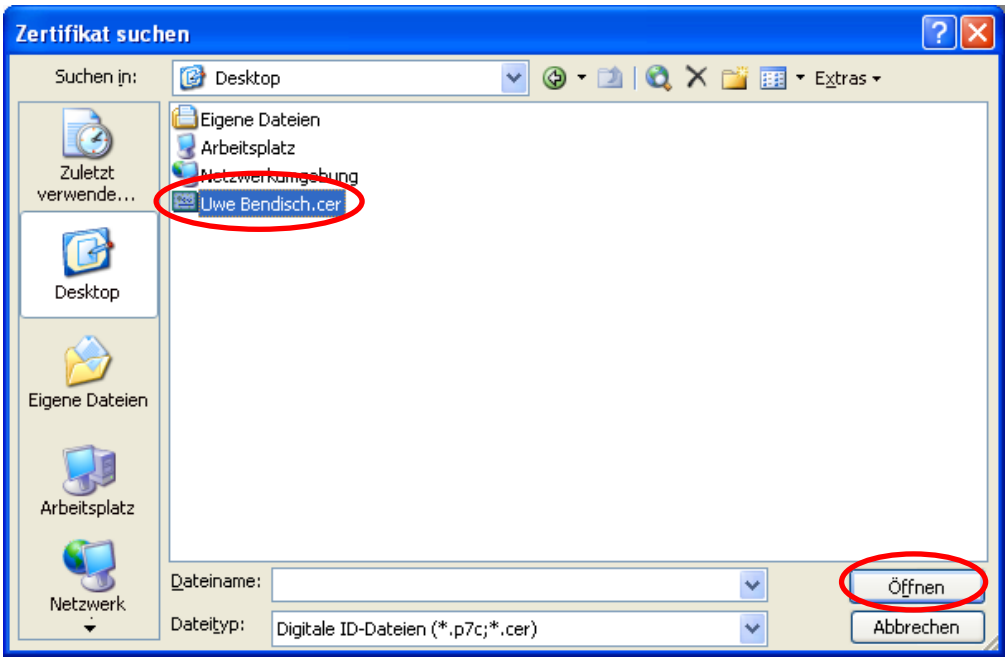


Abbildung 73: Auswahl des Zertifikats des Fraunhofer Mitarbeiters

Das Zertifikat ist nun dem Zertifikatspeicher hinzugefügt. Klicken Sie nun auf **Speichern & schließen** (vgl. Abbildung 74).

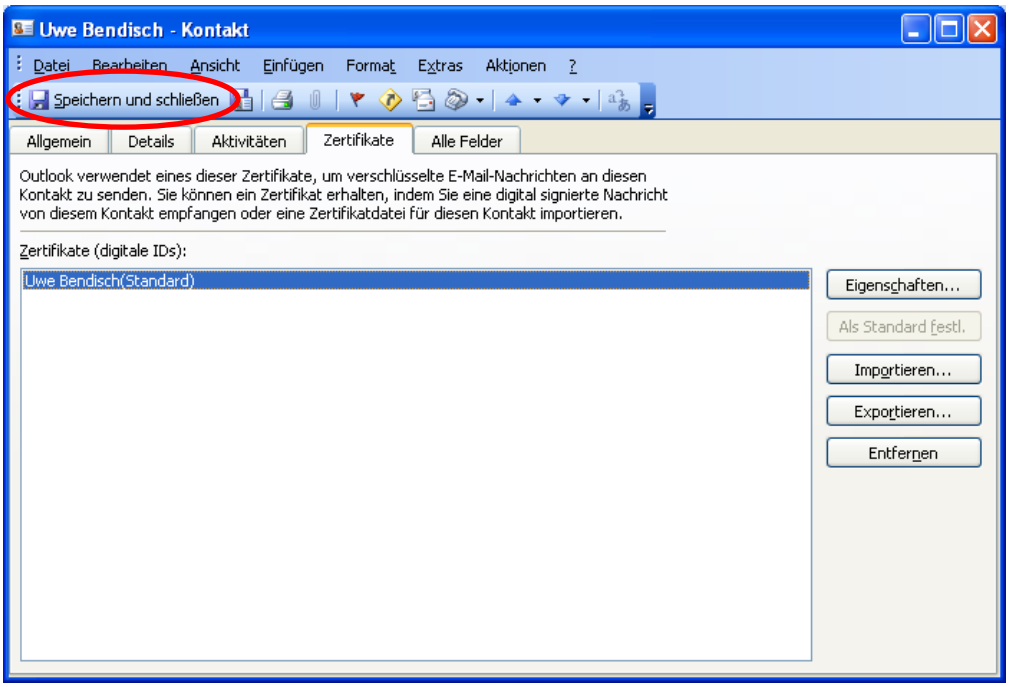


Abbildung 74: Speichern der Zertifikatszuordnung in Outlook 2003

Damit ist die Integration des Zertifikats des Fraunhofer Mitarbeiters in Outlook 2003 abgeschlossen und das Zertifikat kann für den sicheren E-Mail-Verkehr verwendet werden.

4.3.4 Ein Zertifikat eines Fraunhofer Mitarbeiters in Mozilla Thunderbird aufnehmen

Hinweis: Die Screenshots wurden unter Verwendung von Mozilla Thunderbird in der Version 9 angefertigt.

Um das Zertifikat des Fraunhofer Mitarbeiters in Mozilla Thunderbird einzubinden, öffnen Sie zunächst den Zertifikatspeicher, der sich unter **Extras → Einstellungen → Erweitert → Zertifikate → Zertifikate** befindet und öffnen dort den Reiter **Personen**. Klicken Sie auf die Schaltfläche **Importieren** (vgl. Abbildung 75).

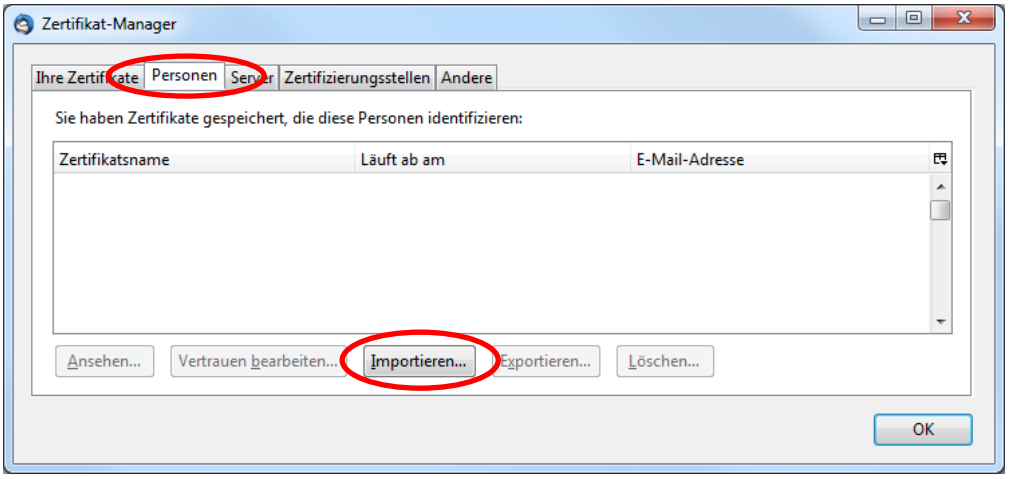


Abbildung 75: Importieren des Zertifikats des Fraunhofer Mitarbeiters in Mozilla Thunderbird

Wechseln Sie nun zu dem Verzeichnis, in dem Sie das Zertifikat des Fraunhofer Mitarbeiters abgelegt haben und wählen Sie das Zertifikat aus. Klicken Sie auf **Öffnen** (vgl. Abbildung 76).

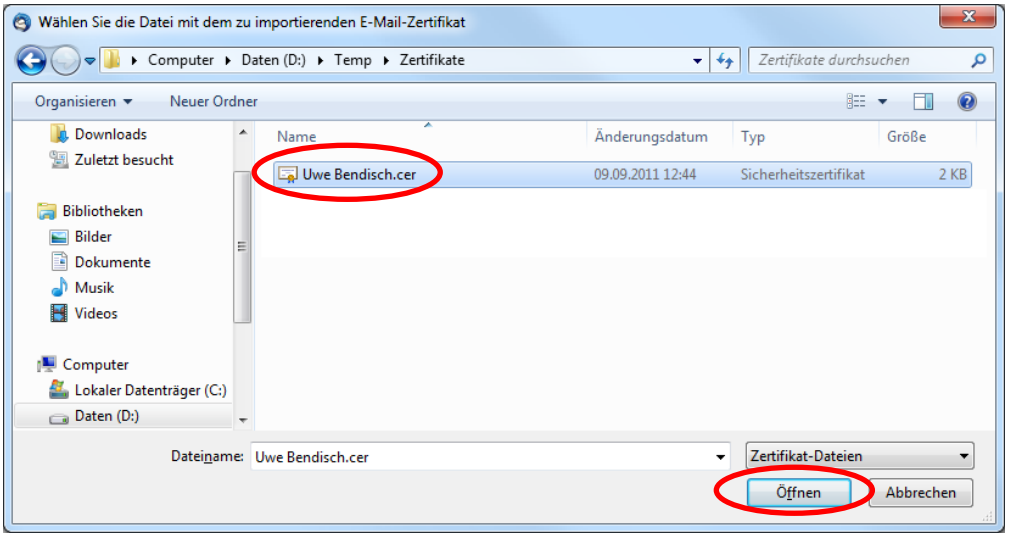


Abbildung 76: Auswahl des Zertifikats des Fraunhofer Mitarbeiters

Das Zertifikat ist nun dem Zertifikatspeicher hinzugefügt (vgl. Abbildung 77) und die Integration des Zertifikats des Fraunhofer Mitarbeiters in Thunderbird abgeschlossen. Schließen Sie den Zertifikat-Manager über die Schaltfläche **OK.** Das Zertifikat kann für damit den sicheren E-Mail-Verkehr verwendet werden.

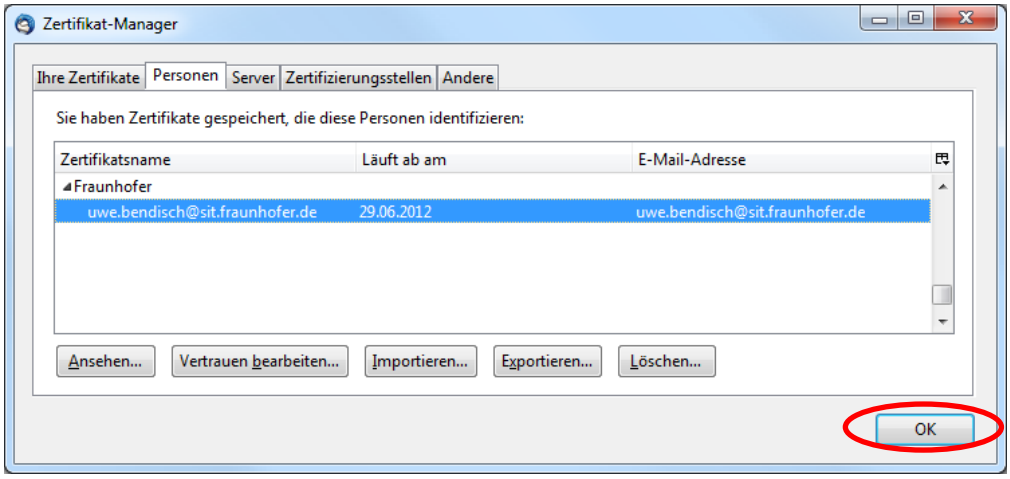


Abbildung 77: Thunderbird-Zertifikatspeicher mit dem Zertifikat des Fraunhofer Mitarbeiters.

4.4 Senden von signierten und/oder verschlüsselten E-Mails

Für das Versenden einer signierten E-Mail wird Ihr eigenes Zertifikat verwendet. Zertifikate der Empfänger werden nicht benötigt. Ihr E-Mail-Client berechnet aus dem Text Ihrer E-Mail eine Prüfsumme, die mit Hilfe Ihres Zertifikats mit einer digitalen Unterschrift versehen wird. Aufgrund der zugrundeliegende mathematischen Verfahren, kann dadurch beim Empfänger sowohl die Integrität (E-Mail wurde während der Übertragung nicht verändert) als auch die Authentizität des Absenders (die E-Mail stammt tatsächlich von Ihnen) geprüft werden.

Beim Versenden einer verschlüsselten E-Mail werden die Verschlüsselungszertifikate aller Empfänger benötigt. Mit Hilfe der Verschlüsselungszertifikate wird die Nachricht derart verschlüsselt, dass sie nur für den Besitzer des zum Verschlüsselungszertifikat gehörenden privaten Schlüssels lesbar ist. Sie garantieren damit Vertraulichkeit.

Aus dem oben Gesagten folgt, dass beim Versand einer signierten und verschlüsselten E-Mail sowohl Ihr eigenes Zertifikat (Zertifikat des Absenders) als auch die Zertifikate aller E-Mail Empfänger benötigt werden.

In Abhängigkeit von dem von Ihnen verwendeten E-Mail-Client unterscheiden sich die Dialoge bzw. Schritte zum Versenden signierter und/oder verschlüsselter E-Mails leicht, so dass das entsprechende Vorgehen in den folgenden Unterabschnitten für verschiedene Versionen von Microsoft Outlook als auch Mozilla Thunderbird beschrieben wird.

4.4.1 Senden von signierten und/oder verschlüsselten E-Mails mit Microsoft Outlook 2010

Erstellen Sie eine neue Nachricht. Beim Verfassen der Nachricht haben Sie auf dem Reiter **Optionen** die Möglichkeit die Nachricht zu signieren, indem Sie die Schaltfläche mit dem **Unterschriftsymbol** betätigen (vgl. Abbildung 78).

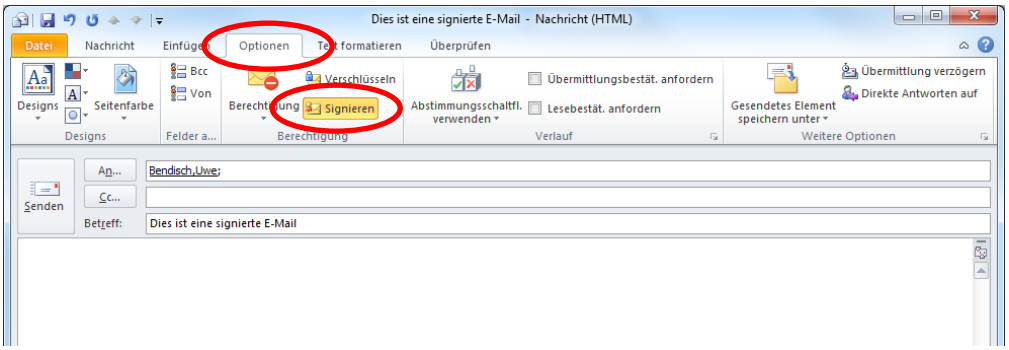


Abbildung 78: Signieren einer E-Mail in Outlook 2010

Zum Verschlüsseln einer E-Mail muss auf dem Reiter **Optionen** das **Symbol zur Verschlüsselung** aktiviert werden (vgl. Abbildung 79).

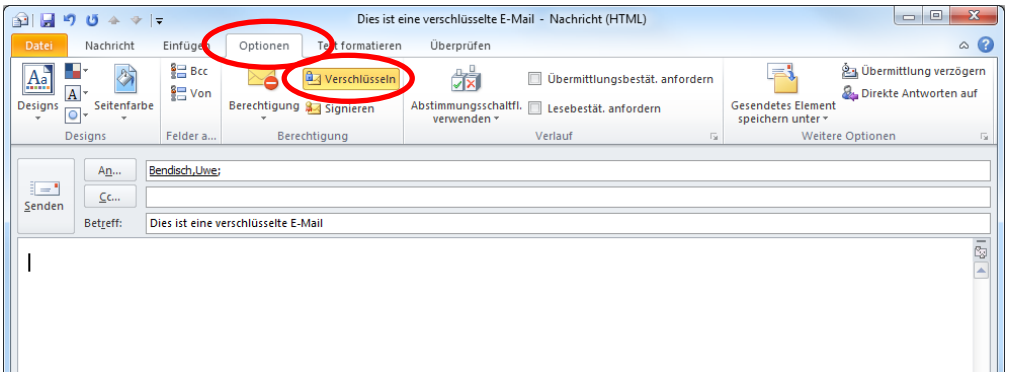


Abbildung 79: Verschlüsseln einer E-Mail in Outlook 2010

4.4.2 Senden von signierten und/oder verschlüsselten E-Mails mit Microsoft Outlook 2007

Erstellen Sie eine neue Nachricht. Beim Verfassen der Nachricht haben Sie auf dem Reiter **Nachricht** die Möglichkeit die Nachricht zu signieren, indem Sie die Schaltfläche mit dem **Unterschriftsymbol** im Bereich **Optionen** des Menübands betätigen (vgl. Abbildung 80).

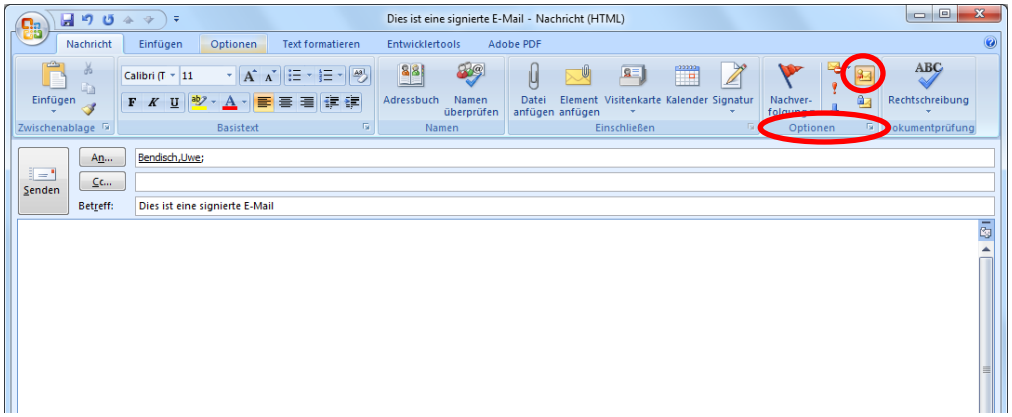


Abbildung 80: Signieren einer E-Mail in Outlook 2007

Zum Verschlüsseln einer E-Mail muss auf dem Reiter **Nachricht** im Bereich **Optionen** das **Symbol zur Verschlüsselung** aktiviert werden (vgl. Abbildung 81).

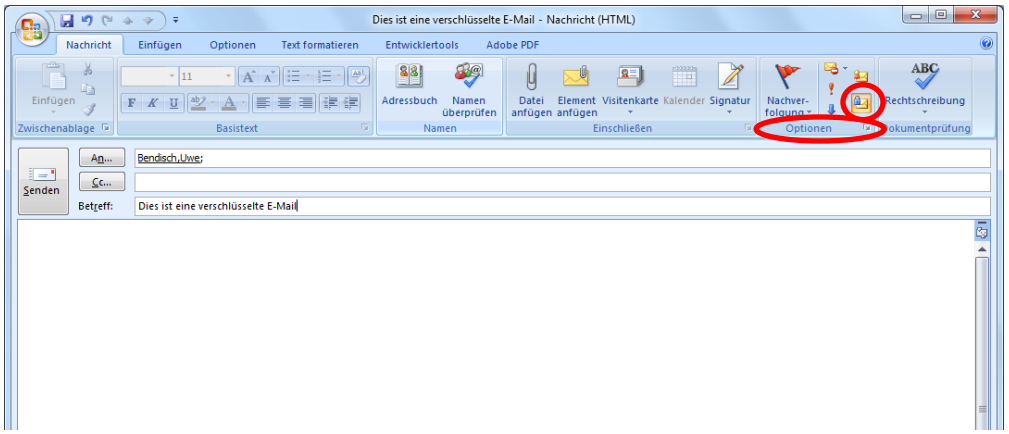


Abbildung 81: Verschlüsseln einer E-Mail in Outlook 2007

4.4.3 Senden von signierten und/oder verschlüsselten E-Mails mit Microsoft Outlook 2003

Erstellen Sie eine neue Nachricht. Beim Verfassen der Nachricht haben Sie die Möglichkeit die Nachricht zu signieren, indem Sie in den die Sicherheit der Nachricht betreffenden Eigenschaften, die Sie über **Datei → Eigenschaften** auf dem Reiter **Sicherheit** erreichen, die Option **Diese Nachricht digital signieren auswählen** (vgl. Abbildung 82).

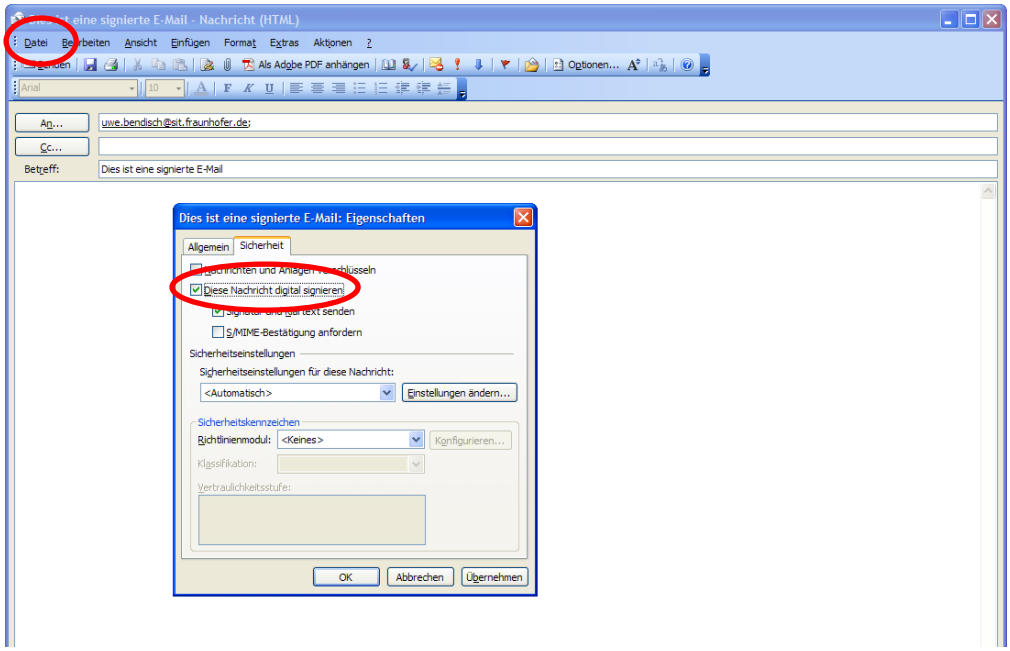


Abbildung 82: Signieren einer E-Mail in Outlook 2003

Zum Verschlüsseln einer E-Mail muss entsprechend die Option **Nachricht und Anlagen verschlüsseln** auf dem Reiter **Sicherheit** aktiviert werden, den Sie unter **Datei → Eigenschaften** der E-Mail-Nachricht erreichen (vgl. Abbildung 83).

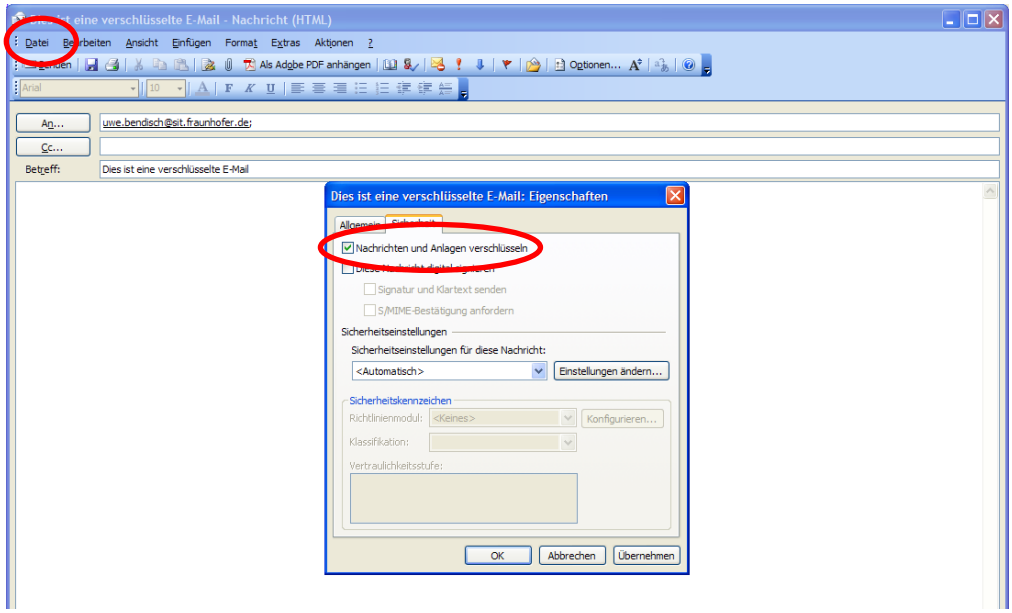


Abbildung 83: Verschlüsseln einer E-Mail in Outlook 2003

4.4.4 Senden von signierten und/oder verschlüsselten E-Mails mit Mozilla Thunderbird

Hinweis: Die Screenshots wurden unter Verwendung von Mozilla Thunderbird in der Version 9 angefertigt.

Erstellen Sie eine neue Nachricht. Beim Verfassen der Nachricht haben Sie im Menü der Nachricht in der Rubrik **S/MIME** die Möglichkeit die Nachricht zu signieren, indem Sie die Option **Nachricht unterschreiben** auswählen (vgl. Abbildung 84). Sie öffnen die S/MIME-Optionen, indem Sie auf den kleinen Pfeil neben dem Text klicken.

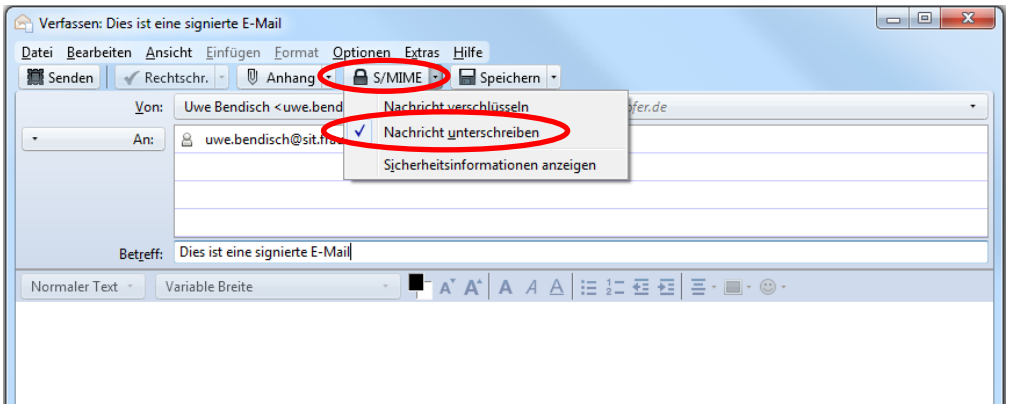


Abbildung 84: Signieren einer E-Mail in Mozilla Thunderbird

Zum Verschlüsseln einer E-Mail muss in der Rubrik **S/MIME** die Option **Nachricht verschlüsseln** angewählt werden (vgl. Abbildung 85).

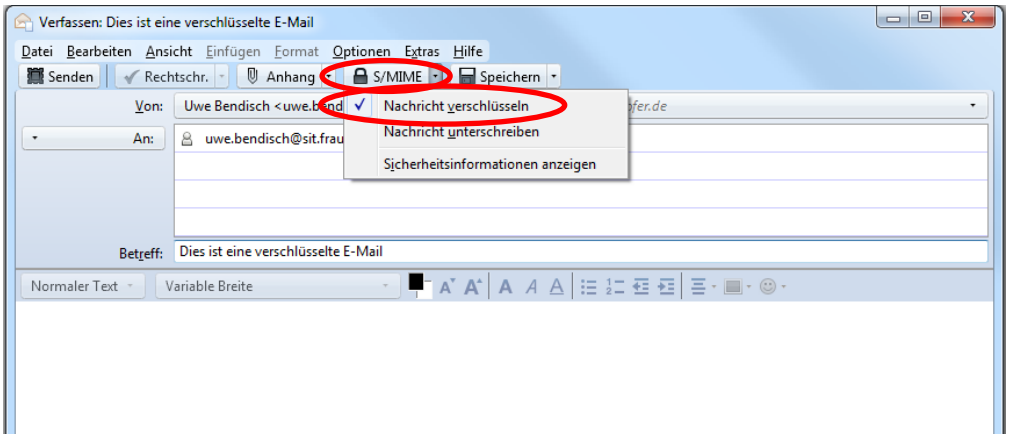


Abbildung 85: Verschlüsseln einer E-Mail in Mozilla Thunderbird

5 Ein eigenes Zertifikat sperren

Besitzen Sie bereits ein Zertifikat der Zertifizierungsstelle für Fraunhofer Kontakte und möchten es sperren, so können Sie unter https://contacts.pki.fraunhofer.de eine Sperrung veranlassen. Eine Sperrung ist beispielsweise erforderlich falls

- sich Ihre E-Mail-Adresse geändert hat oder ändern wird,
- Sie das Zertifikat nicht weiter zur Kommunikation im Fraunhofer-Kontext nutzen möchten,
- Sie die Nutzungsbedingungen der PKI für Fraunhofer Kontakte nicht länger akzeptieren bzw. Sie diese nicht mehr erfüllen, oder
- insbesondere falls ein Missbrauch oder eine Kompromittierung des privaten Schlüssels befürchtet wird oder tatsächlich stattgefunden hat.

Um zu vermeiden, dass eine dritte Person Ihr Zertifikat sperrt, ist der Sperrvorgang zweistufig ausgestaltet. Zunächst muss das zu sperrende Zertifikat identifiziert werden. Hierzu geben Sie bitte die im Zertifikat eingetragene E-Mail-Adresse an. An diese E-Mail-Adresse wird dann eine E-Mail versendet, die – ähnlich wie bei der Zertifikatsbeantragung – einen speziellen Link enthält. Mit diesem Link führen Sie die Sperrung des Zertifikats dann selbst durch.

5.1 Anforderung der Zertifikatssperrung eines eigenen Zertifikats per E-Mail

Rufen Sie bitte die Webseite https://contacts.pki.fraunhofer.de in Ihrem Browser auf und wählen Sie anschließend im Bereich **Für Kommunikationspartner** den Menüeintrag **Zertifikat sperren** (vgl. Abbildung 86).

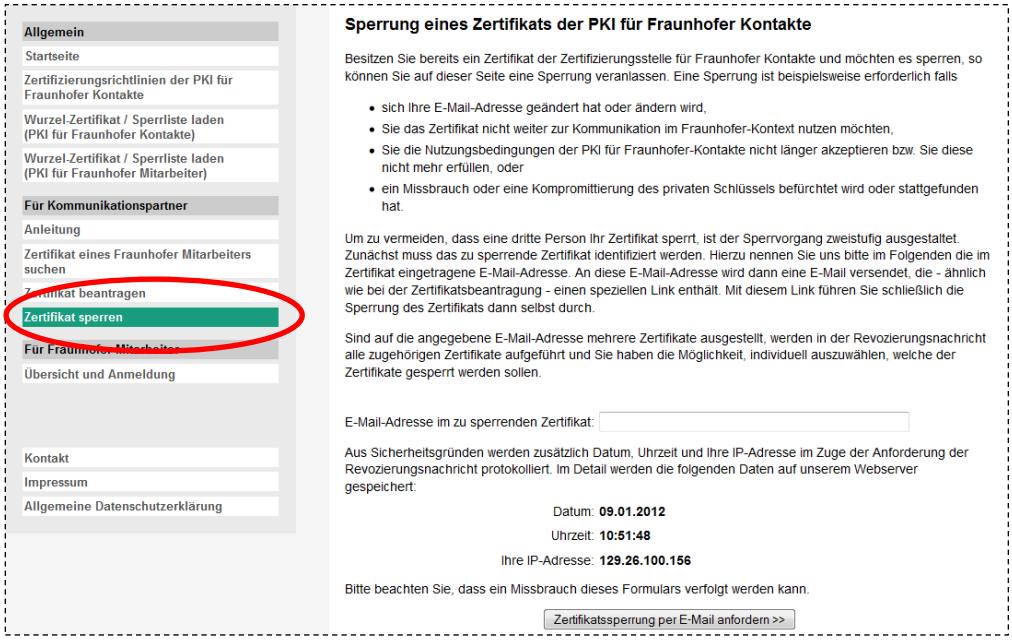


Abbildung 86: Anforderung einer Zertifikatssperrung

Geben Sie nun in das Feld **E-Mail-Adresse im zu sperrenden Zertifikat** diejenige E-Mail-Adresse ein, für die Ihr persönliches Zertifikat ausgestellt ist und betätigen Sie anschließend die Schaltfläche **Zertifikatssperrung per E-Mail anfordern**. Sofern für die E-Mail-Adresse ausgestellte und noch gültige Zertifikate vorhanden sind, erhalten Sie die Meldung, dass an die angegebene E-Mail-Adresse eine Liste aller zugehörigen gültigen Zertifikate – mit der Möglichkeit diese zu sperren – versendet wurde (vgl. Abbildung 87).

Abbildung 87: Erfolgreiche Anforderung einer Zertifikatssperrung

Andernfalls erfolgt ein Hinweis, dass keine E-Mail versendet wurde. Damit ist die Anforderung der Revozierungsnachricht abgeschlossen und Sie müssen für die eigentliche Zertifikatsperrung zunächst auf den Empfang der automatisch erzeugten Revozierungsnachricht warten, die nach kurzer Zeit bei Ihnen eintrifft (vgl. Abbildung 88).

Von: Fraunhofer-Gesellschaft
An: max.m.mustermann@t-online.de
Betreff: Link zur Sperrung eines Zertifikats (PKI für Fraunhofer Kontakte)
Datum: 09.01.2012, 15:40

Sehr geehrte Dame, sehr geehrter Herr,

diese E-Mail wurde nach einer Anforderung über die Website http://contacts.pki.fraunhofer.de/ automatisch erzeugt. Sie enthält eine Liste aller gültigen Zertifikate der PKI für Fraunhofer Kontakte für Ihre E-Mail-Adresse max.m.mustermann@t-online.de.

Falls ein Zertifikat aus dieser Liste nicht mehr benötigt wird oder um Missbrauch zu verhindern, kann es gesperrt werden. Wählen Sie hierzu bitte den entsprechenden Link, um auf unsere Website zu gelangen und dort das ausgewählte Zertifikat zu sperren.

Falls Sie kein Zertifikat sperren wollen, brauchen Sie nichts weiter zu unternehmen.

Liste der gültigen / aktiven Zertifikate für die E-Mail-Adresse max.m.mustermann@t-online.de:

- Zertifikat ausgestellt für Max Mustermann mit der Seriennummer 2744C33D000000000016,
gültig vom 12.09.2011 bis 11.09.2012. Dieses Zertifikat sperren:
https://contacts.pki.fraunhofer.de/default.asp?cancel=kUvBiXuInLxNIIFDfquiW152Eq3j&language=DE

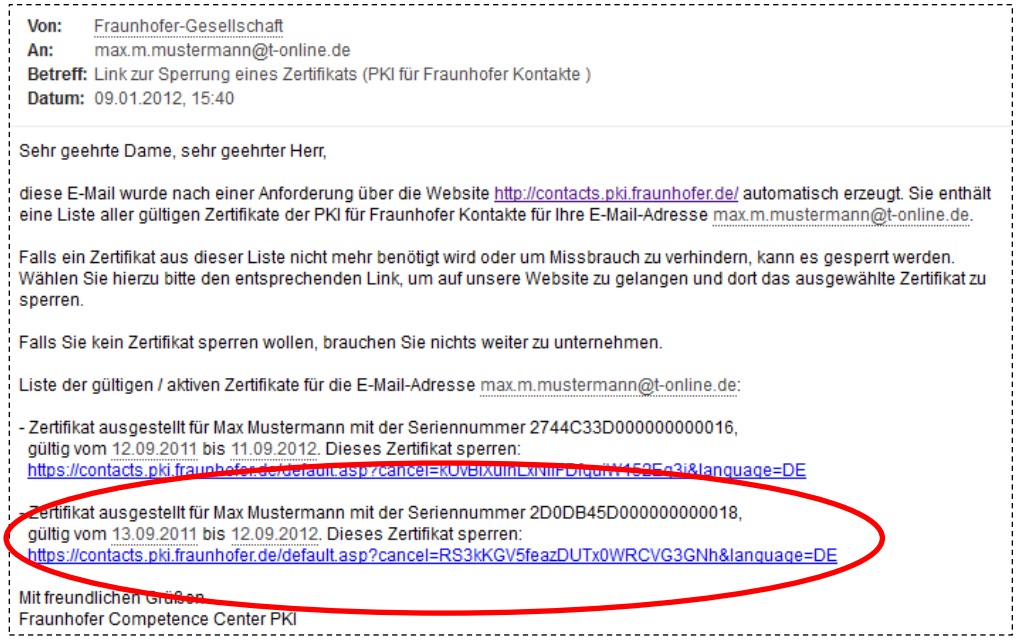
- Zertifikat ausgestellt für Max Mustermann mit der Seriennummer 2D0DB45D000000000018,
gültig vom 13.09.2011 bis 12.09.2012. Dieses Zertifikat sperren:
https://contacts.pki.fraunhofer.de/default.asp?cancel=RS3kKGV5feazDUTx0WRCVG3GNh&language=DE

Mit freundlichen Grüßen
Fraunhofer Competence Center PKI

Abbildung 88: Beispiel für eine Revozierungsnachricht zur Zertifikatssperrung

5.2 Ein eigenes Zertifikat mit Hilfe der Revozierungsnachricht endgültig sperren

Sind auf die angegebene E-Mail-Adresse mehrere Zertifikate ausgestellt, werden in der Revozierungsnachricht alle zugehörigen noch gültigen Zertifikate aufgeführt und Sie haben die Möglichkeit, individuell auszuwählen, welche der Zertifikate gesperrt werden sollen. Um ein in der E-Mail genanntes Zertifikat endgültig zu sperren, klicken Sie auf den betreffenden Link in der E-Mail oder kopieren Sie ihn in die Adressleiste Ihres Browsers (vgl. Abbildung 89).



Von: Fraunhofer-Gesellschaft
An: max.m.mustermann@t-online.de
Betreff: Link zur Sperrung eines Zertifikats (PKI für Fraunhofer Kontakte)
Datum: 09.01.2012, 15:40

Sehr geehrte Dame, sehr geehrter Herr,

diese E-Mail wurde nach einer Anforderung über die Website http://contacts.pki.fraunhofer.de/ automatisch erzeugt. Sie enthält eine Liste aller gültigen Zertifikate der PKI für Fraunhofer Kontakte für Ihre E-Mail-Adresse max.m.mustermann@t-online.de.

Falls ein Zertifikat aus dieser Liste nicht mehr benötigt wird oder um Missbrauch zu verhindern, kann es gesperrt werden. Wählen Sie hierzu bitte den entsprechenden Link, um auf unsere Website zu gelangen und dort das ausgewählte Zertifikat zu sperren.

Falls Sie kein Zertifikat sperren wollen, brauchen Sie nichts weiter zu unternehmen.

Liste der gültigen / aktiven Zertifikate für die E-Mail-Adresse max.m.mustermann@t-online.de:

- Zertifikat ausgestellt für Max Mustermann mit der Seriennummer 2744C33D000000000016,
gültig vom 12.09.2011 bis 11.09.2012. Dieses Zertifikat sperren:
https://contacts.pki.fraunhofer.de/default.asp?cancel=KUVBIXdlhLxNIIFDfqdW452Eq3j&language=DE

- Zertifikat ausgestellt für Max Mustermann mit der Seriennummer 2D0DB45D000000000018,
gültig vom 13.09.2011 bis 12.09.2012. Dieses Zertifikat sperren:
https://contacts.pki.fraunhofer.de/default.asp?cancel=RS3kKGV5feazDUTx0WRCVG3GNh&language=DE

Mit freundlichen Grüßen
Fraunhofer Competence Center PKI

Abbildung 89: Auswahl eines zu sperrenden Zertifikats in der Revozierungsnachricht zur Zertifikatssperrung

Der Link leitet Sie auf eine spezielle Webseite der *PKI-Contacts*, die Sie durch die Zertifikatssperrung führt (vgl. Abbildung 90). Lesen Sie den Text auf Webseite genau und machen Sie sich insbesondere bewusst, dass

- Sie unabhängig von einer Sperrung Ihren zum Zertifikat gehörender privaten Schlüssel **nicht** vernichten sollten, da Sie ansonsten insbesondere an Sie mit diesem Zertifikat verschlüsselte E-Mails nicht mehr lesen, d. h. entschlüsseln können. Sie sollten deshalb ggfs. eine Sicherung Ihres Zertifikats einschließlich des privaten Schlüssels an einem sicheren Ort (z. B. auf einem externen Datenträger) aufbewahren. Alternativ sind das Zertifikat und der private Schlüssel auch noch im Zertifikatspeicher des Browsers vorhanden, mit dem Sie ursprünglich die Zertifikatsbeantragung durchgeführt haben. Aus diesem können Sie es wie in Kapitel 3 beschrieben, exportieren.

- eine Sperrung nicht rückgängig gemacht werden kann. Sollten Sie nach der Sperrung feststellen, dass Sie doch wieder ein Zertifikat benötigen, müssen Sie ein neues (anderes) Zertifikat beantragen.

Um das angezeigte Zertifikat zu sperren, selektieren Sie bitte anschließend die Auswahlbox vor dem ausgewählten Zertifikatseintrag und betätigen Sie die Schaltfläche **Zertifikat sperren** (vgl. Abbildung 90).

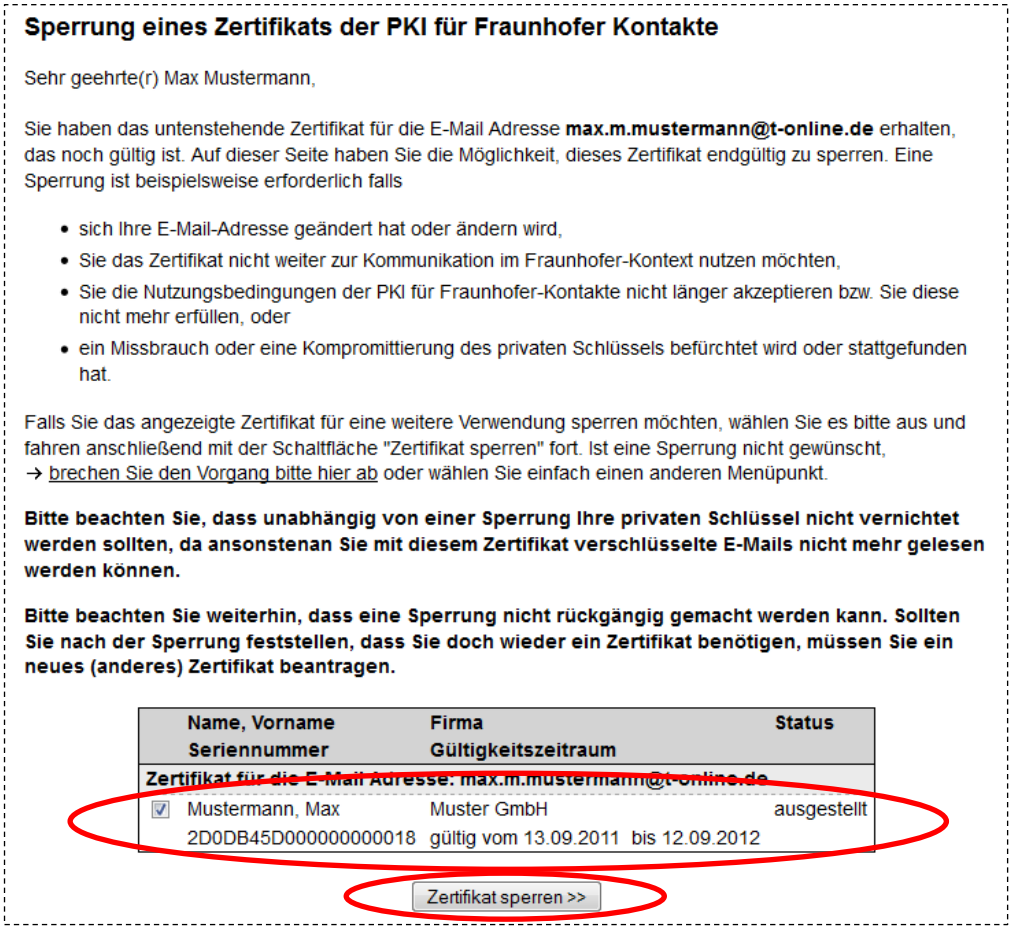


Abbildung 90: Bestätigung der Auswahl eines zu sperrenden Zertifikats

Sie erhalten nun die Meldung, dass die Sperrung durchgeführt wurde und in Kürze eine neue Sperrliste veröffentlicht wird (vgl. Abbildung 91). Außerdem werden Sie über die vorgenommene Sperrung nochmals automatisch per E-Mail unterrichtet (vgl. Abbildung 92). Der Sperrvorgang ist damit erfolgreich abgeschlossen.

Hinweis: Die Sperrliste, auf der sich die Seriennummer des gesperrten Zertifikats befindet, steht spätestens dreißig Minuten nach einer erfolgreich durchgeführten Sperrung auf der Website der PKI für Fraunhofer Kontakte zur Verfügung.

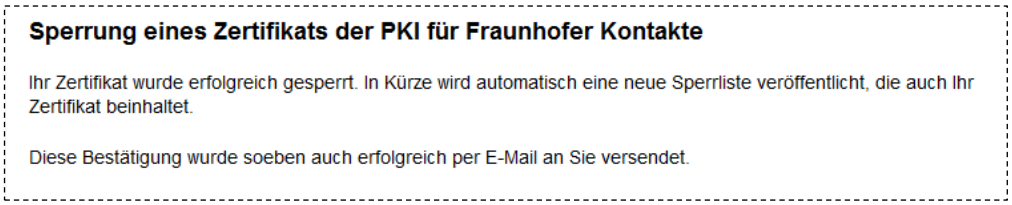
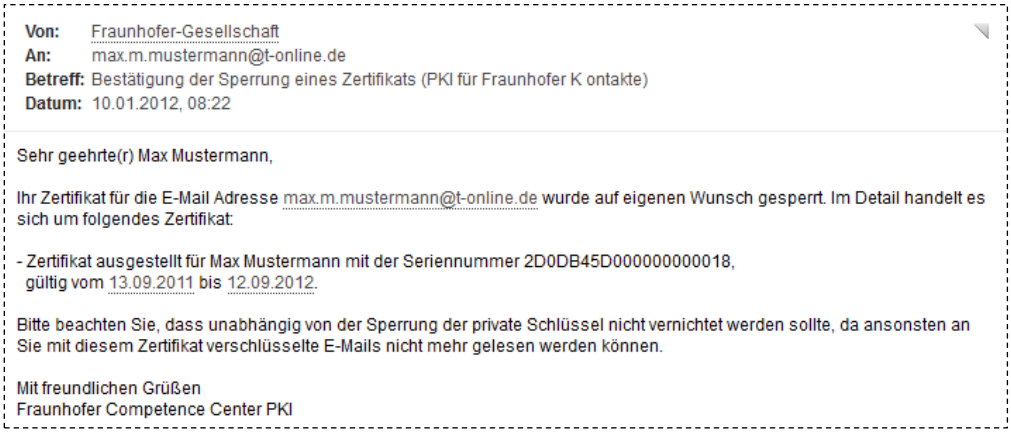


Abbildung 91: Bestätigung der Sperrung Ihres eigenen Zertifikats



Von: Fraunhofer-Gesellschaft
An: max.m.mustermann@t-online.de
Betreff: Bestätigung der Sperrung eines Zertifikats (PKI für Fraunhofer K ontakte)
Datum: 10.01.2012, 08:22

Sehr geehrte(r) Max Mustermann,

Ihr Zertifikat für die E-Mail Adresse max.m.mustermann@t-online.de wurde auf eigenen Wunsch gesperrt. Im Detail handelt es sich um folgendes Zertifikat:

- Zertifikat ausgestellt für Max Mustermann mit der Seriennummer 2D0DB45D000000000018,
  gültig vom 13.09.2011 bis 12.09.2012.

Bitte beachten Sie, dass unabhängig von der Sperrung der private Schlüssel nicht vernichtet werden sollte, da ansonsten an Sie mit diesem Zertifikat verschlüsselte E-Mails nicht mehr gelesen werden können.

Mit freundlichen Grüßen
Fraunhofer Competence Center PKI

Abbildung 92: E-Mail-Bestätigung der Sperrung Ihres eigenen Zertifikats