INSTITUT FÜR IT-SERVICE service

Inhalt

Die Verschlüsselung von E-Mails wird im folgenden Dokument anschaulich erklärt und gewährleistet die Vertraulichkeit der übertragenen Daten. Die Verschlüsselung stellt sicher, dass die Daten tatsächlich nur von Ihrem vorgesehenen Kommunikationspartnern eingesehen und gelesen werden können.

Hierzu benötigen Sie ein E-Mail-Programm (z.B. Microsoft Outlook, Mozilla Thunderbird etc.), dass die S/MIME basierte E-Mail-Verschlüsselung unterstützt. Um verschlüsselte E-Mails senden oder empfangen zu können, benötigen Sie selbst ein Zertifikat welches Ihr zugehörige Schlüsselmaterial enthält. Dieses Zertifikat kann bei uns an der Hochschule Bonn-Rhein-Sieg erworben uns werden, da die H-BRS eine vom DFN-Verein autorisierte Zertifizierungsstelle ist.

Wichtige Links:

Beantragung des Nutzerzertifikats: https://pki.pca.dfn.de/hs-bonn-rhein-sieg-ca-g2/pub/

Informationswebsite: https://www.h-brs.de/de/digitale-signatur-und-verschluesselung

FAQ: https://www.h-brs.de/de/faq-digitale-signatur-und-verschluesselung

Information für Zertifikatinhaber: https://www.pki.dfn.de/fileadmin/PKI/Info_Zertifikatinhaber.pdf

Video Tutorial:

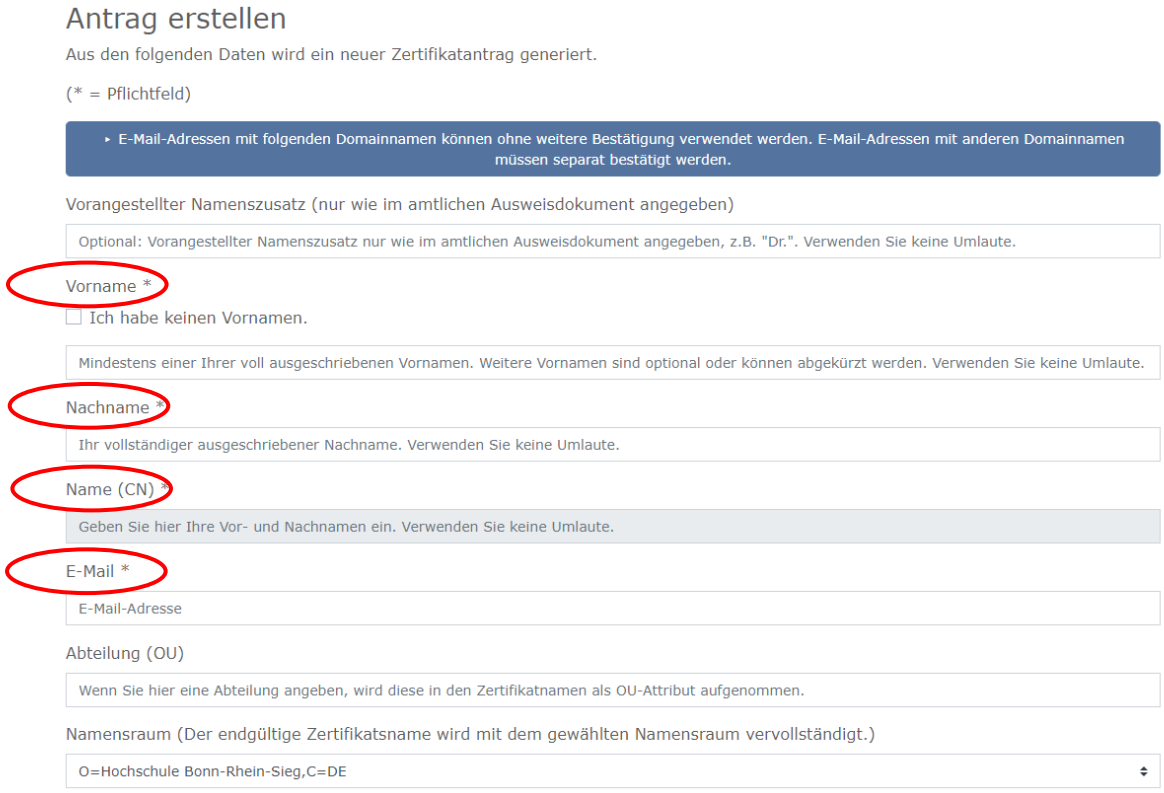
1 Beantragen eines personenbezogenen Nutzerzertifikats

Öffnen Sie bitte folgenden Link, um das Nutzerzertifikat zu beantragen:

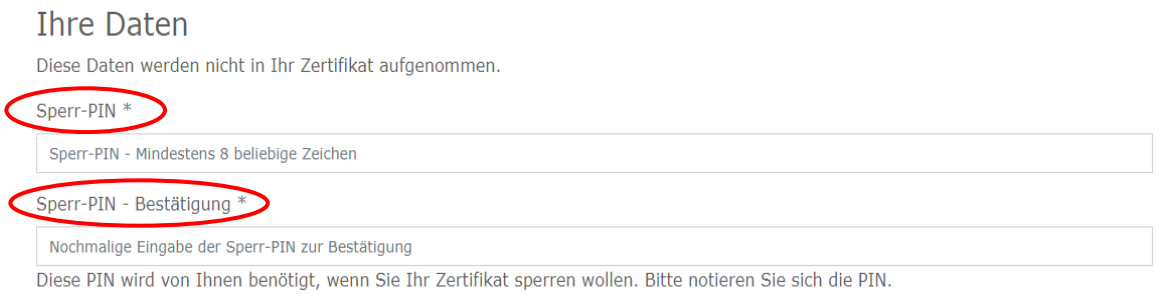
https://pki.pca.dfn.de/hs-bonn-rhein-sieg-ca-g2/pub/

Schritt 1: Klicken Sie bitte auf **„Nutzerzertifikat“**.

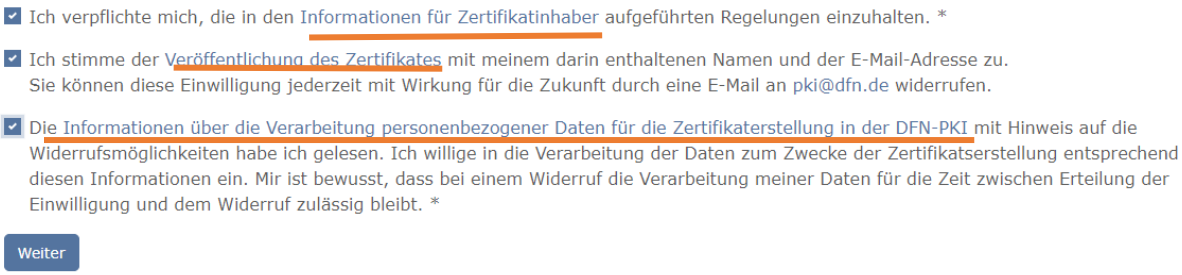
Schritt 2: Füllen Sie bitte nun die Pflichtfelder aus.



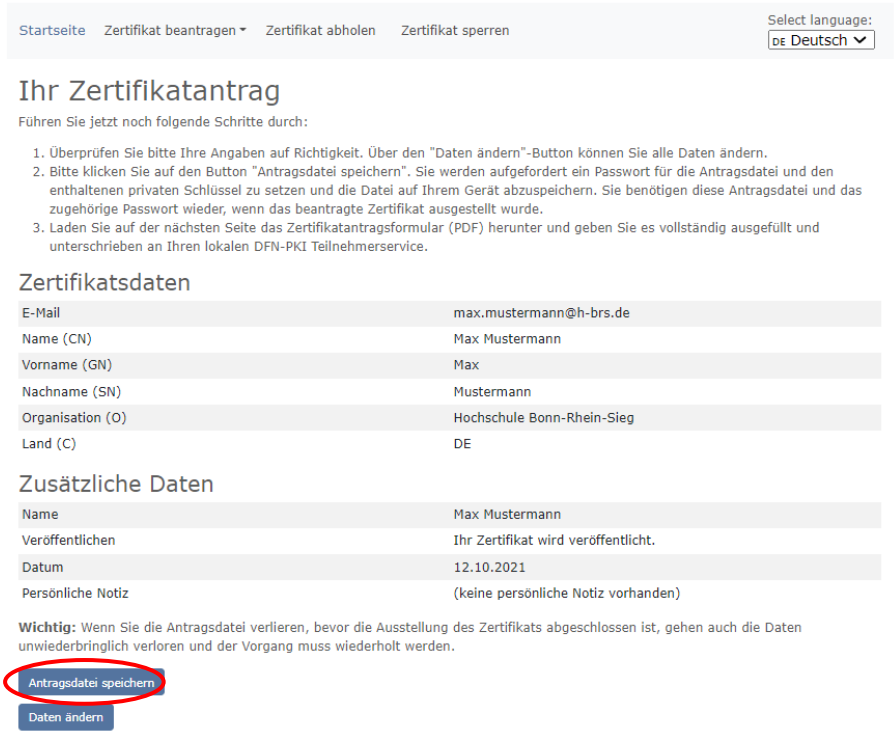
Schritt 3: Bitte wählen Sie eine 8-stellige Pin bestehend aus beliebigen Zeichen aus. Mit der PIN können Sie ihr Zertifikat entsperren und im Falle des Verlustes sperren lassen.



Schritt 4: Lesen Sie sich nun bitte die Informationen zu: „Informationen für Zertifikatinhaber", „Veröffentlichung des Zertifikates" und „Die Information über die Verarbeitung personenbezogener Daten für Zertifikaterstellung in der DFN-PKI" durch und stimmen Sie zu. Im nächsten Schritt auf „weiter" klicken.

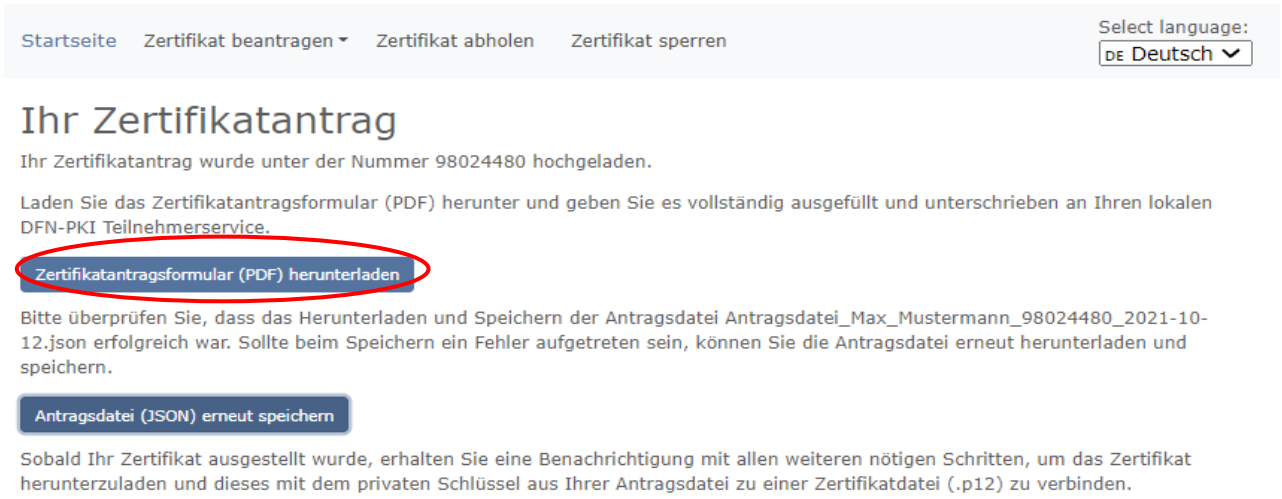


Schritt 5: Überprüfen Sie Ihre Angaben auf Richtigkeit – bei Änderungen klicken Sie auf „Daten ändern". Sollten die Angaben soweit richtig sein klicken Sie auf **„Antragsdatei speichern"**.



Schritt 6: Erstellen Sie ein Passwort für die Antragsdatei (inkl. Privaten Schlüssel) aus mindestens 8 Zeichen. Bitte heben Sie ihr Passwort gut auf!

Schritt 7: Drucken Sie das Zertifikatsantragsformular aus. Überprüfen Sie Ihre Angaben erneut auf Richtigkeit. Nach der Überprüfung unterschreiben Sie den Antrag mit Orts- und Datumsangabe. Des Weiteren können Sie hier auch die Antragsdatei als JSON erneut speichern. Bitte vergewissern Sie sich, dass Sie die Antragsdatei gesichert haben für die spätere Herunterladung des Zertifikats.



2 Verifizierung beim Teilnehmerservice

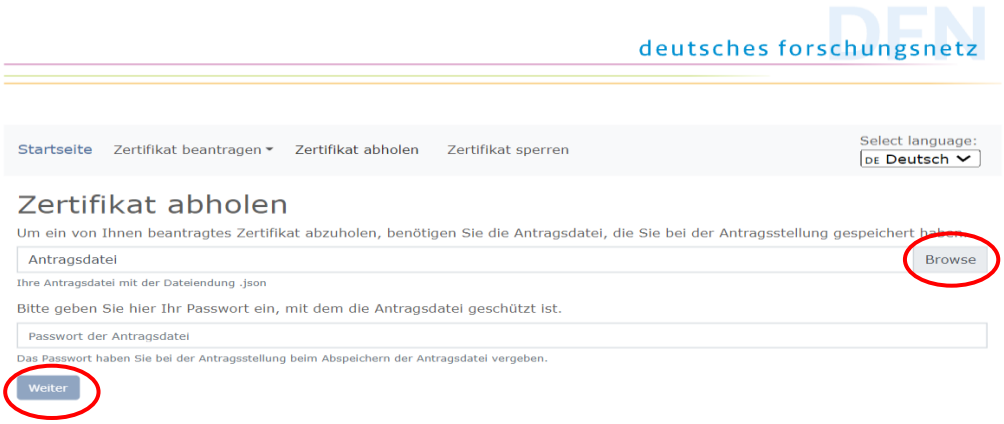
Schritt 8: Für die erfolgreiche Beantragung eines Zertifikates ist die Verifizierung beim Teilnehmerservice (TS) erforderlich. Dem TS gehören folgende Personen an: Herr Muntz, Herr Schleicher, Herr Dreyer und Frau Lewandowski.

WICHTIG!

- **Denken Sie an Ihren Personalausweis!** Dieser wird benötigt, damit der TS Ihre Identität bestätigen kann, um das Zertifikat final zu beantragen.
- **Denken Sie an das unterschriebene Antragsformular**
- Die Verifizierung beim TS dauert i.d.R. max. 5 min. Bitte erscheinen Sie pünktlich zu Ihrem Termin, um einen reibungslosen Ablauf zu gewährleisten.

3 Abholung des Zertifikats

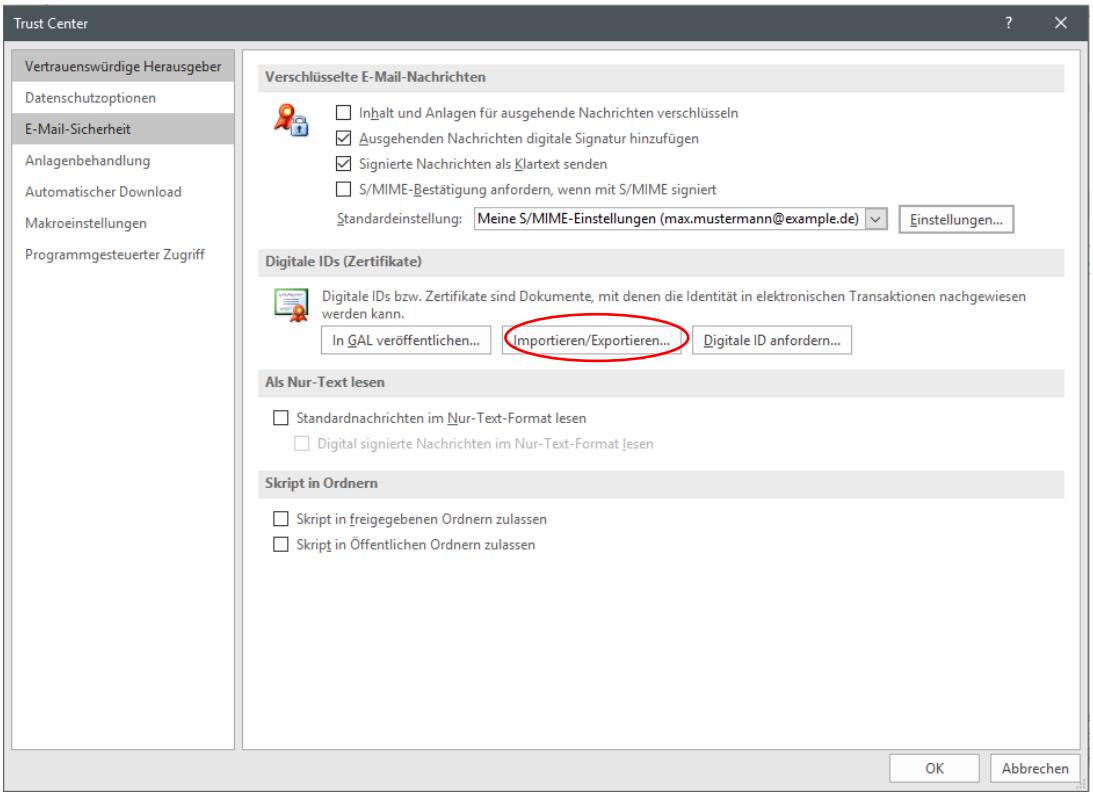
Schritt 9: Nach der Verifizierung können Sie Ihr Zertifikat beim DFN abholen. Sie erhalten nach erfolgreicher Verifizierung eine E-Mail vom DFN mit einem persönlichen Downloadlink für Ihr Zertifikat. Folgen Sie dem Link und laden Sie die JSON Antragsdatei hoch, die Sie nach der initialen Beantragung herunterladen konnten. Des Weiteren geben Sie ihr Passwort der Antragsdatei ein. Klicken Sie dann auf „weiter“ und laden Sie Ihre Zertifikatsdatei als .p12 Datei herunter.



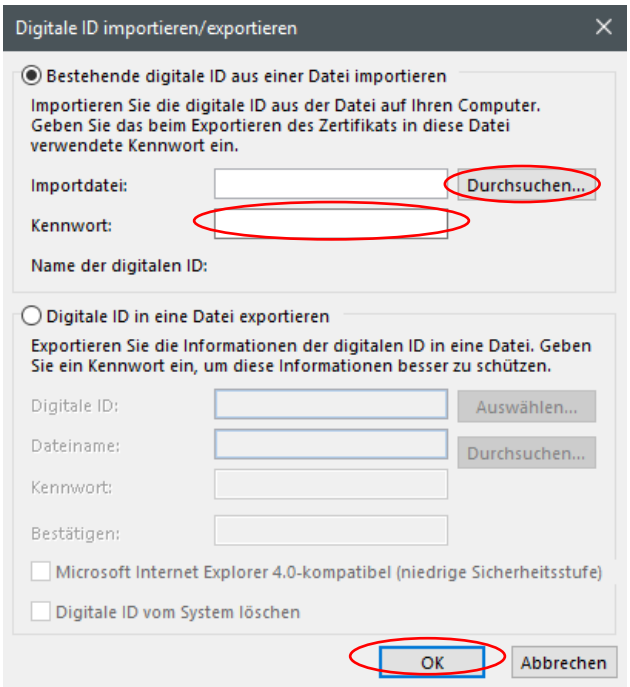
4 Verschlüsselung mit Outlook konfigurieren

Um mit Outlook verschlüsselte E-Mails zu verschicken, müssen zuvor noch einige Einstellungen angepasst werden. Dies geschieht in den Einstellungen des Trust Centers von Outlook.

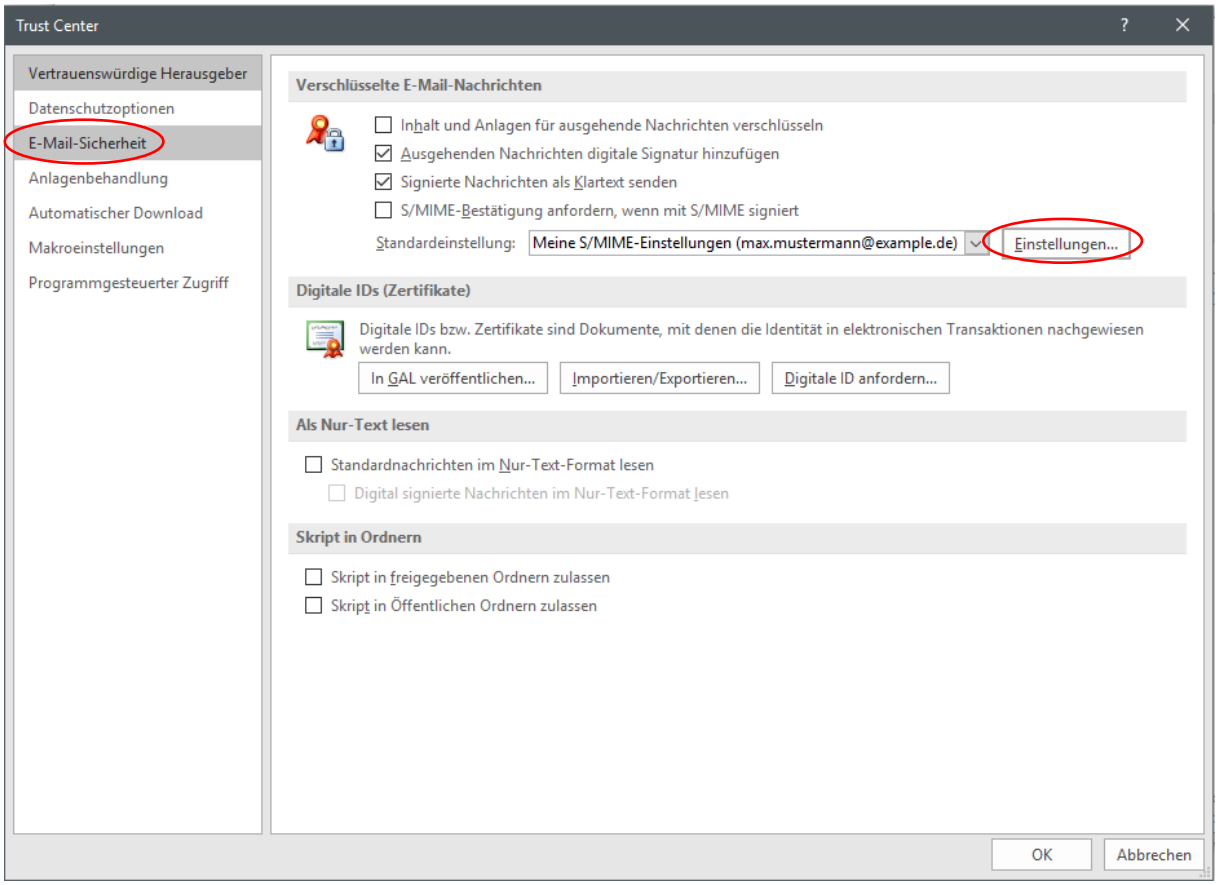
1. Klickten Sie in Outlook in der oberen Leiste auf Datei -> Optionen -> Trust Center -> Einstellungen für das Trust Center
2. Klicken Sie nun auf den Eintrag „E-Mail-Sicherheit“ links in der Leiste.
3. Klicken Sie auf Importieren/Exportieren



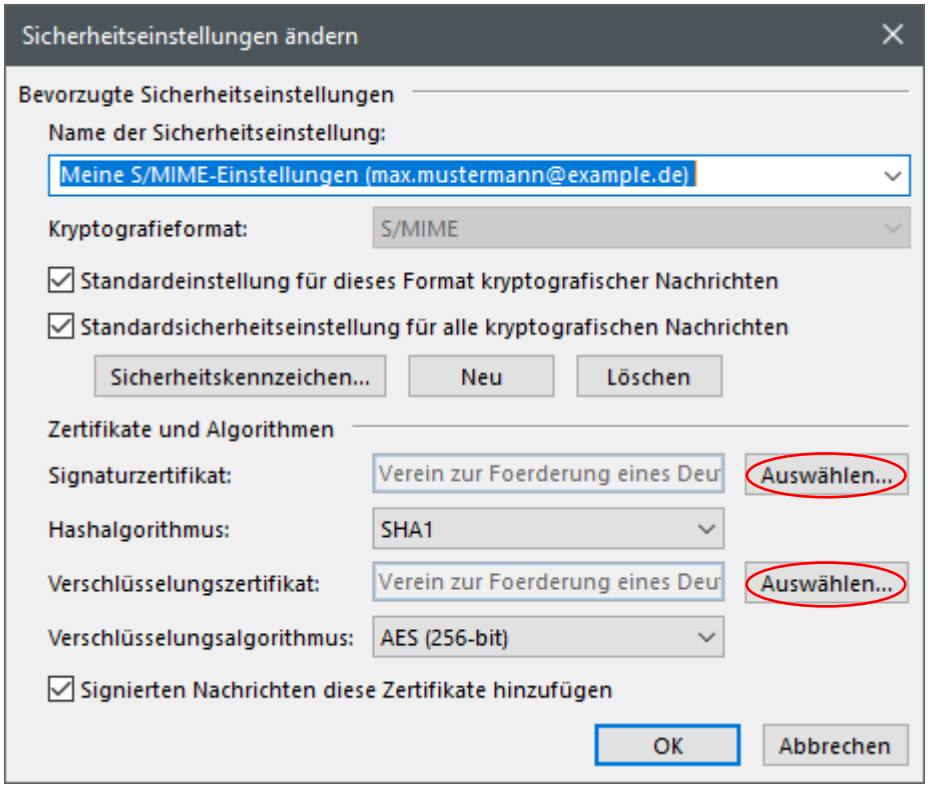
4. Wählen Sie dort nun über einen Klick auf „Durchsuchen“ Ihr eben exportiertet Zertifikat aus. Geben Sie nun im Feld darunter Ihr eben gewähltes Backup-Passwort ein und klicken zuletzt auf „Ok“.



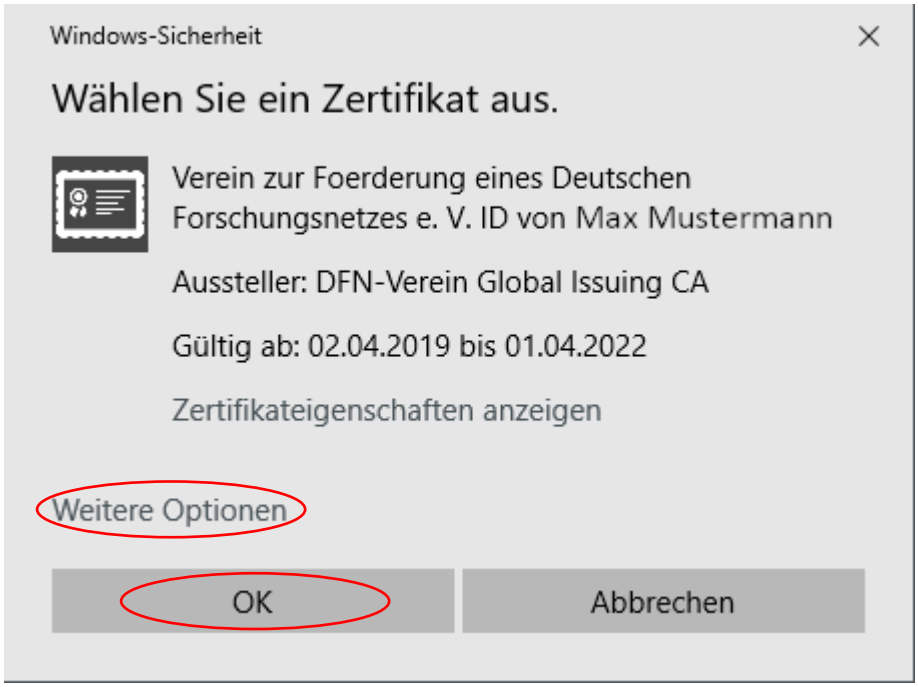
5. Klicken Sie nun auf den Button „Einstellungen“



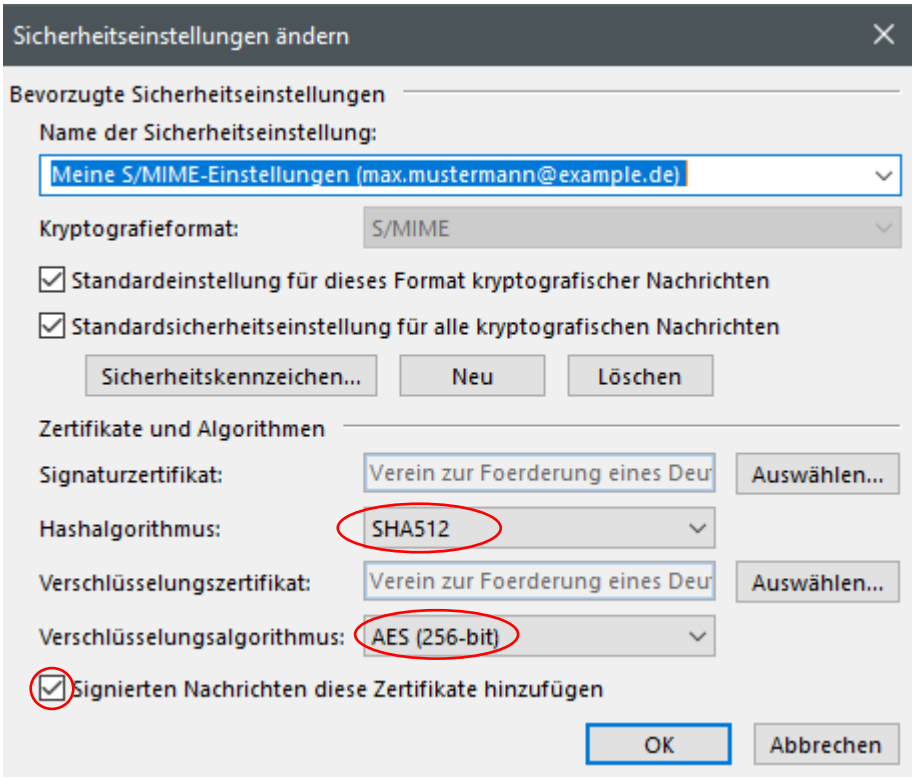
6. Klicken Sie nun bitte jeweils einmal bei „Signaturzertifikat“ und bei „Verschlüsselungszertifikat“ auf „Auswählen“ und wählen Sie ihr Zertifikat in Schritt 7.



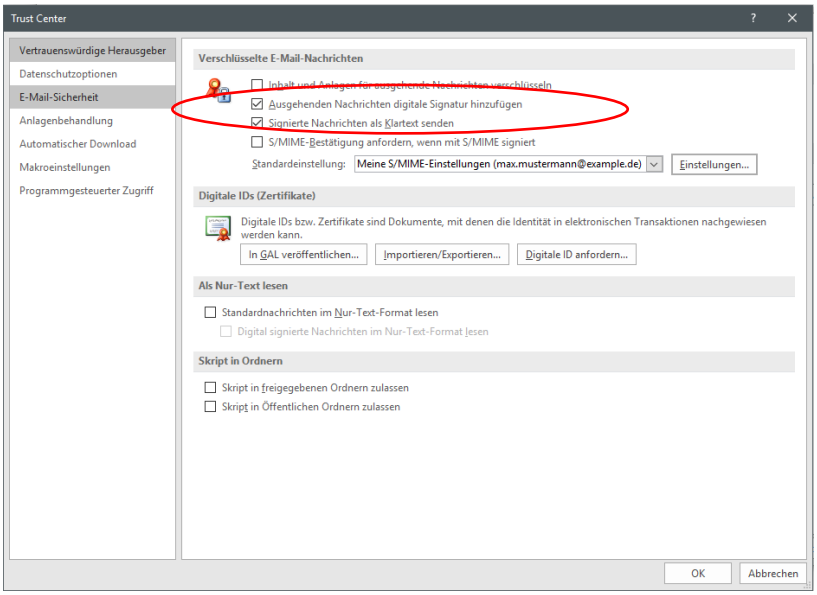
7. Klicken Sie nun auf „Ok“, wenn Ihnen Ihr Zertifikat mit dem Aussteller „DFN-Verein Global Issuing CA“ angezeigt wird und „Verein zur Foerderung eines Deutschen Forschungsnetzes e. V. ID von …“ heißt. Sollte das nicht der Fall sein, dann klicken Sie bitte auf „Weitere Optionen“ um es auswählen zu können.



8. Wählen Sie nun bitte als Hashalgorithmus den „SHA256“ oder den „SHA512“ und als Verschlüsselungsalgorithmus den „AES (256-bit)“ aus. Setzen Sie zudem einen Haken bei „Signierte Nachrichten diese Zertifikate hinzufügen“. Klicken Sie dann auf „Ok“.



9. Um E-Mails standardgemäß gegen Manipulation zu schützen sollte die Option „Ausgehenden Nachrichten digitale Signaturen hinzufügen“ eingeschaltet werden. Klicken Sie anschließend auf „Ok“.

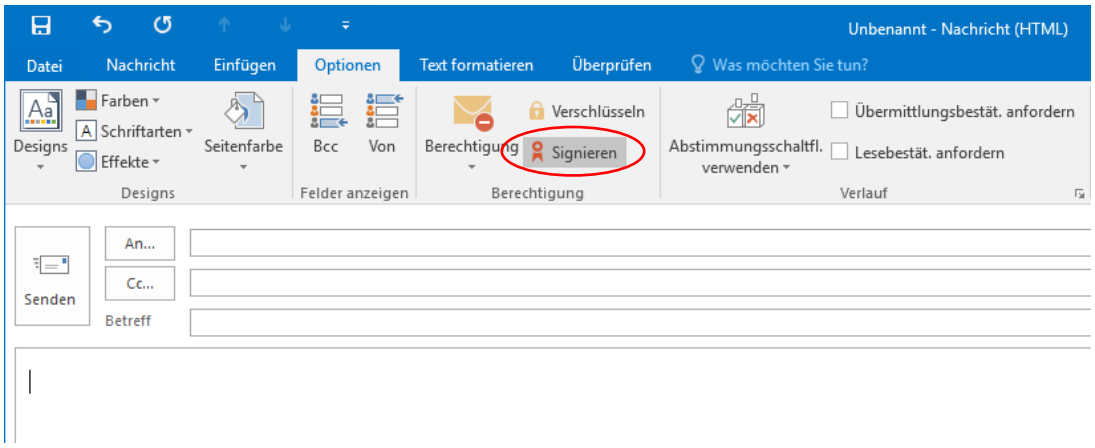


6 Signieren von E-Mails

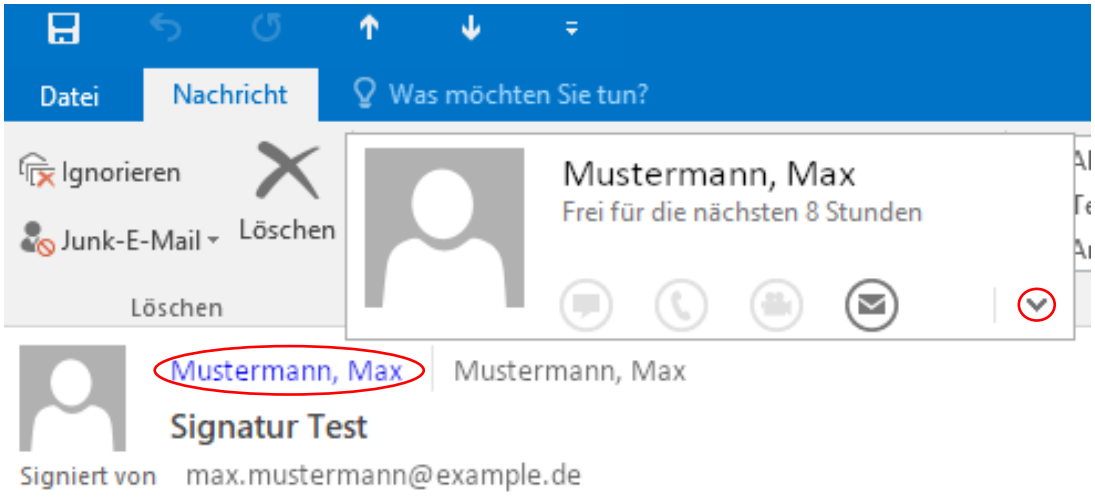
Nun sind beinahe alle Vorbereitungen abgeschlossen, um mit Outlook verschlüsselte E-Mails versenden zu können. Alles was Ihnen nun noch fehlt ist das öffentliche Zertifikat des Kontaktes, dem Sie eine verschlüsselte E-Mail zukommen lassen möchten. Dies ist notwendig, dass der Verschlüsselungsalgorithmus die E-Mail mit dem Zertifikat ihres Kontaktes verschlüsselt. Somit ist es auch notwendig, dass Ihr Kontakt Ihr öffentliches Zertifikat besitzt um Ihnen verschlüsselte E-Mails zu senden. Am einfachsten ist es, wenn sie Ihrem Kontakt eine von Ihnen signierte E-Mail zukommen lassen. Diese enthält dann, wenn alle Einstellungen so wie hier beschrieben getroffen sind, Ihr Zertifikat. Gemeint ist dabei keine Signatur im Sinne von Name, Nachname, Anschrift etc., sondern eine kryptographische Signatur. Im Folgenden ist beschrieben, wie Sie genau dies durchführen.

E-Mail mit Signatur verschicken:

1. Erstellen Sie eine ganz normale E-Mail
2. Bevor Sie diese absenden, vergewissern Sie sich, dass diese auch kryptographisch signiert ist. Dies machen Sie in dem Sie auf den Reiter „Optionen“ klicken und prüfen ob die Schaltfläche „Signieren“ dunkelgrau hinterlegt ist. Ist dies nicht der Fall, klicken Sie einmal auf „Signieren“ um dies dunkelgrau zu hinterlegen. Nun können Sie die E-Mail verschicken.



3. Sind Sie nun der Empfänger einer solchen signierten E-Mail, dann können Sie das Zertifikat des Absenders speichern, indem Sie diesen zu Ihren Kontakten in Ihrem Outlook Adressbuch hinzufügen. Gehen Sie dazu mit Ihrem Mauszeiger über den Absender in der E-Mail, klicken dann auf den kleinen Pfeil und dann an der Stelle des Pfeils auf „Hinzufügen“.



7 Verschlüsselte E-Mails verschicken

1. Erstellen Sie eine ganz normale E-Mail
2. Klicken Sie zunächst auf „Optionen“. Klicken Sie nun auf die Schaltfläche „Verschlüsseln“, um die Verschlüsselung zu aktivieren. Die Schaltfläche sollte nun dunkelgrau hinterlegt sein. Anschließend können Sie die E-Mail versenden. Beachten Sie, dass nur Personen deren Zertifikat Sie besitzen, verschlüsselte E-Mails von Ihnen empfangen können.