

 ISC	Nutzerzertifikat beantragen und in Outlook einbinden	Dokument Nr.	Rev. Nr.
		ISC_VA_K06_03	06

Inhaltsverzeichnis

1	Beantragung	2
1.1	Allgemeines	2
1.2	Beantragung des Zertifikats	2
2	Import des Gesamtzertifikats in den Windows Zertifikatsspeicher	12
3	Verwendung im Outlook.....	15
3.1	Allgemeine Bereitstellung.....	15
3.2	Signierung von E-Mails.....	21
3.3	Verschlüsselung von E-Mails.....	25
3.3.1	Vorbereitungen treffen	25
3.3.2	Kontakt für Verschlüsselung anlegen	25
3.3.3	Zertifikat für Verschlüsselung besorgen	28
3.3.4	Verschlüsselte E-Mail an sich selbst	32
4	Überarbeitung	34
5	Ablage und Archivierung	34
6	Änderungshistorie	34
7	Überprüfung und Genehmigung.....	34

 ISC	Nutzerzertifikat beantragen und in Outlook einbinden	Dokument Nr.	Rev. Nr.
		ISC_VA_K06_03	06

1 Beantragung

1.1 Allgemeines

Der Service für die Erstellung vertrauenswürdiger Zertifikate (TCS=Trusted Certificate Service) ist ein PKI-Angebot, das der DFN-Verein über GÉANT bezieht. GÉANT realisiert den Dienst mit Hilfe von externen Anbietern, die über regelmäßige Ausschreibungen gefunden werden. Der aktuelle Anbieter ist Harica. Viele Funktionen des Zertifikatsmanagers von Harica können nach einem Login über die DFN-AAI genutzt werden.

Der DFN-Verein betreibt die AAI (Authentifizierungs- und Autorisierungs-Infrastruktur), um Nutzenden einen Zugang zu geschützten Ressourcen zu ermöglichen. Die Nutzenden authentisieren sich an ihrer Heimateinrichtung (z. B. HS Anhalt) und erhalten nach Übertragung der zur Autorisierung notwendigen Daten (Hochschulzugangsdaten) an den betreffenden Dienst Zugriff auf die von der Hochschule jeweils freigegebenen Ressourcen.

Die Hochschule Anhalt betreibt seine Dienste überwiegend intern, nutzt aber die AAI des DFN-Vereins für die Authentifizierung der Nutzenden im Rahmen der Beantragung des Nutzerzertifikats.

Die Identifizierung der Berechtigten erfolgt erst- und letzt- bzw. einmalig bei der Einstellung oder Immatrikulation der entsprechenden Person über den Abgleich mit den amtlichen Ausweispapieren. Ist die Person einmal identifiziert, kann sie sich **selbst auf <https://cm.harica.gr> ein Nutzerzertifikat generieren.**

Erstellte Zertifikate können für die elektronische Authentifizierung und für Verschlüsselungszwecke verwendet werden.

Das IT-Service-Center und die jeweiligen Administratoren in den Organisationseinheiten sind dabei verantwortlich für die:

- Ausstellung von Zertifikaten für Server
- Beratung der Nutzer bei der eigenständigen Beantragung von Zertifikaten

Jeder Angehörige der Hochschule Anhalt kann sich ein Nutzerzertifikat beantragen.

1.2 Beantragung des Zertifikats

Die Beantragung eines Nutzerzertifikats kann **eigenständig vom Nutzer** mit den Hochschulzugangsdaten durchgeführt werden. Dazu wählt man im linken Menü unter „Certificate Requests“ den Menüpunkt „Email“ aus und befolgt den Assistenten. Das Zertifikat gilt ab Beantragung maximal 2 Jahre (730 Tage) und ist mit dem RSA-Algorithmus und einer Schlüssellänge von 2048 Bit abgesichert.

Gehen Sie wie im Folgenden beschrieben vor, um sich Ihr Zertifikat zu erstellen.

 ISC	Nutzerzertifikat beantragen und in Outlook einbinden	Dokument Nr.	Rev. Nr.
		ISC_VA_K06_03	06

1. Registrieren Sie sich auf der Seite <https://cm.harica.gr/> mit Ihrer HSA E-Mail-Adresse oder über Academic Login.

Login

New to HARICA? [Sign Up](#)

Email address

Type your email address

Password

Type your password

Forgot password?

Login

Or

 **Academic Login**

 **Sign in**

GREEK UNIVERSITIES NETWORK (GUnet)
 General Commercial Registry Number: 160729401000

2. Institution wählen

Choose Your Institution

Recent institutions


Anhalt University of Applied Sciences
 hs-anhalt.de

Wählen Sie Ihre Institution.

Es erfolgt eine Weiterleitung an den Identity Provider (IdP) der Hochschule.

 ISC	Nutzerzertifikat beantragen und in Outlook einbinden	Dokument Nr.	Rev. Nr.
		ISC_VA_K06_03	06

3. Anmeldung mit Hochschul-Account am IdP



Anmelden bei HARICA

Benutzername

Geben Sie Ihre Zugangsdaten aus der zentralen Nutzerverwaltung der HSA ein.

- ☐ Anmeldung nicht speichern
- ☐ Die zu übermittelnden Informationen anzeigen, damit ich die Weitergabe gegebenenfalls ablehnen kann.

Anmelden



 ISC	Nutzerzertifikat beantragen und in Outlook einbinden	Dokument Nr.	Rev. Nr.
		ISC_VA_K06_03	06

4. Datenübergabe an HARICA Dienst



Sie sind dabei auf diesen Dienst zuzugreifen:
HARICA von Greek University Network (GUnet)

Beschreibung dieses Dienstes:
*Hellenic Academic and Research Institutions
Certification Authority*

[Zusätzliche Informationen über diesen Dienst](#)

An den Dienst zu übermittelnde Informationen	
Targeted ID (pseudonyme Kennung)	
Vorname	Max
E-Mail	max.mustermann @hs-anhalt.de
Nachname	Mustermann

[Datenschutzinformationen dieses Dienstes](#)

Die oben aufgeführten Informationen werden an den Dienst weitergegeben, falls Sie fortfahren.
Sind Sie einverstanden, dass diese Informationen bei jedem Zugriff auf diesen Dienst an ihn weitergegeben werden?

Wählen Sie die Dauer, für die Ihre Entscheidung zur Informationsweitergabe gültig sein soll:

☐ Bei nächster Anmeldung erneut fragen.

- Ich bin einverstanden, meine Informationen dieses Mal zu senden.

☒ Erneut fragen, wenn sich die Informationen ändern, welche diesem Dienst weitergegeben werden.

- Ich bin einverstanden, dass dieselben Informationen in Zukunft automatisch an diesen Dienst weitergegeben werden.

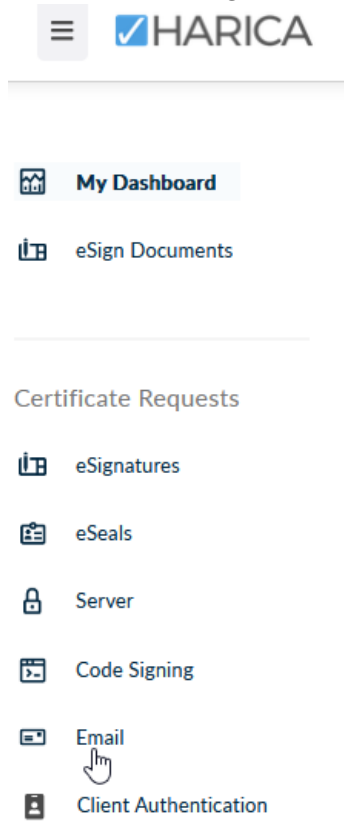
Diese Einstellung kann jederzeit mit der Checkbox auf der Anmeldeseite widerrufen werden.

Ablehnen

Akzeptieren

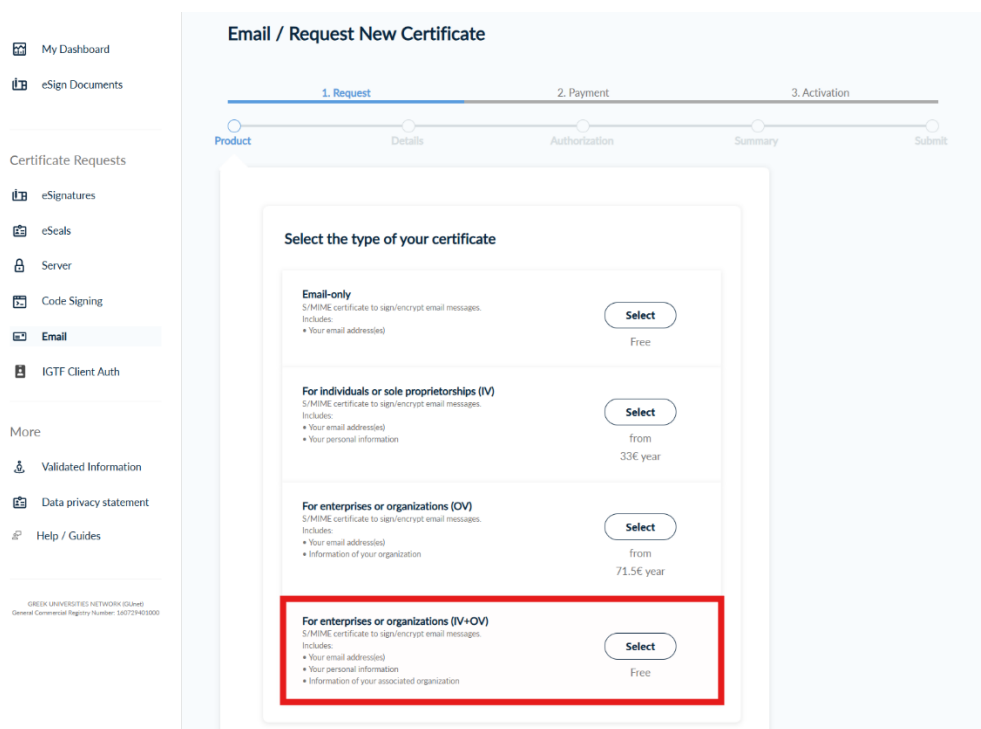
 ISC	Nutzerzertifikat beantragen und in Outlook einbinden	Dokument Nr.	Rev. Nr.
		ISC_VA_K06_03	06

5. HARICA CertManager (Persönliches Dashboard) wird geöffnet



Wählen Sie „Email“ für E-Mail-Zertifikate

6. Zertifikatstyp „For enterprises or organizations (IV+OV)“ auswählen



 ISC	Nutzerzertifikat beantragen und in Outlook einbinden	Dokument Nr.	Rev. Nr.
		ISC_VA_K06_03	06

7. Zusammenfassung

Email / Request New Certificate

1. Request
2. Payment

Product
Details
Authorization
Summary

Select the type of your certificate

[Change](#)

For enterprises or organizations (IV+OV)
S/MIME certificate to sign/encrypt email messages.
Includes:
• Your email address(es)
• Your personal information
• Information of your associated organization

Selected
Free

Enter your email address

Email Addresses
Include one or more email addresses in your certificate.

email max.mustermann @hs-anhalt.de

Next

Confirm your personal information

Subscriber Details

Given Name: .
Surname

Confirm that your personal information (Given name and Surname), as provided by your organization, is accurate and **fully matches** (letter-by-letter) the information of your identity document. Then, press Next.

Back
Next

 ISC	Nutzerzertifikat beantragen und in Outlook einbinden	Dokument Nr.	Rev. Nr.
		ISC_VA_K06_03	06

Organization information

Legal name
Hochschule Anhalt

Country
DE

State or province
Sachsen-Anhalt

Organization identifier
GOVDE\+ST

[< Back](#)
[Next](#)

8. Autorisierung

Email / Request New Certificate

1. Request
2. Payment
3. Activation

Product
Details
Authorization
Summary
Submit

Select a method to validate your email address(es)

Validate via email to selected email address

Validate via email to selected email address

Selected

[< Back](#)
[Next](#)

9. Request abschicken

 ISC	Nutzerzertifikat beantragen und in Outlook einbinden	Dokument Nr.	Rev. Nr.
		ISC_VA_K06_03	06

Review the application before submitting

Certificate Type
S/MIME IV+OV

Service Duration
2 years

Emails

1. max.mustermann@hs-anhalt.de

Subscriber Details

Given name: Henning
Surname: Zinner
Country:
City:
State or province:

Organization Details

Legal name: Hochschule Anhalt
State or province: Sachsen-Anhalt
Organization Identifier: GOVDE\+ST
Country: DE

Supporting Documents

Document Type	Files
Identity Document	

Authorization Method

Method	Files

☒ I, Max Mustermann, declare that I read and agree with, by submitting this request, the [Terms of Use](#) and the [Certification Practices](#) of HARICA. I also agree that HARICA shall process, use and store the data from this request in accordance with the [Data Privacy Statement](#).

← Back
Submit

10. Nach dem Abschicken des Requests kommt eine E-Mail vom HARICA Certificate Manager. Im E-Mail Client die Nachricht öffnen und mit „Confirm“ die angegebene E-Mailadresse validieren

 ISC	Nutzerzertifikat beantragen und in Outlook einbinden	Dokument Nr.	Rev. Nr.
		ISC_VA_K06_03	06

Validate your email

We have received your request to issue an S/MIME email-only certificate for max.mustermann@hs-anhalt.de.

Please confirm that you control the specific e-mail address and that you authorize HARICA to issue a certificate on your behalf by clicking the link below.

[Confirm](#)

11. Im HARICA CertManager E-Mail-Adresse bestätigen

Validate your email address

max.mustermann@hs-anhalt.de

Confirm that you own the above email address.

[Confirm](#)

12. Im Dashboard ist das Zertifikat nun sichtbar

Ready Certificates

Product	Validity	Information	Actions
S/MIME		max.mustermann@hs-anh...	Enroll your Certificate

 ISC	Nutzerzertifikat beantragen und in Outlook einbinden	Dokument Nr.	Rev. Nr.
		ISC_VA_K06_03	06

13. Zertifikat im .p12 Format erstellen
Die Passphrase muss mindestens 8 Zeichen lang sein!

Certificate Enrollment

Generate Certificate

Submit CSR manually

or

Generate your certificate in .p12 format. Use your (already created) CSR and submit it here.

Set a passphrase to protect your certificate. Please note that the passphrase is required to use the certificate and should therefore be **secured and not forgotten**.

Algorithm

Key size

RSA (default)

2048 (default)

Set a passphrase

.....

👁

Confirm passphrase

.....|

👁

☒ I understand that this passphrase is under my sole knowledge and HARICA does not have access to it.

Close

Enroll Certificate

14. Zertifikat herunterladen und an einem sicheren Ort speichern

Get your certificate

✓

Your certificate is ready. Press the **Download** button to retrieve it.

Download

👁

ATTENTION: This is the **ONLY TIME** you can perform this action, you cannot download the certificate later.

Close

 ISC	Nutzerzertifikat beantragen und in Outlook einbinden	Dokument Nr.	Rev. Nr.
		ISC_VA_K06_03	06

15. Anzeige im Dashboard

Valid Certificates			
Product	Validity	Information	
S/MIME	25/02/2027	E= max.mustermann@hs-a...	 

16. Spätere Downloadmöglichkeiten

Certificate



 Details
 Download
 Revocation
 Notifications
 Order

You can download your Certificate in a variety of formats, depending on your needs.

PEM	DER	DER CA	PKCS#7 (chain)	PEM bundle
Typical text format	Typical binary format	Typical binary format of the Issuing Authority Certificate	Typical text format including all certificate chain	Typical text format including all certificate chain

If your Certificate's Private Key is installed in a cryptographic device (token), you can download the **DER** and **DER (CA)** files and import them to your device through the token's management software. Otherwise, you can download the **PEM**, **PEM bundle** files and along with the **Private Key** file that you created earlier during the request process (**privateKey.pem**), visit <https://www.harica.gr/en/Tools/PemToP12> and convert them into a single **.p12** file which is used by various operating systems/applications.

2 Import des Gesamtzertifikats in den Windows Zertifikatsspeicher

Um Ihr persönliches Zertifikat benutzen zu können, müssen Sie diese *.p12 Datei an jedem PC, wo Sie es benutzen wollen, importieren. Das ist recht einfach, weil diese Datei bereits alle erforderlichen Teile enthält und unter Windows i. d. R. die Dateiendung *.p12 mit dem Windows-Zertifikats-Assistenten verknüpft ist.

Doppelklicken Sie einfach auf Ihre Zertifikatsdatei oder gehen Sie mit der rechten Maustaste auf die .p12-Datei und wählen „pfx installieren“ aus.

Es öffnet sich der Zertifikats-Import-Assistent.

Sie müssen nichts Besonderes bedenken. Klicken Sie einfach alles immer mit <Weiter> bzw. <Fertig stellen> durch bis zum Ende.

 ISC	Nutzerzertifikat beantragen und in Outlook einbinden	Dokument Nr.	Rev. Nr.
		ISC_VA_K06_03	06

Willkommen

Dieser Assistent hilft Ihnen beim Kopieren von Zertifikaten, Zertifikatvertrauenslisten und Zertifikatssperlisten vom Datenträger in den Zertifikatspeicher.

Ein von einer Zertifizierungsstelle ausgestelltes Zertifikat dient der Identitätsbestätigung. Es enthält Informationen für den Datenschutz oder für den Aufbau sicherer Netzwerkverbindungen. Ein Zertifikatspeicher ist der Systembereich, in dem Zertifikate gespeichert werden.

Speicherort:

☒ Aktueller Benutzer
☐ Lokaler Computer

Klicken Sie auf "Weiter", um den Vorgang fortzusetzen.

Zu importierende Datei

Geben Sie die Datei an, die importiert werden soll.

Dateiname:

Hinweis: Mehrere Zertifikate können in einer Datei in folgenden Formaten gespeichert werden:

Privater Informationsaustausch - PKCS #12 (.PFX, .P12)
 Syntaxstandard kryptografischer Meldungen - "PKCS #7"-Zertifikate (.P7B)
 Microsoft Serieller Zertifikatspeicher (.SST)

Tragen Sie das Passwort ein, welches Sie bei der Beantragung vergeben haben und lassen Sie den Zertifikatspeicher automatisch auswählen.

Schutz für den privaten Schlüssel

Der private Schlüssel wurde mit einem Kennwort geschützt, um die Sicherheit zu gewährleisten.

Geben Sie das Kennwort für den privaten Schlüssel ein.

Kennwort:

☐ Kennwort anzeigen

Importoptionen:

☐ Hohe Sicherheit für den privaten Schlüssel aktivieren. Wenn Sie diese Option aktivieren, werden Sie immer dann, wenn der private Schlüssel von einer Anwendung verwendet wird, zur Kennworteingabe aufgefordert.
☒ Schlüssel als exportierbar markieren. Dadurch können Sie Ihre Schlüssel zu einem späteren Zeitpunkt sichern bzw. überführen.
☐ Privaten Schlüssel mit virtualisierungsbasierter Sicherheit schützen (nicht exportierbar)
☒ Alle erweiterten Eigenschaften mit einbeziehen

Zertifikatspeicher

Zertifikatspeicher sind Systembereiche, in denen Zertifikate gespeichert werden.

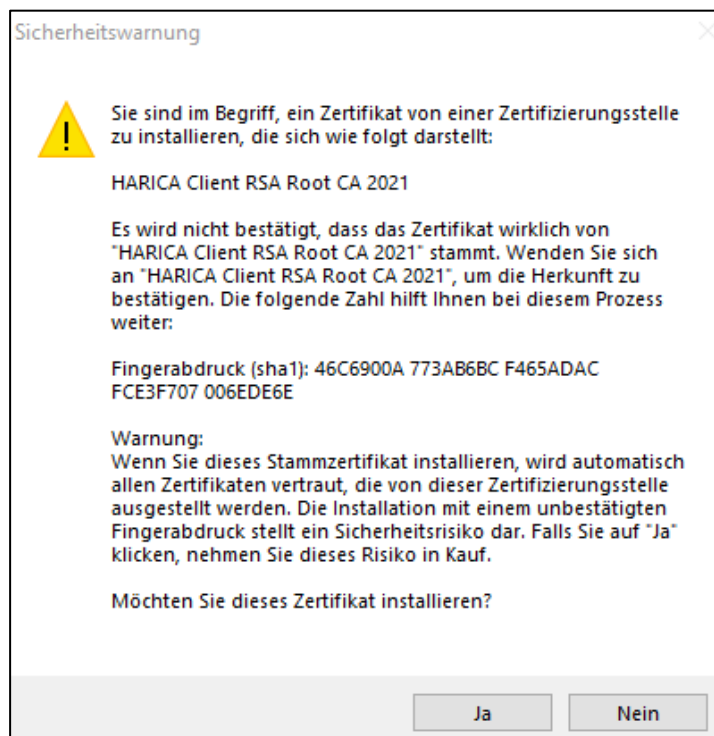
Windows kann automatisch einen Zertifikatspeicher auswählen, oder Sie können einen Speicherort für die Zertifikate angeben.

☒ Zertifikatspeicher automatisch auswählen (auf dem Zertifikattyp basierend)
☐ Alle Zertifikate in folgendem Speicher speichern

Zertifikatspeicher:

Möglicherweise kommt es bei der Fertigstellung zu einer Sicherheitswarnung. Diese erscheint, wenn dem System nicht die gesamte sog. Zertifikatskette bekannt ist. Stimmen Sie mit „Ja“ zu, damit das Stammzertifikat und alle nachrangigen Zertifikate als vertrauenswürdig aufgenommen werden können.

 ISC	Nutzerzertifikat beantragen und in Outlook einbinden	Dokument Nr.	Rev. Nr.
		ISC_VA_K06_03	06



Wenn der Zertifikatsimport erfolgreich war, erhalten Sie eine entsprechende System-Meldung.

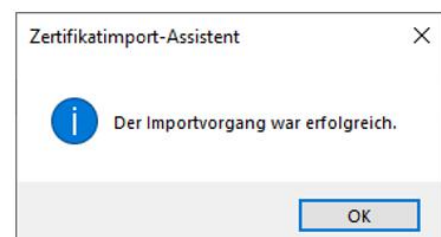
←  Zertifikatimport-Assistent

Fertigstellen des Assistenten

Das Zertifikat wird importiert, nachdem Sie auf "Fertig stellen" geklickt haben.

Sie haben folgende Einstellungen ausgewählt:

Gewählter Zertifikatspeicher	Auswahl wird vom Assistenten automatisch festgelegt
Inhalt	PFX
Dateiname	.p12



Falls Sie das Ergebnis gern kontrollieren möchten, öffnen Sie den Windows-Zertifikatsspeicher über die Windows Start-Taste. Geben Sie dann certmgr.msc ein gefolgt von Enter. Öffnen Sie links „Eigene Zertifikate“ und darunter nochmals „Zertifikate“. Dann sollten Sie rechts das frisch importierte Zertifikat sehen.



 ISC	Nutzerzertifikat beantragen und in Outlook einbinden	Dokument Nr.	Rev. Nr.
		ISC_VA_K06_03	06

Zertifikate - Aktueller Benutzer	Ausgestellt für	Ausgestellt von	Ablaufdatum	Beabsichtigte Zwecke	Anzeigenname
- Eigene Zertifikate - Zertifikate	max.mustermann@hs-anhalt.de	HARICA S/MIME RSA	25.02.2027	Clientauthentifizierung, Sichere E-Mail	<Keine>

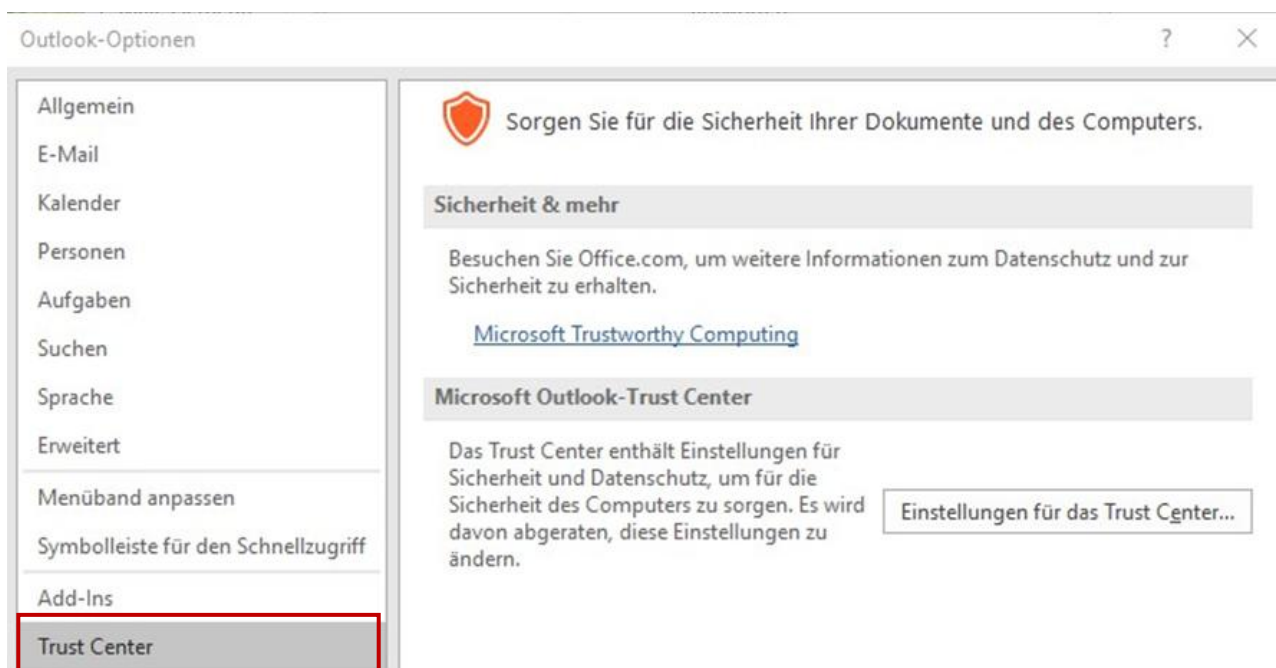
3 Verwendung im Outlook

3.1 Allgemeine Bereitstellung

In der Regel wollen Sie das Zertifikat auch an anderen PCs mit Outlook verwenden. Dazu müssen Sie das Zertifikat auch dort aus der *.p12-Datei in den Windows-Zertifikatsspeicher importieren. Dafür gibt es die Möglichkeit, das Zertifikat über Outlook zu importieren.

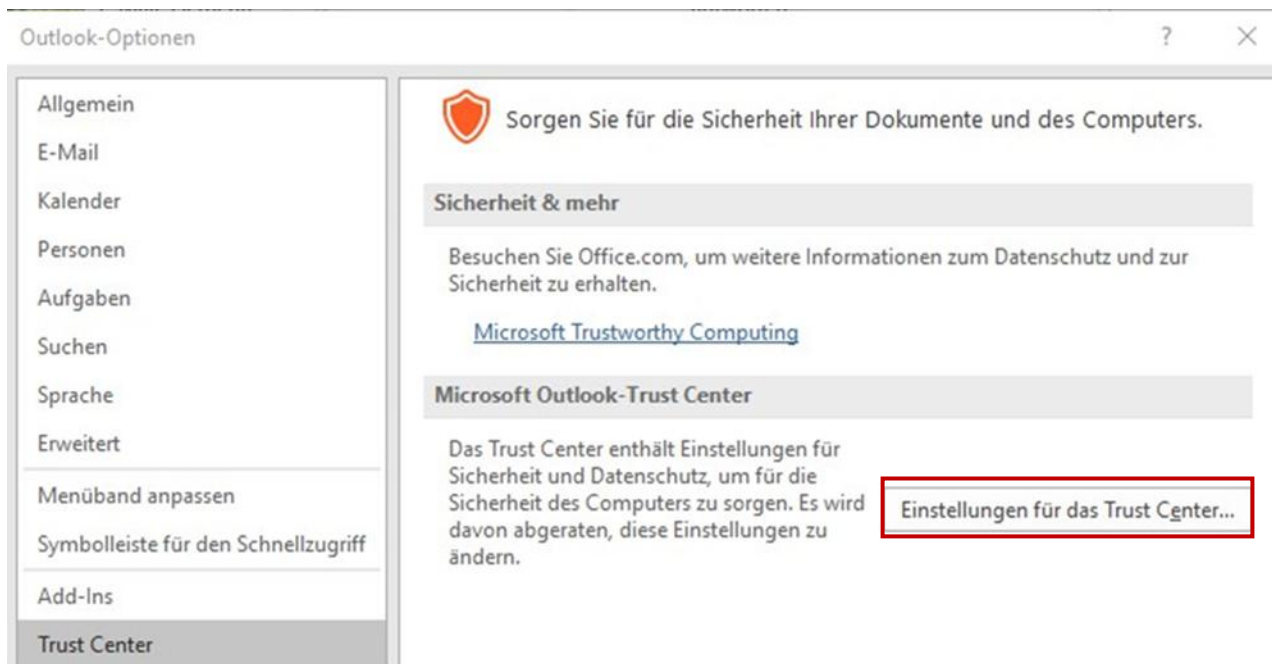
Outlook sollte gestartet und am besten mit Ihrem Postfach verbunden sein. Hier ein Beispiel mit Outlook 2016.

Im Outlook wählen Sie <Datei>, <Optionen>, <Trust Center>

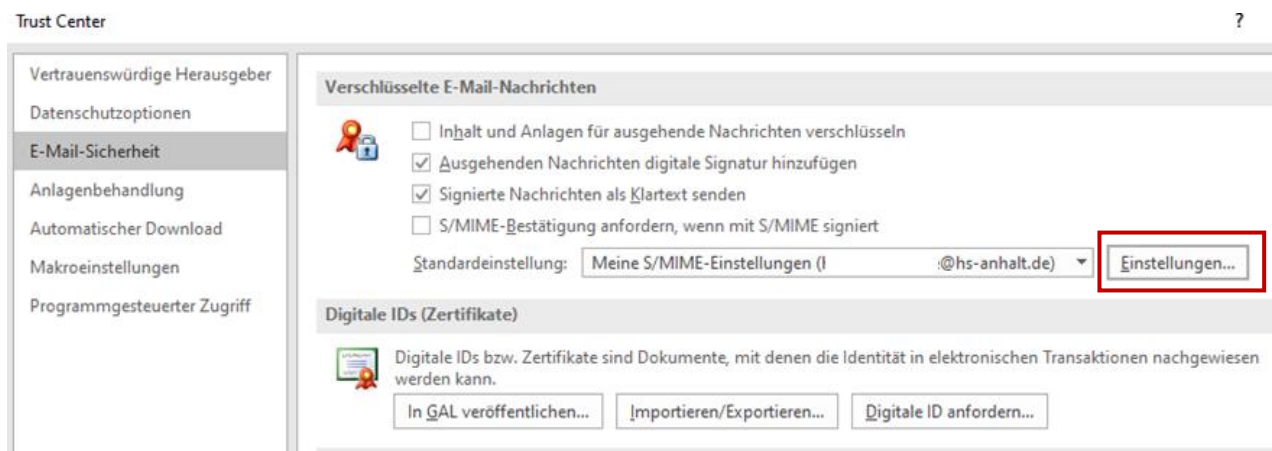


Als Nächstes <Einstellungen für das Trust Center...>

 ISC	Nutzerzertifikat beantragen und in Outlook einbinden	Dokument Nr.	Rev. Nr.
		ISC_VA_K06_03	06



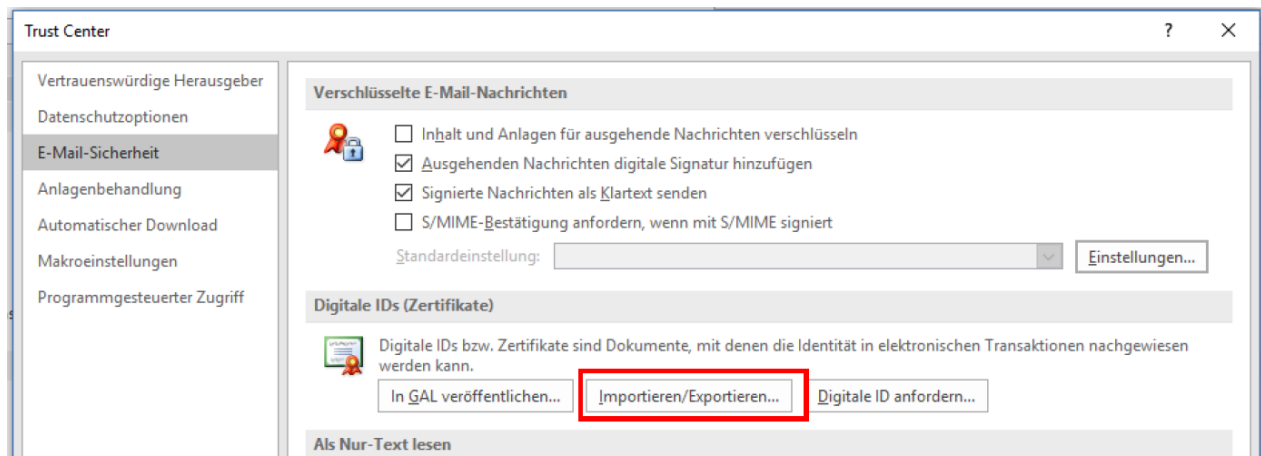
Wählen Sie nun E-Mail-Sicherheit



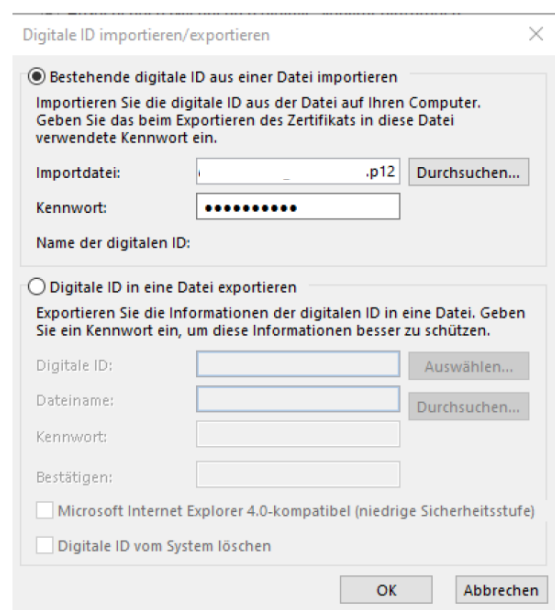
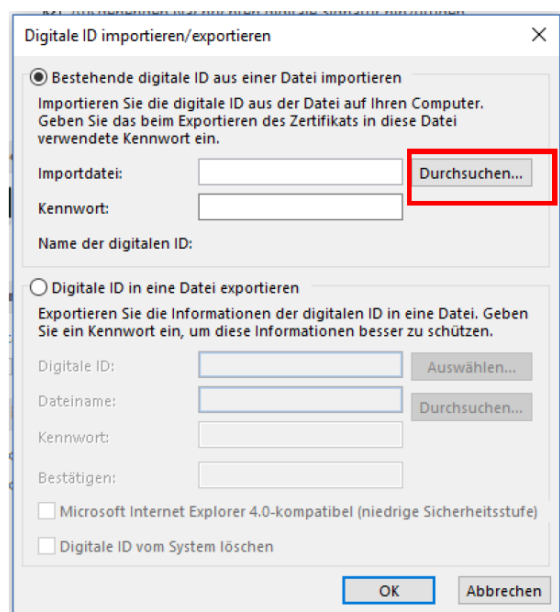
Klicken Sie auf <Einstellungen...>

Bei mir gibt es schon S/MIME-Einstellungen. Bei Ihnen ist das u. U. leer. Sie könnten (falls es nicht leer ist) im aktuellen Fenster auf <Löschen> klicken und mit <OK> bestätigen. Danach sieht es dann so (leer) aus wie im folgenden Bild.

 ISC	Nutzerzertifikat beantragen und in Outlook einbinden	Dokument Nr.	Rev. Nr.
		ISC_VA_K06_03	06



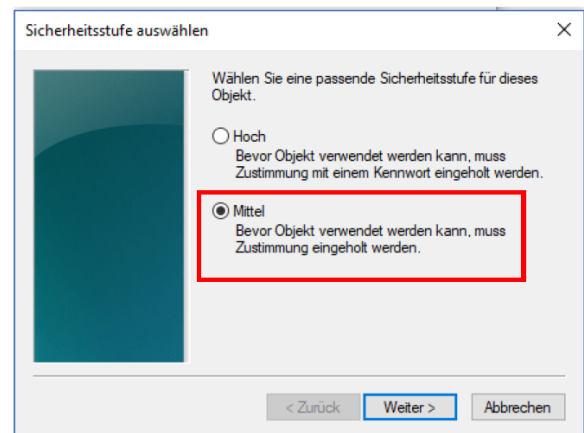
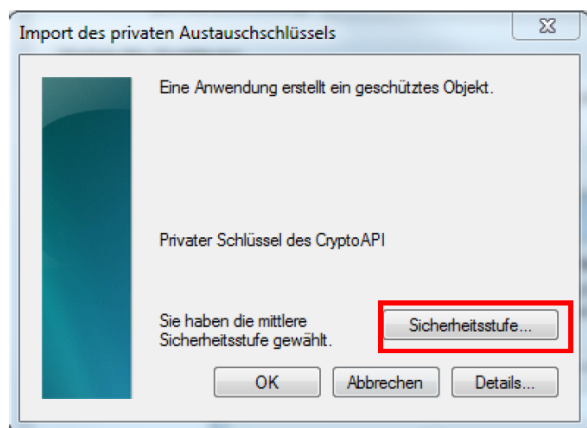
Klicken Sie auf <Importieren/Exportieren...>



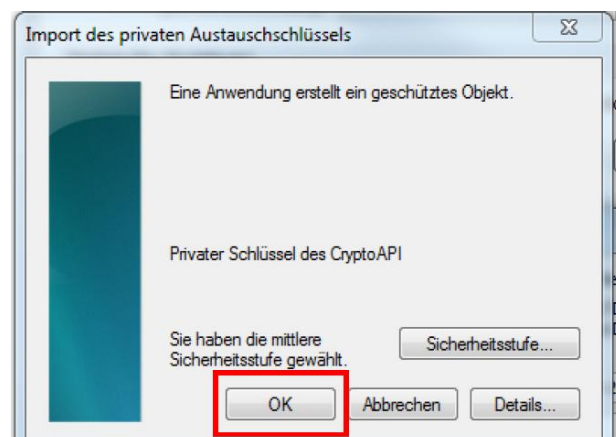
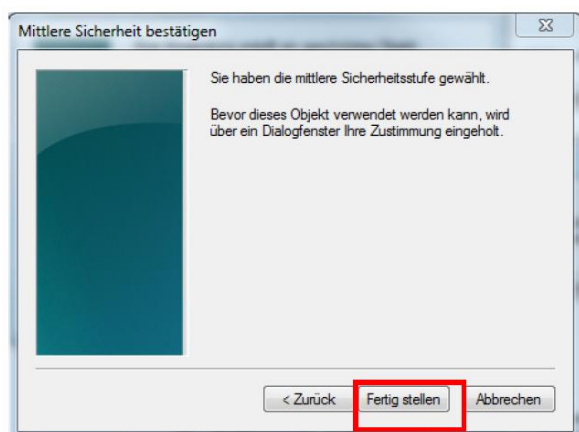
Klicken Sie auf **Durchsuchen** und wählen Sie die *.p12-Datei aus. Als Kennwort geben Sie das Kennwort ein, was Sie beim Exportieren des Zertifikats angegeben haben. Damit ist der private Schlüssel geschützt. Er muss ja nun entnommen werden. Dazu ist das Passwort erforderlich. Bestätigen Sie mit **OK**.

Nun müssen Sie die Sicherheitsstufe angeben. Klicken Sie auf die entsprechende Schaltfläche <Sicherheitsstufe...>.

 ISC	Nutzerzertifikat beantragen und in Outlook einbinden	Dokument Nr.	Rev. Nr.
		ISC_VA_K06_03	06



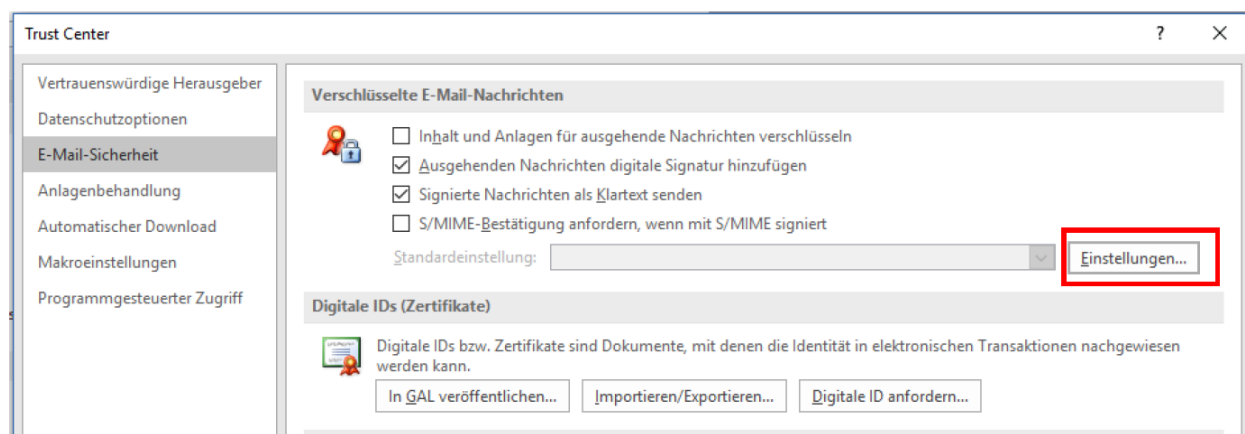
Wählen Sie am besten <Mittel> und klicken auf <Weiter> und danach auf <Fertig stellen>



Bestätigen Sie erst jetzt mit OK.

Danach ist das Zertifikat im Windows-Zertifikatsspeicher importiert.

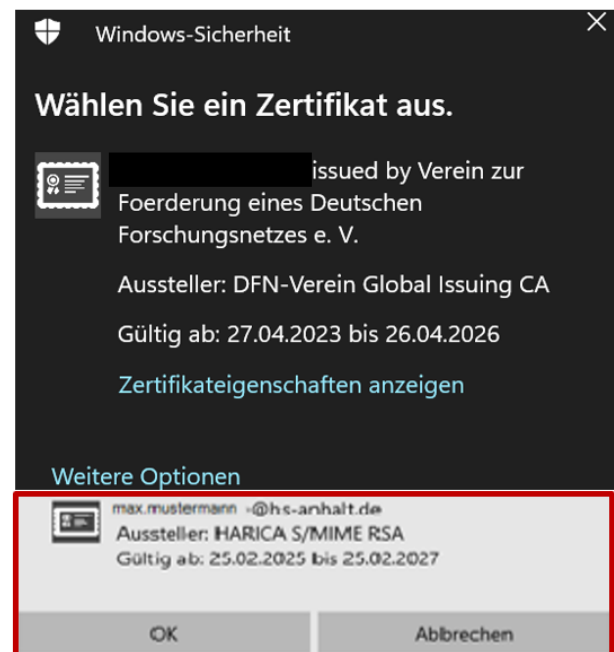
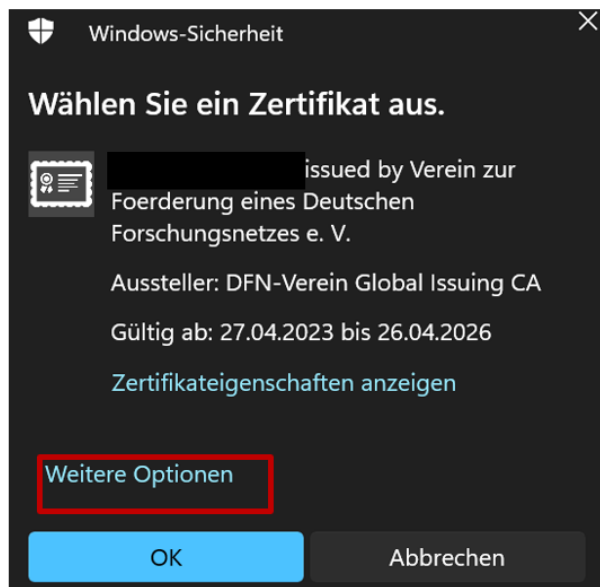
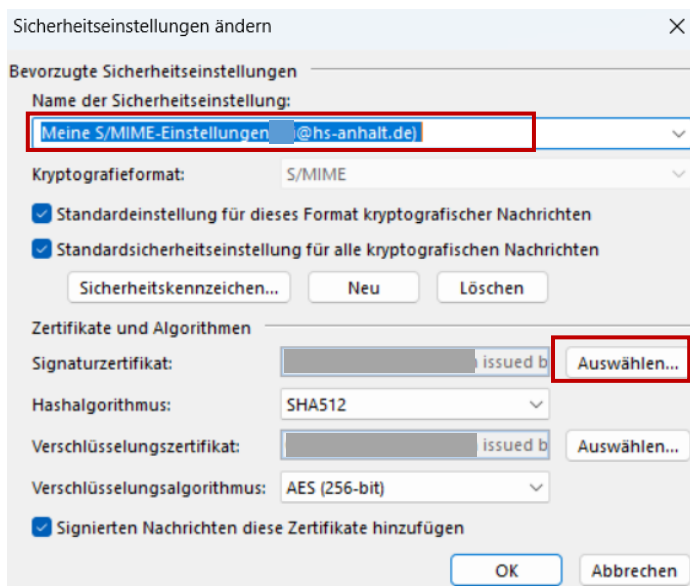
Klicken Sie nun auf <Einstellungen...>



 ISC	Nutzerzertifikat beantragen und in Outlook einbinden	Dokument Nr.	Rev. Nr.
		ISC_VA_K06_03	06

Vergeben Sie einen Namen für die Sicherheitseinstellung (z. B. Ihr Name). Das ist hier im Beispiel bereits vergeben gewesen und stammt noch von dem alten Zertifikat. Bei Ihrem ersten Zertifikat ist das oberste Feld wahrscheinlich leer.

Klicken Sie hinter Signaturzertifikat auf <Auswählen...>



U. U. wird noch das alte Zertifikat angezeigt, was vielleicht auch noch nicht abgelaufen ist, es soll aber nicht genutzt werden.

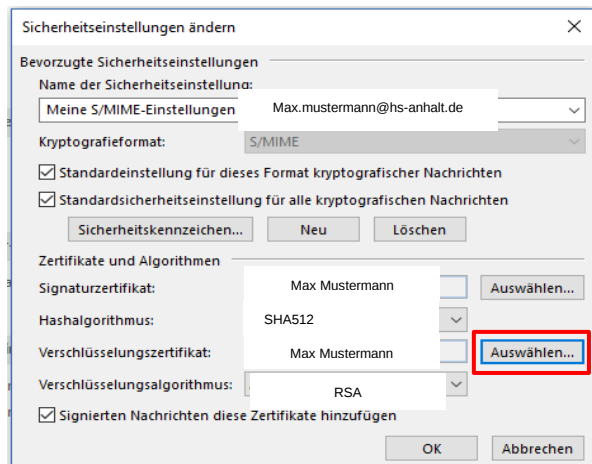
Wählen Sie deshalb <Weitere Optionen>.

 ISC	Nutzerzertifikat beantragen und in Outlook einbinden	Dokument Nr.	Rev. Nr.
		ISC_VA_K06_03	06

Im unteren Bereich wählen Sie das neue Zertifikat aus und bestätigen mit <OK>.

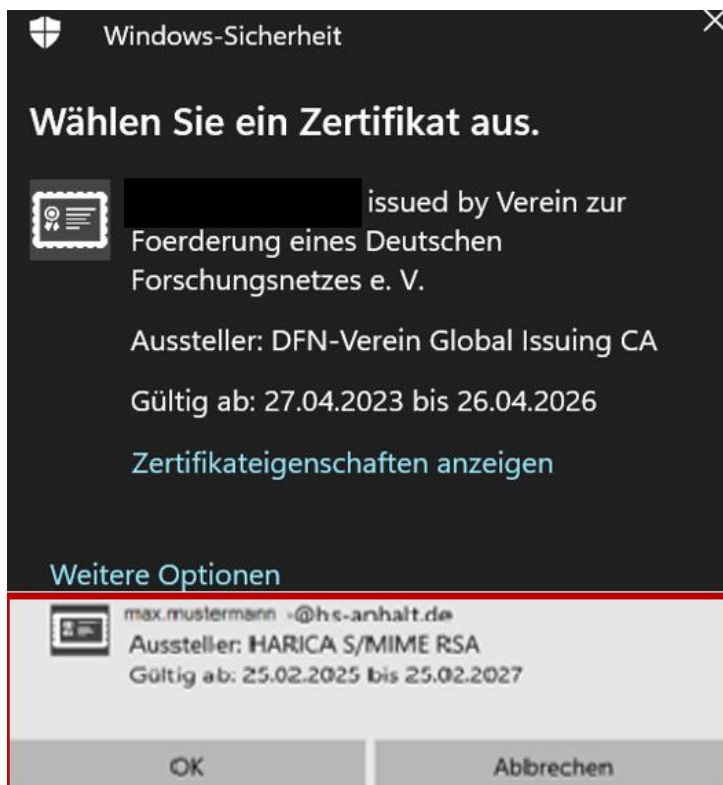
Das Gleiche muss unbedingt auch noch mit dem Verschlüsselungszertifikat erfolgen.

Klicken Sie hinter Verschlüsselungszertifikat dazu auf <Auswählen...>



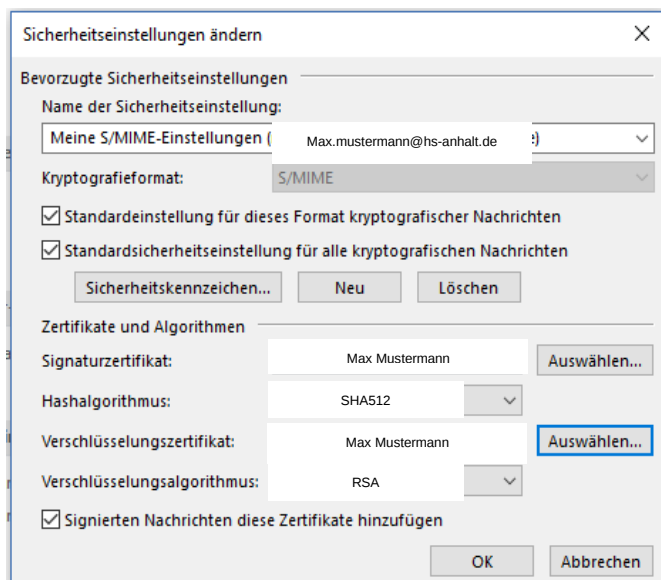
Hier wird ebenfalls noch das alte Zertifikat angezeigt, das nicht mehr genutzt werden soll. Wählen Sie deshalb auch wieder <Weitere Optionen>.

Im unteren Bereich wählen Sie das neue Zertifikat aus und bestätigen mit <OK>

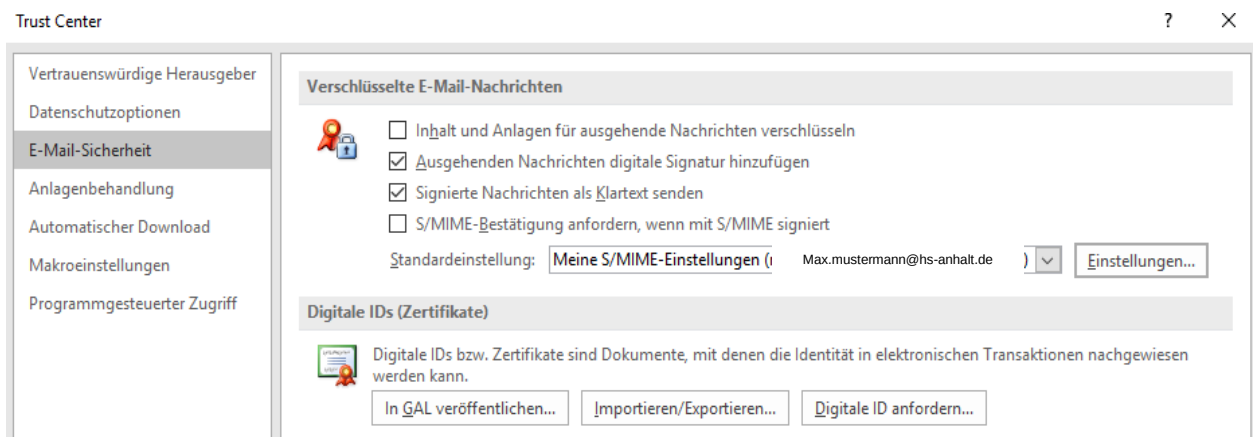


 ISC	Nutzerzertifikat beantragen und in Outlook einbinden	Dokument Nr.	Rev. Nr.
		ISC_VA_K06_03	06

Kontrollieren Sie ob die 3 Häkchen gesetzt sind wie im folgenden Bild.



Bestätigen Sie mit OK.



Nun können Sie alle weiteren Dialogfenster schließen. Outlook ist nun komplett vorbereitet.

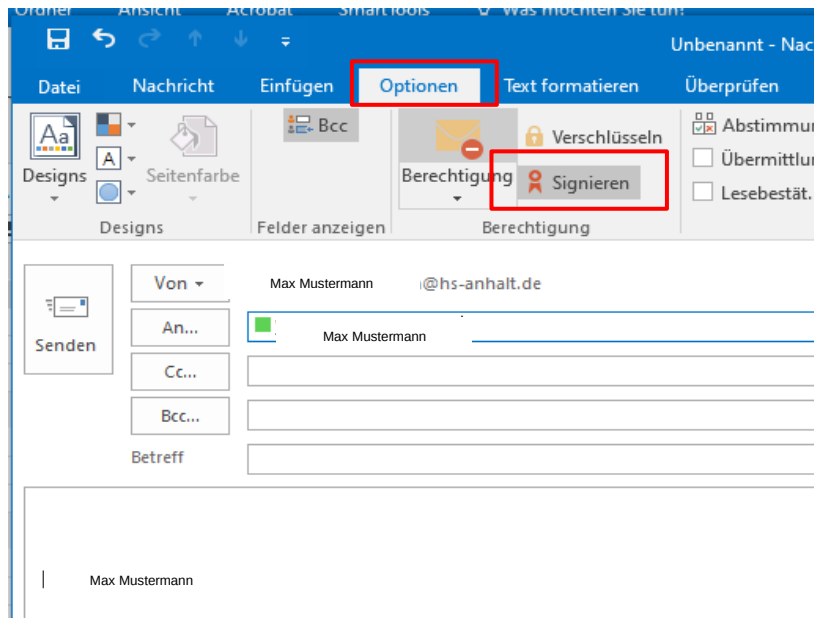
3.2 Signierung von E-Mails

Nun sollten Sie sich selbst einmal eine signierte E-Mail schicken und prüfen, ob das richtige Zertifikat verwendet worden ist und ob die Signierung funktioniert.

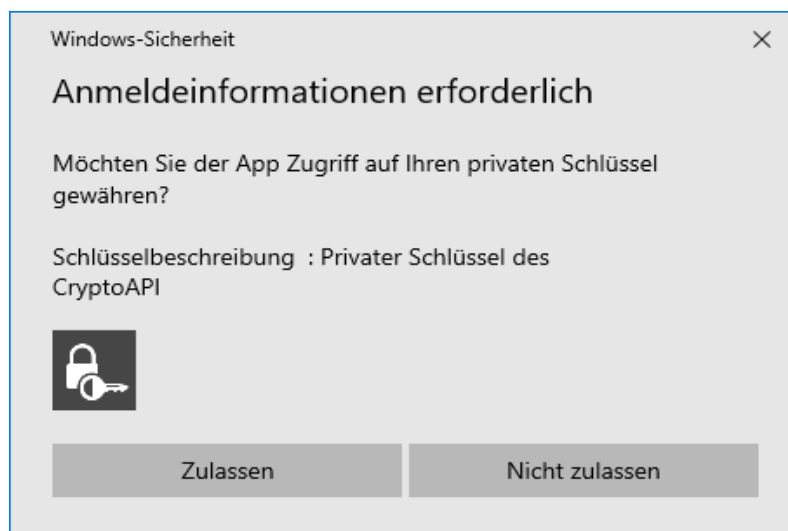
Die Signierung sollte gemäß den Einstellungen automatisch erfolgen und ist innerhalb der neuen E-Mail auf dem Register Optionen kontrollierbar.

 ISC	Nutzerzertifikat beantragen und in Outlook einbinden	Dokument Nr.	Rev. Nr.
		ISC_VA_K06_03	06

Beginnen Sie also, eine neue E-Mail zu schreiben und wechseln Sie auf das Register Optionen. Dort sollte nun im Bereich Berechtigung bereits die Schaltfläche Signieren betätigt sein.



Stellen Sie die E-Mail fertig und senden Sie sie an sich selbst ab.
Wenn Sie auf <Senden> klicken erfolgt eine Sicherheitsabfrage.

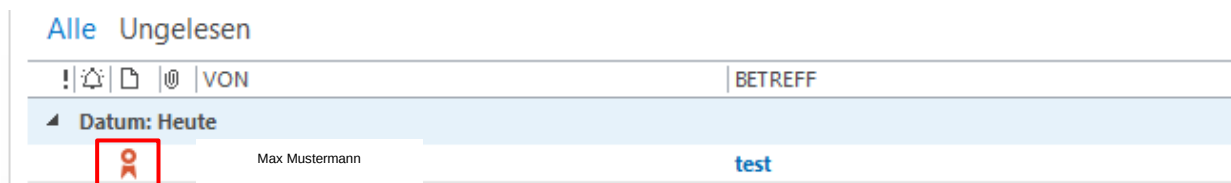


Es erfolgt ein Zugriff auf Ihren privaten Schlüssel im Zertifikatsspeicher. Diese Abfrage erfolgt, weil wir beim Import des Zertifikats die Sicherheitsstufe Mittel angegeben hatten.

Diese Abfrage durch Outlook erfolgt nur bei der ersten Benutzung. Bitte auf <Zulassen> klicken. Diese Berechtigung bleibt erhalten bis Outlook beendet wurde. Nach einem Neustart von Outlook erfolgt bei der ersten E-Mail die Abfrage erneut.

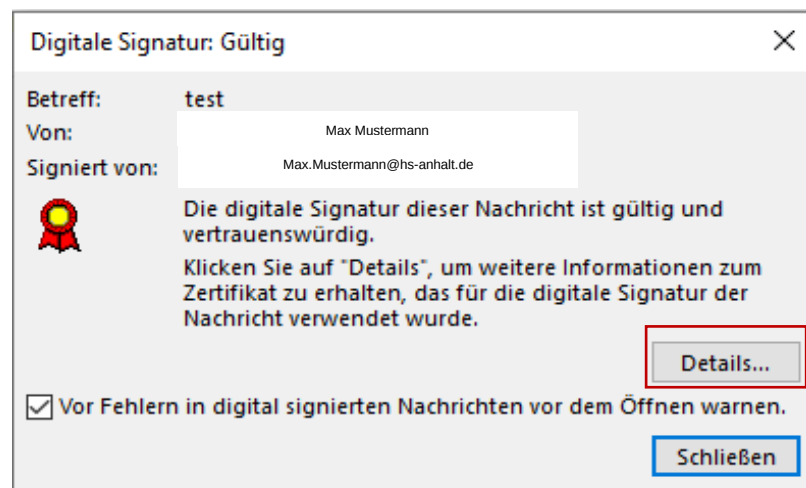
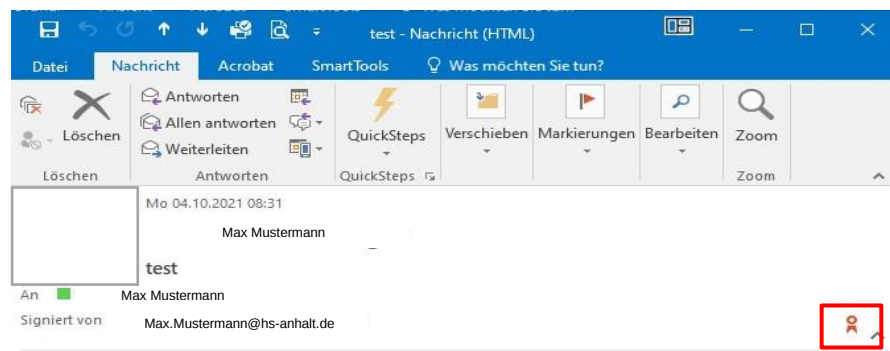
 ISC	Nutzerzertifikat beantragen und in Outlook einbinden	Dokument Nr.	Rev. Nr.
		ISC_VA_K06_03	06

Eine Signierte E-Mail erkennen Sie jeweils am roten Siegel. Hier im Posteingang am Zeilenanfang in der Symbolspalte:



Auch bei der geöffneten E-Mail ist das Siegel zu sehen. Unter <Betreff> steht Signiert von <Ihre E-Mail-Adresse> und am Zeilenende das Siegel-Symbol.

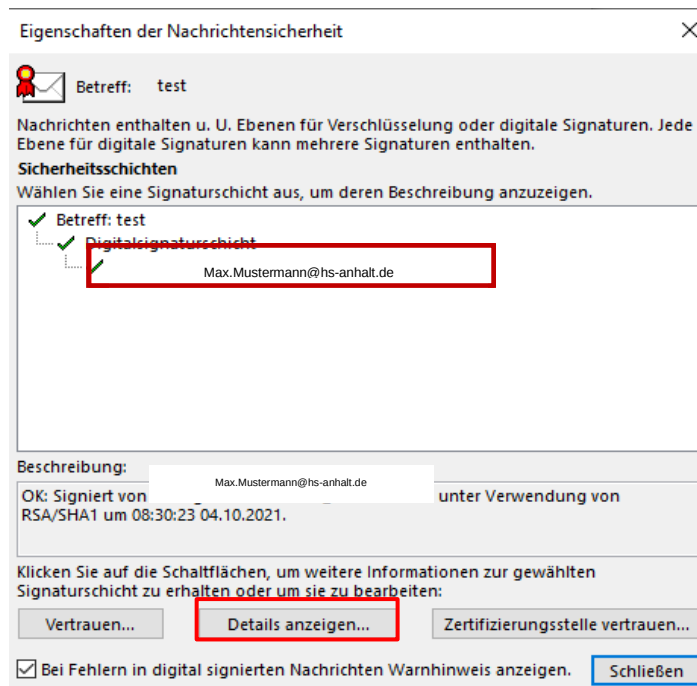
Das Zertifikat prüfen Sie durch Klick auf das Siegel-Symbol.



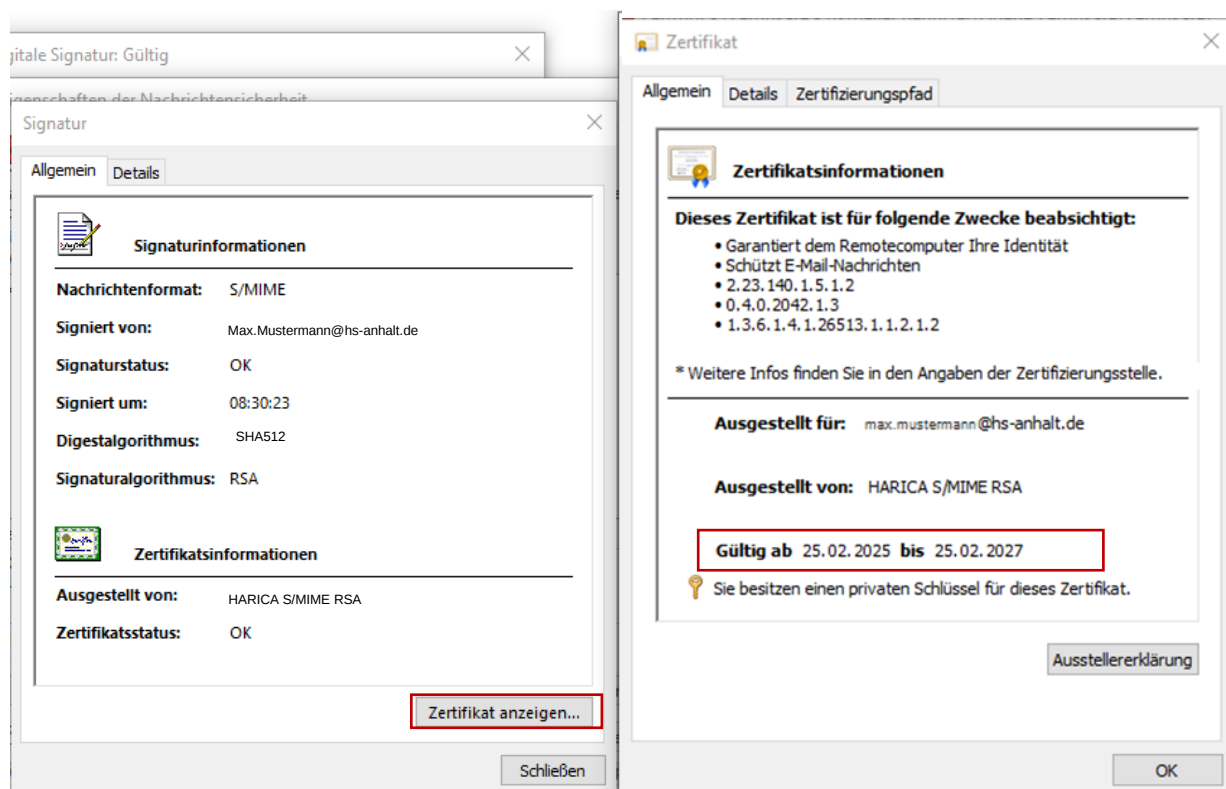
Hier sollte angezeigt werden, dass alles gültig und vertrauenswürdig ist.

Klicken Sie auf Details....

 ISC	Nutzerzertifikat beantragen und in Outlook einbinden	Dokument Nr.	Rev. Nr.
		ISC_VA_K06_03	06



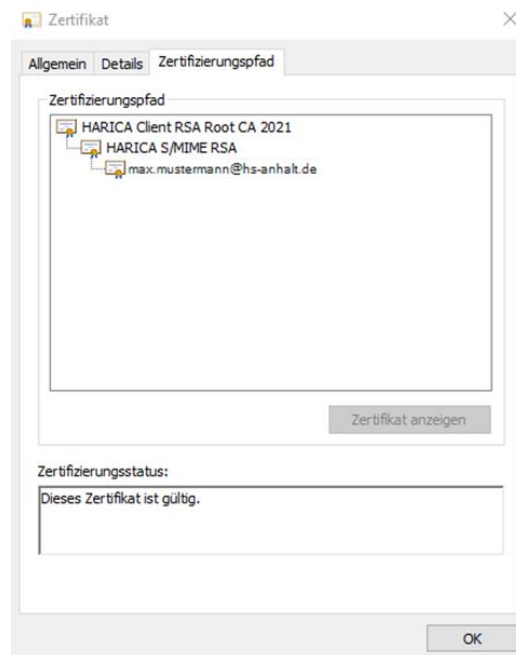
Unter Sicherheitsschichten markieren Sie die Zeile Signierer: und wählen <Details anzeigen>. Nun auf <Zertifikat Anzeigen...> klicken.



 ISC	Nutzerzertifikat beantragen und in Outlook einbinden	Dokument Nr.	Rev. Nr.
		ISC_VA_K06_03	06

Auf der Registerkarte „Allgemein“ bitte den Gültigkeitszeitrahmen prüfen. Daran sollten Sie Ihr Zertifikat erkennen und evtl. bemerken, ob vielleicht noch ein altes Zertifikat benutzt worden ist.

Wechseln Sie nun auf die Registerkarte „Zertifizierungspfad“ und prüfen Sie die Zertifikatskette.



Schließen Sie alle Fenster.

3.3 Verschlüsselung von E-Mails

3.3.1 Vorbereitungen treffen

Wenn Sie einer anderen Person eine verschlüsselte E-Mail schicken wollen, benötigen Sie von dieser Person den öffentlichen Teil des Zertifikats. Damit kann Outlook die E-Mail verschlüsseln. Nur der Besitzer des Zertifikats kann mit seinem privaten Schlüssel die E-Mail wieder entschlüsseln. Wenn der Empfänger seinen E-Mail-Client entsprechend konfiguriert hat, geschieht das völlig automatisch und für den Benutzer transparent.

Sie müssen sich also immer den öffentlichen Teil des Zertifikats des Partners besorgen. Dazu wird das in der Regel auch öffentlich im Internet publiziert. Auch Ihr Zertifikat wird unter unserer Zertifizierungsstelle veröffentlicht. Um mit Outlook E-Mails verschlüsseln zu können, müssen Sie sich für jede Person, der Sie verschlüsselte E-Mails senden wollen, einen Kontakt anlegen und in diesem Kontakt den öffentlichen Teil von dessen Zertifikat einfügen.

3.3.2 Kontakt für Verschlüsselung anlegen

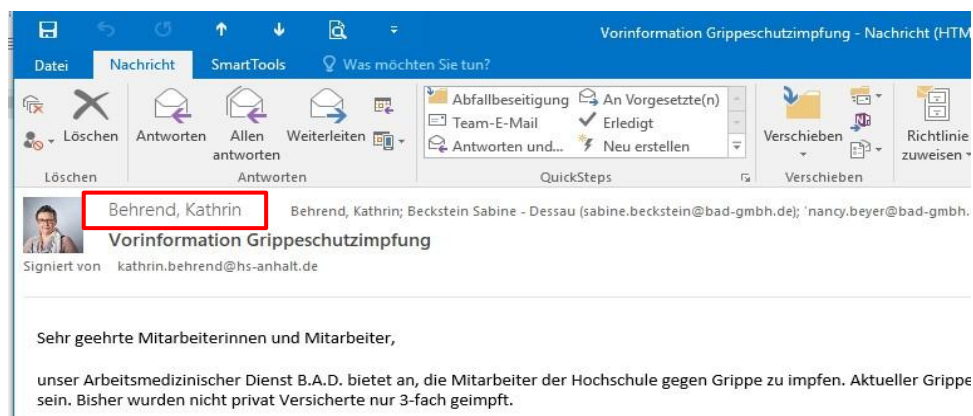
Outlook nutzt dazu den Ordner Kontakte des Postfachs. Alle persönlichen Kontakte, die Sie im Outlook pflegen, werden dort gespeichert. Sie sind serverbasiert und weltweit von überall aus benutzbar, was ein großer Vorteil ist. Dort können Sie das Zertifikat des Benutzers speichern. Wenn Sie für diese Person noch

 ISC	Nutzerzertifikat beantragen und in Outlook einbinden	Dokument Nr.	Rev. Nr.
		ISC_VA_K06_03	06

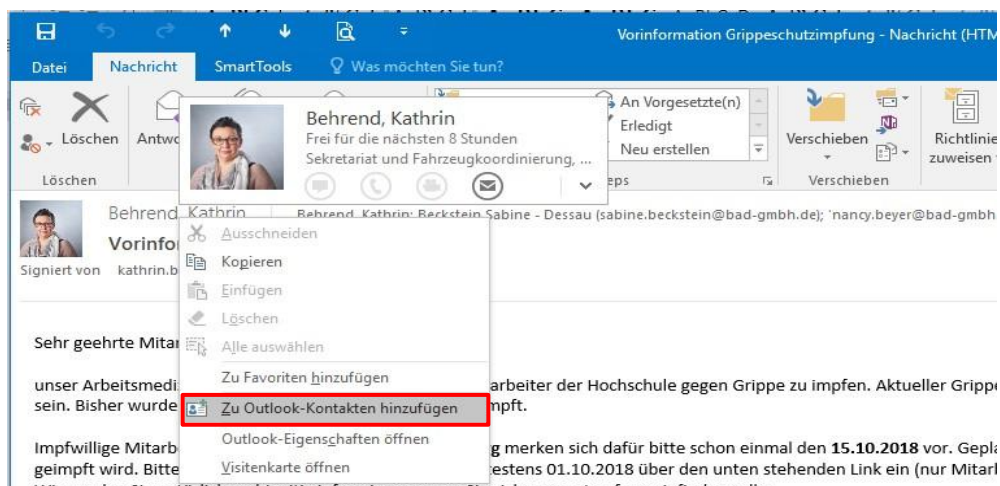
keinen Kontakt angelegt haben, müssen Sie das als erstes durchführen. Das gilt auch für Personen, die Sie sonst im serverbasierten Adressbuch finden und natürlich auch für Sie selbst.

Sie können manuell einen Kontakt mit den üblichen Mitteln von Outlook anlegen. Wenn Sie schon einmal eine E-Mail von dieser Person erhalten haben, können Sie einfach aus der E-Mail heraus einen Kontakt erzeugen.

Öffnen Sie dazu diese E-Mail. Im oberen Bereich finden Sie den Absender. Hier Behrend, Kathrin in grauer Schrift rechts neben dem Foto.



Machen Sie einen rechten Mausklick auf den Namen des Absenders und wählen Sie im Kontextmenü den Eintrag „Zu Outlook-Kontakten hinzufügen“.

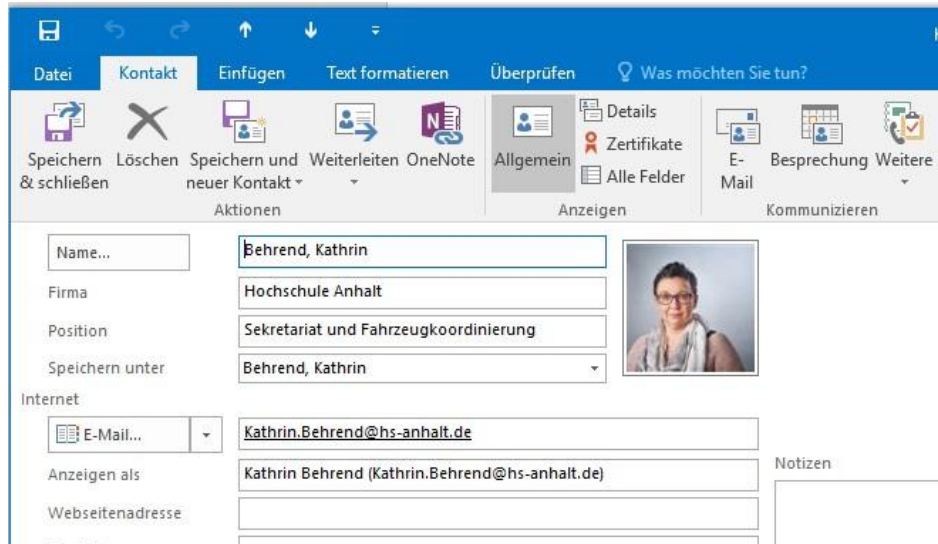


Folgen Sie den Anweisungen und speichern Sie abschließend. Danach finden Sie in Ihren Kontakten den entsprechenden Eintrag, z. B. so:

Behrend, Kathrin	
Postanschrift:	Bernburger Straße 55
	06366 Köthen (Anhalt) Sachsen...
Geschäftlich:	4010
E-Mail:	Kathrin.Behrend@hs-anhalt.de
Nachname:	Behrend
Vorname:	Kathrin

 ISC	Nutzerzertifikat beantragen und in Outlook einbinden	Dokument Nr.	Rev. Nr.
		ISC_VA_K06_03	06

Öffnen Sie diesen Kontakt und ergänzen Sie ggf. weitere Informationen.

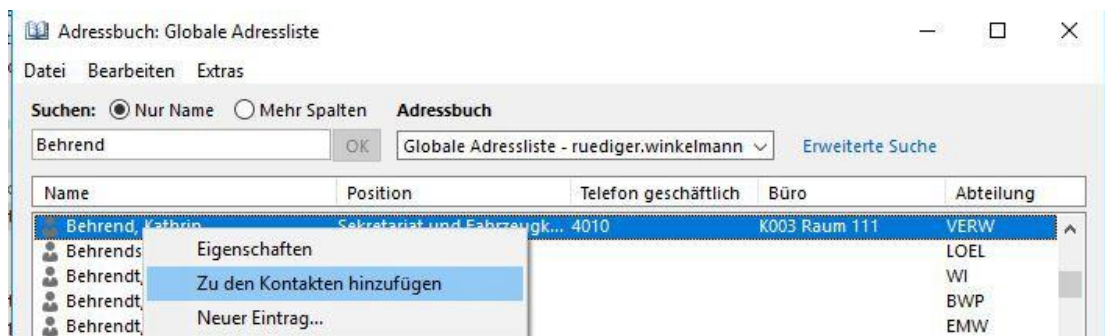


Eine weitere elegante Möglichkeit ist es, den Kontakt einfach aus dem entsprechenden Eintrag des serverbasierten Adressbuches zu erzeugen. Das ist aber natürlich nur möglich, wenn ein Eintrag im serverbasierten Adressbuch existiert, die Person also zur Hochschule gehört. Öffnen Sie das serverbasierte Adressbuch und suchen Sie die Person.



Name	Position	Telefon geschäftlich	Büro	Abteilung
Behrend, Kathrin	Sekretariat und Fahrzeug...	4010	K003 Raum 111	VERW
Behrends, Hinnerk	LOEL-LW2018-Wi			LOEL
Behrendt, Christine				WI
Behrendt, Fritz Heinz	BWP-VT2014-Wi			BWP

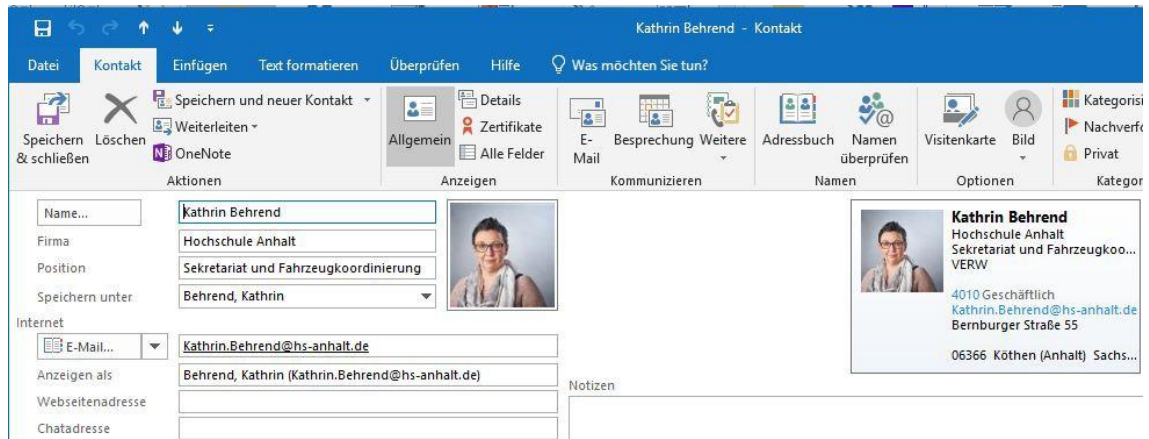
Nach einem rechten Mausklick auf den Datensatz wählen Sie <Zu den Kontakten hinzufügen>.



Name	Position	Telefon geschäftlich	Büro	Abteilung
Behrend, Kathrin	Sekretariat und Fahrzeug...	4010	K003 Raum 111	VERW
Behrends, Hinnerk	LOEL-LW2018-Wi			LOEL
Behrendt, Christine				WI
Behrendt, Fritz Heinz	BWP-VT2014-Wi			BWP

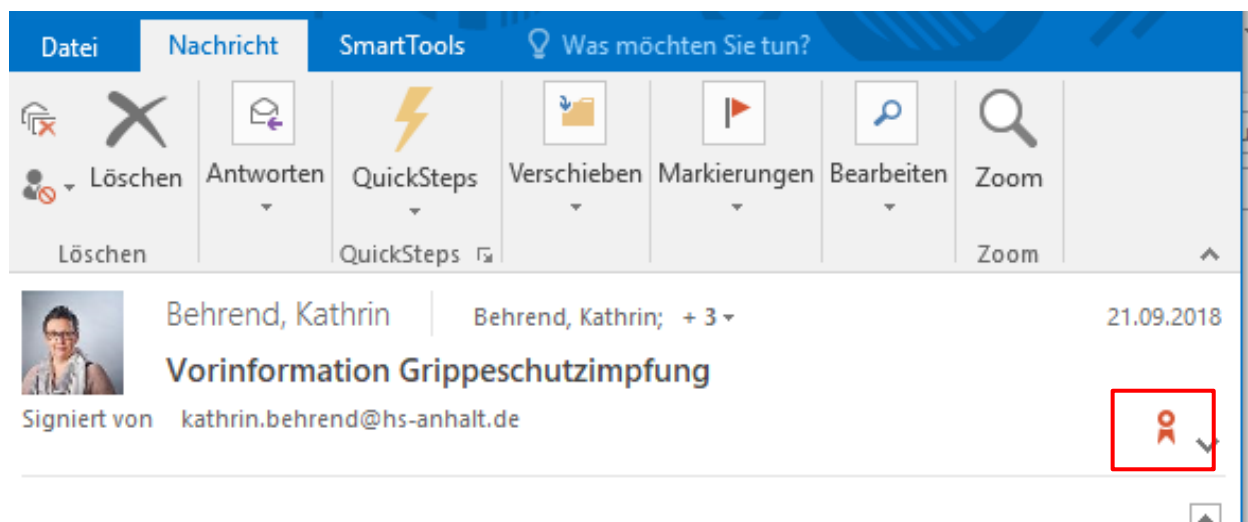
 ISC	Nutzerzertifikat beantragen und in Outlook einbinden	Dokument Nr.	Rev. Nr.
		ISC_VA_K06_03	06

Es sind bereits viele Daten sinnvoll eingetragen und übernommen worden. Speichern Sie.



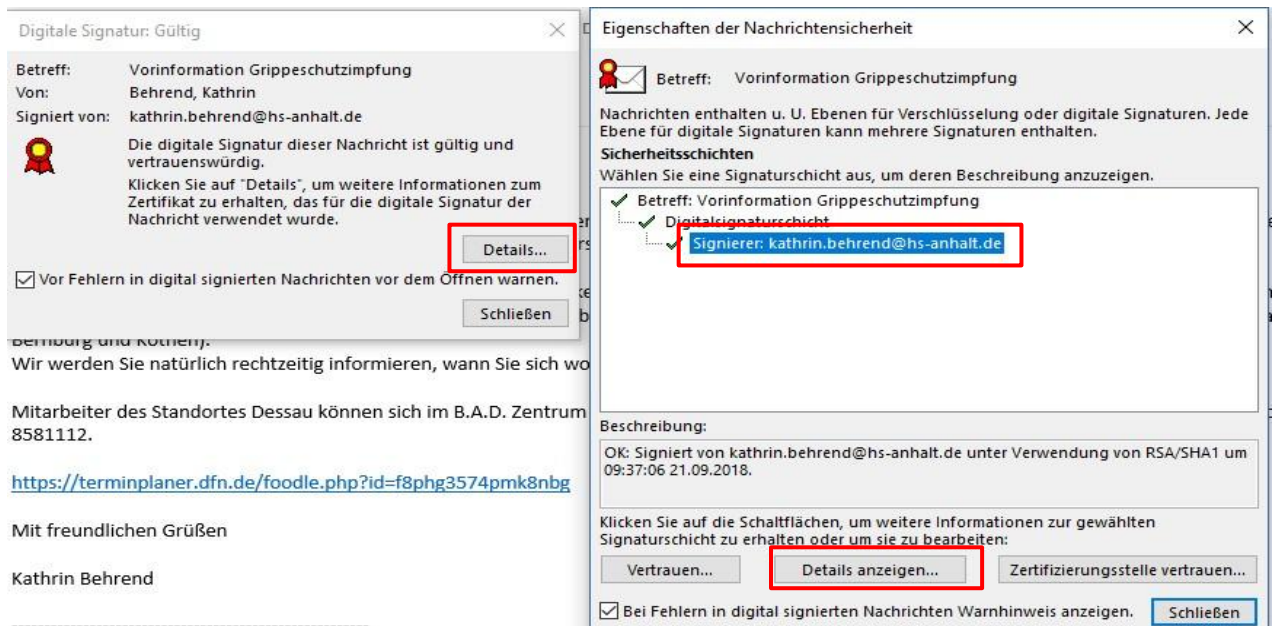
3.3.3 Zertifikat für Verschlüsselung besorgen

Hat dieser Absender seine E-Mail mit seinem Zertifikat signiert, können Sie daraus einfach das Zertifikat exportieren. In diesem Fall klicken Sie einfach auf das Siegel am rechten Ende im oberen Bereich der E-Mail, der Absender, Betreff usw. enthält.



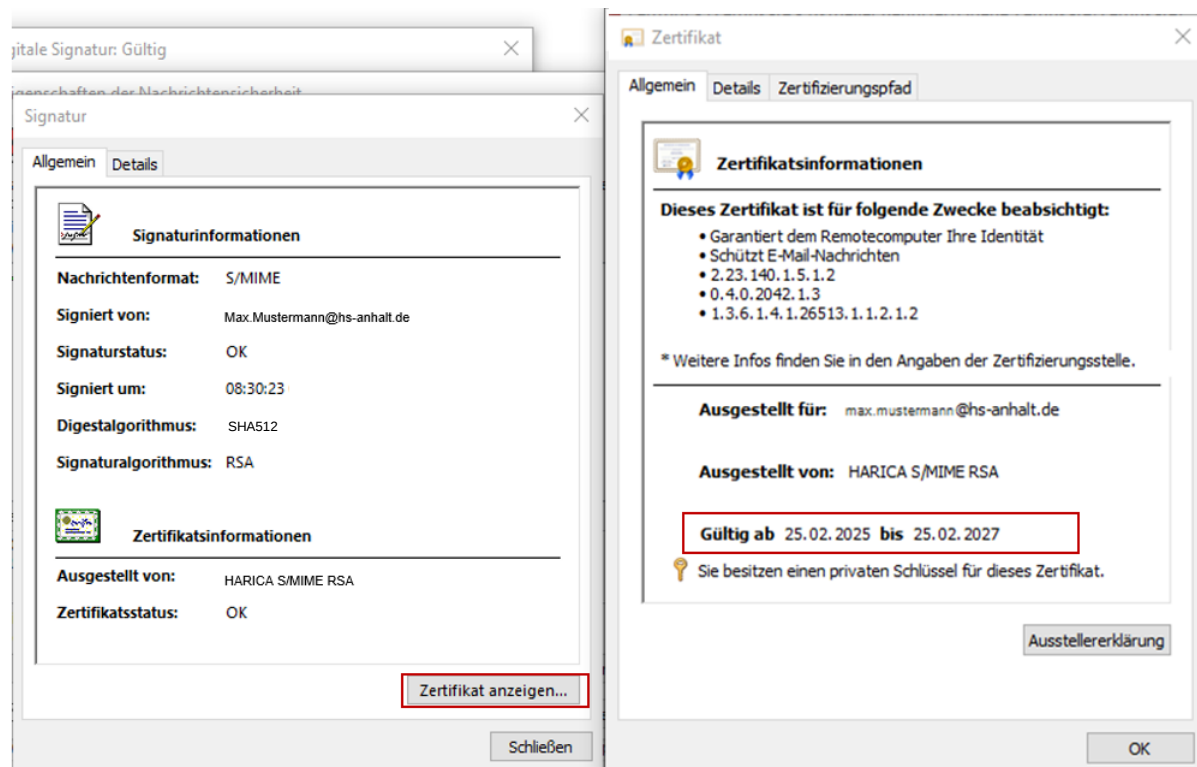
Es öffnet sich das Fenster „Digitale Signatur“. Klicken Sie auf „Details“.

 ISC	Nutzerzertifikat beantragen und in Outlook einbinden	Dokument Nr.	Rev. Nr.
		ISC_VA_K06_03	06



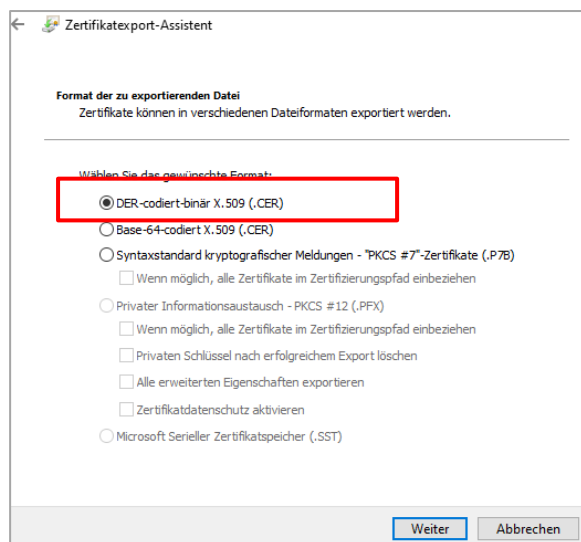
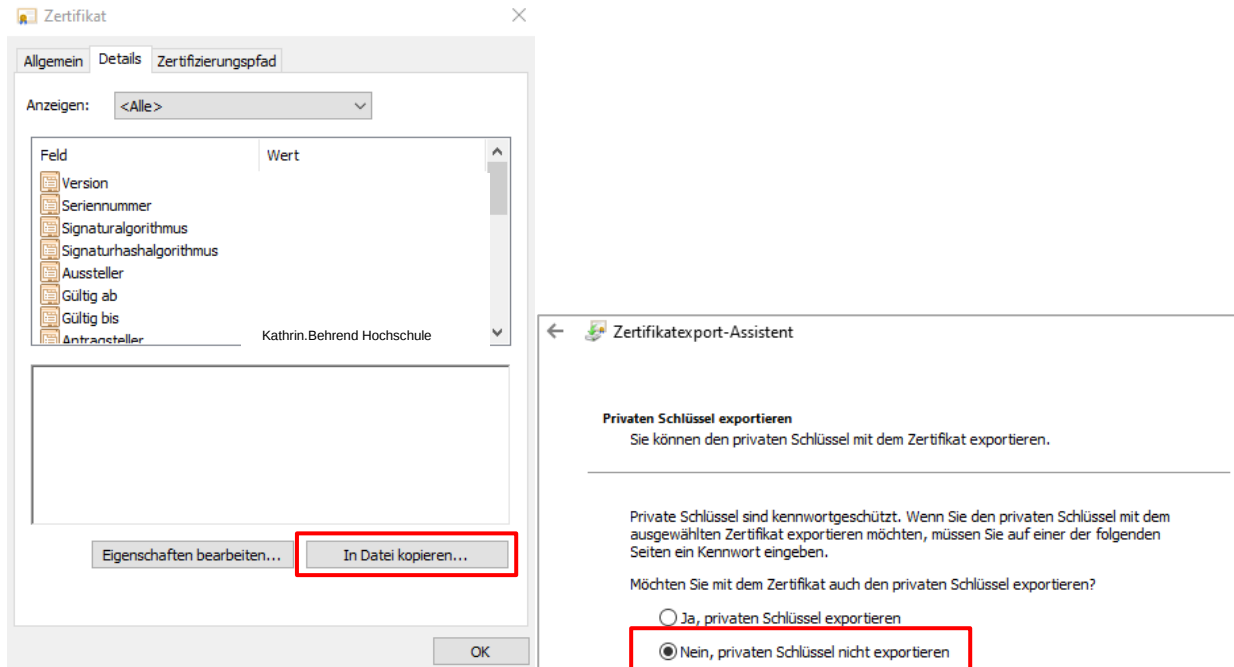
Im Detailfenster wählen Sie im Bereich Sicherheitsschichten den Signierer aus. Das ist der unterste Eintrag (hier schon blau unterlegt). Klicken Sie dann auf <Details anzeigen...>. In den Signaturdetails können Sie sich nun das Zertifikat anzeigen lassen. Wählen Sie dazu die Schaltfläche <Zertifikat anzeigen>

Auf dem ersten Register finden Sie Gültigkeitsdaten (ab – bis)



 ISC	Nutzerzertifikat beantragen und in Outlook einbinden	Dokument Nr.	Rev. Nr.
		ISC_VA_K06_03	06

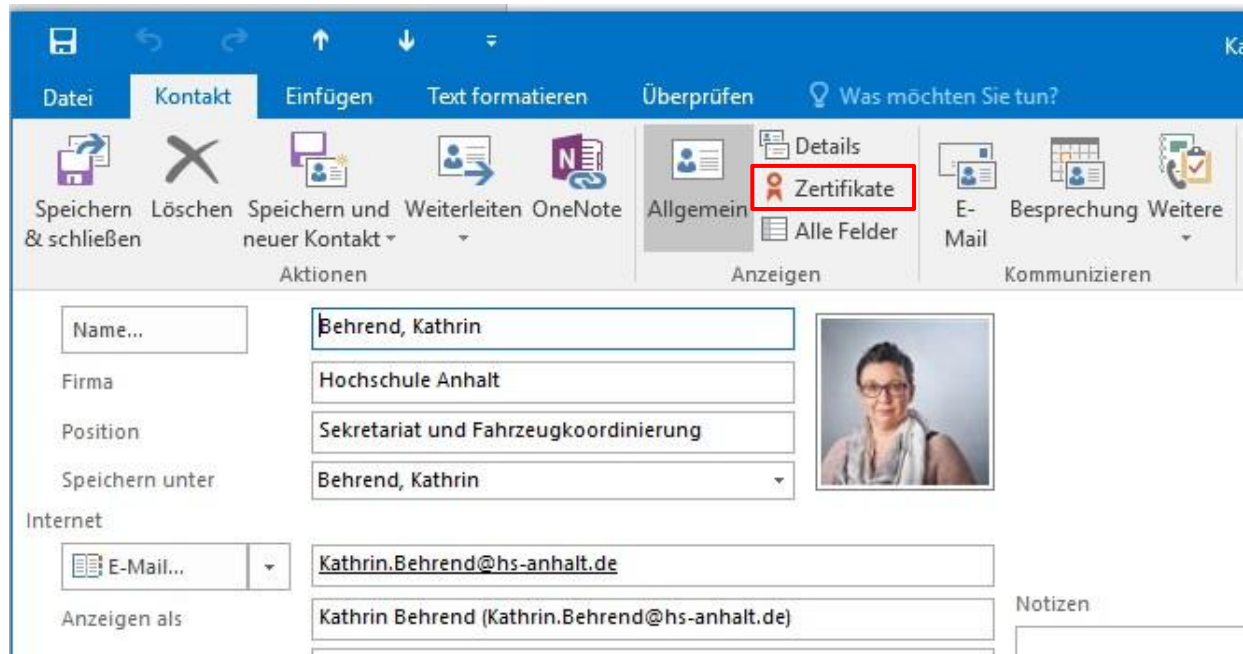
Wechseln Sie auf das Register „Details“. Hier können Sie das Zertifikat in eine Datei kopieren.



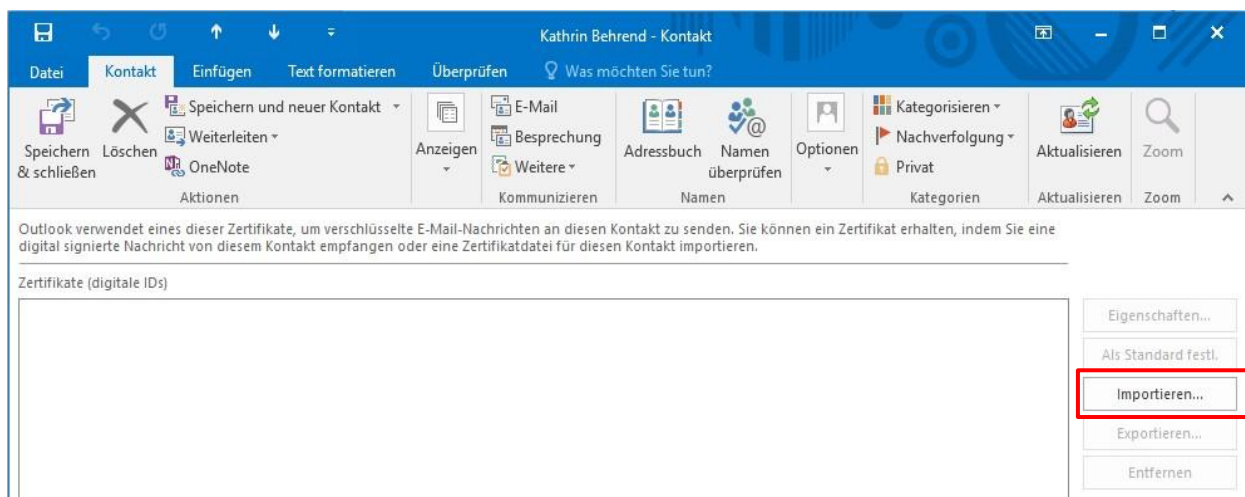
Lassen Sie das Format auf DER (.CER) stehen und speichern Sie die Datei entsprechend mit einem sprechenden Namen an einem temporären Ort. (z.B. C:\Temp)

Nun kehren Sie zum entsprechenden Kontakt zurück und öffnen ihn.

 ISC	Nutzerzertifikat beantragen und in Outlook einbinden	Dokument Nr.	Rev. Nr.
		ISC_VA_K06_03	06

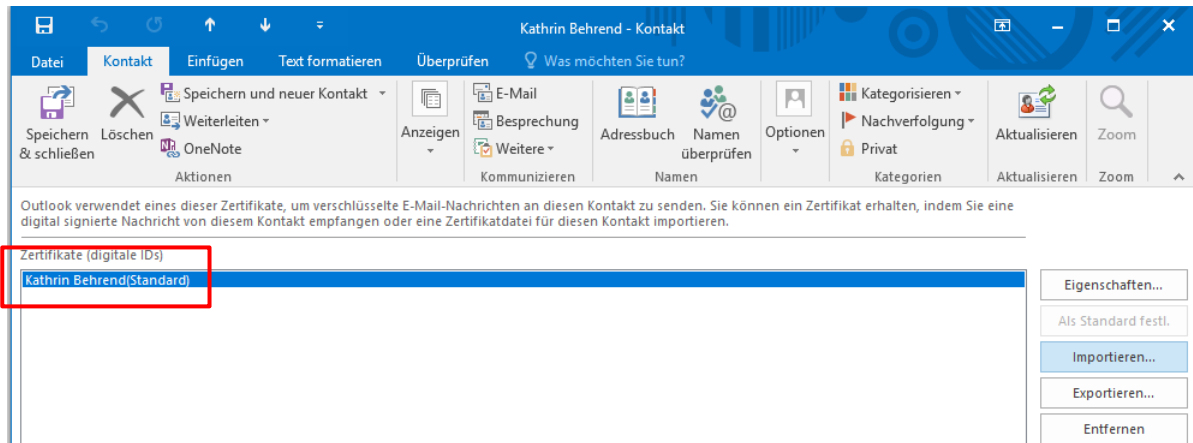


Sie finden dort eine Schaltfläche „Zertifikate“. Nach einem Klick darauf können Sie hier nun das eben exportierte Zertifikat importieren. Klicken Sie dazu rechts auf die Schaltfläche <Importieren>.



 ISC	Nutzerzertifikat beantragen und in Outlook einbinden	Dokument Nr.	Rev. Nr.
		ISC_VA_K06_03	06

Navigieren Sie zu der Datei und schließen Sie den Import ab.



Nun sehen Sie hier das Zertifikat. Es wird beim Versenden verschlüsselter E-Mails von hier entnommen. Speichern Sie den aktualisierten Kontakt. Er enthält jetzt dauerhaft das Zertifikat und es kann von überall aus mittels Outlook zum Versenden verschlüsselter E-Mails verwendet werden.

3.3.4 Verschlüsselte E-Mail an sich selbst

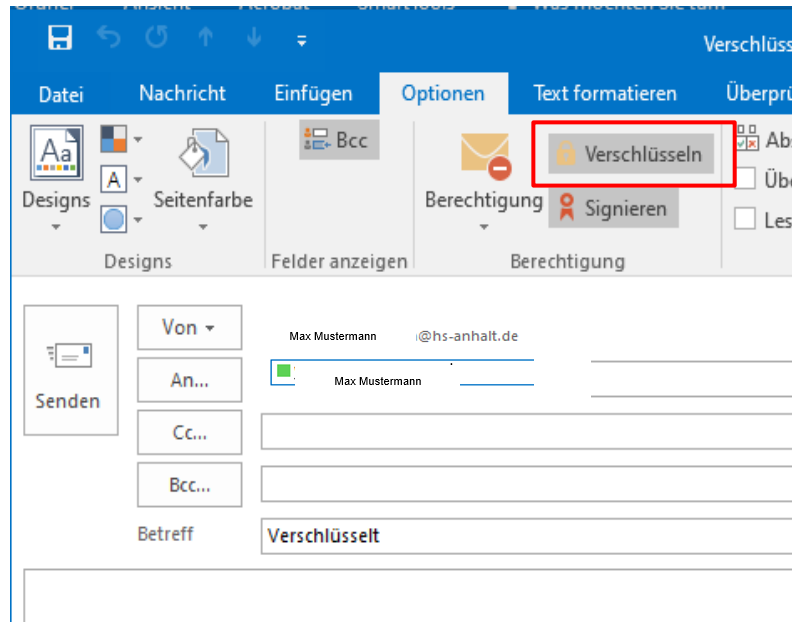
Nun sollten Sie sich selbst einmal eine verschlüsselte E-Mail schicken und ebenfalls prüfen, ob das richtige Zertifikat verwendet worden ist und ob die Verschlüsselung funktioniert.

Falls noch nicht geschehen, legen Sie sich einen Kontakt für sich selbst an. Siehe dazu Abschnitt 3.3.2. Fügen Sie ebenfalls wie unter 3.3.3 beschrieben Ihr Zertifikat in Form einer *.cer-Datei (also nur den öffentlichen Teil Ihres Zertifikates) diesem Kontakt hinzu.

Gemäß der vorgenommenen Einstellung muss aber innerhalb der neuen E-Mail auf dem Register „Optionen“ jeweils separat die Verschlüsselung eingeschaltet werden. Beginnen Sie also eine neue E-Mail und wechseln Sie auf das Register „Optionen“.

 ISC	Nutzerzertifikat beantragen und in Outlook einbinden	Dokument Nr.	Rev. Nr.
		ISC_VA_K06_03	06

Dort müssen Sie nun jeweils auf die Schaltfläche <Verschlüsseln> klicken.

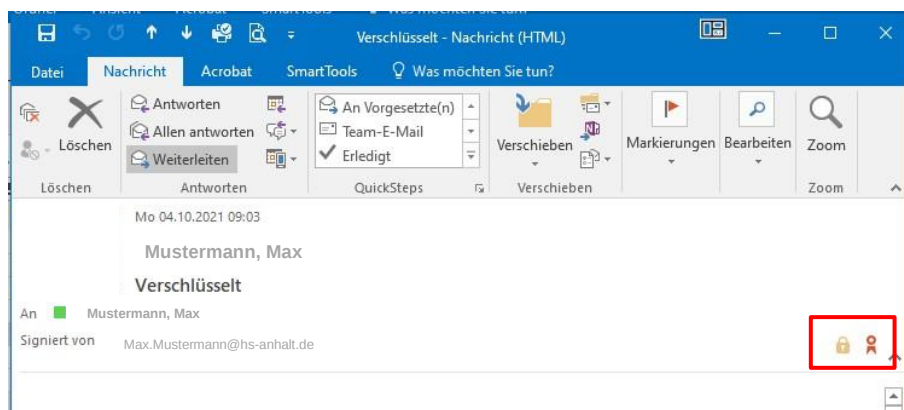


Vervollständigen Sie die E-Mail und senden Sie sie ab.

Eine verschlüsselte E-Mail erkennen Sie jeweils am gelben, geschlossenen Schloss. Hier im Posteingang am Zeilenanfang in der Spaltenpalette:



Und auch bei der geöffneten E-Mail ist das gelbe Schloss zu sehen. Am Zeilenende finden Sie das Siegel-Symbol und das gelbe Schloss.



 ISC	Nutzerzertifikat beantragen und in Outlook einbinden	Dokument Nr.	Rev. Nr.
		ISC_VA_K06_03	06

Das Verschlüsselungszertifikat prüfen Sie durch Klick auf das Schloss-Symbol (nicht das Siegel). Prüfen Sie das bitte genauso, wie im Abschnitt 3.2 für die signierte E-Mail beschrieben.

4 Überarbeitung

Diese Benutzeranleitung wird regelmäßig auf ihren Revisionsbedarf überprüft und angepasst. Darüber hinaus werden wichtige Änderungen, z.B. aus aktuellem Anlass, sofort eingearbeitet.

5 Ablage und Archivierung

Dieses Dokument wird beim IT-Service-Center aufbewahrt.

Hinsichtlich der Archivierung gelten die Bestimmungen der HSA_VA_F02_00 „Archivierung von Daten und Dokumenten“.

6 Änderungshistorie

Revision	
Revision 01 – Neuerstellung (07.02.2022)	
Rev. 02	06.11.2023: Beantragung des Zertifikats bei einem anderen Anbieter
Rev. 03	07.02.2024: Bilder aktualisiert
Rev. 04	05.03.2025: Überarbeitung aufgrund von Anbieterwechsel
Rev. 05	02.09.2025: Überarbeitung/Fehlerbereinigung
Rev. 06	17.09.2025: Fehlerbereinigung

7 Überprüfung und Genehmigung

Erstellung / formale Prüfung:		
Position: Mitarbeiter ISC		
Name: Susanne Nitschke	Datum: 17.09.2025	Unterschrift:
Freigegeben: entfällt		
Position:		
Name:	Datum:	Unterschrift:
Genehmigt: entfällt		

 ISC	Nutzerzertifikat beantragen und in Outlook einbinden	Dokument Nr.	Rev. Nr.
		ISC_VA_K06_03	06

Position:

Name:

Datum:

Unterschrift: