

HAW DFN - Mail Zertifikate

Hierbei handelt es sich um ein Zertifikat für die Signierung von E-Mails.

Zertifikate Anfordern

Nachfolgende Anleitung hilft Ihnen dabei sich ein Zertifikat für die Signierung und Verschlüsselung Ihrer HAW E-Mails zu beantragen. Weiterführende Leitfäden zeigen Ihnen im Anschluss wie Sie dieses Zertifikat in ihrem jeweiligen Betriebssystem und E-Mail Programm einrichten.

Hinweis

Merken Sie sich mit welchem Browser und auf welchem Rechner Sie das Zertifikat beantragt haben! Sie werden später nur mit diesem Browser auf diesem Rechner in der Lage sein das Zertifikat von der DFN herunterzuladen!

Führen Sie die folgenden Schritte an einem Computer in der HAW durch. Sie benötigen Zugriff auf einen Drucker!

1. Rufen Sie in ihrem Browser die folgende Adresse auf:
<https://pki.pca.dfn.de/haw-hamburg-ca/pub> . Sie gelangen auf die PKI (Private Key Infrastructure) Seite des Deutsches Forschungsnetzes (DFN).
2. Wählen Sie hier den Menüpunkt „Nutzerzertifikat,“



The screenshot shows the web interface for requesting certificates. At the top left is the logo of Hochschule für Angewandte Wissenschaften Hamburg (HAW). At the top right is the DFN (Deutsches Forschungsnetz) logo. Below the logos is a navigation menu with the following items: **Zertifikate**, CA-Zertifikate, Gesperrte Zertifikate, Policies, Hilfe, Beenden. Below this menu is a sub-menu with: Nutzerzertifikat, Serverzertifikat, Zertifikat sperren, Zertifikat suchen. The main content area has a heading: **Willkommen zur DFN-PKI Schnittstelle für Nutzer und Administratoren - Zertifikate**. Below the heading is the text: "Hier können Sie Zertifikate beantragen, sperren lassen und nach Zertifikaten suchen." There are two bullet points: "Bitte importieren Sie alle CA-Zertifikate in Ihren Browser über die Registerkarte 'CA-Zertifikate'." and "Bitte wählen Sie aus den Registerkarten eine Funktion aus." At the bottom of the main content area, it says: "Kontaktinformationen für Rückfragen finden Sie unter 'Hilfe'". In the bottom right corner of the page, there is a link for "Impressum".

3. Füllen Sie das nun erscheinende Formular mit Ihren Daten aus (Hinweis: Beim Namensfeld sind keine Umlaute möglich). Notieren Sie sich die PIN an einem sicheren Ort. Sie benötigen diese später ggf. um Ihr Zertifikat zu sperren, sollten Sie z.B. ein mobiles Gerät verlieren. Setzen Sie abschließend noch die beiden Haken, nachdem Sie sowohl die Informationen für Zertifikatinhaber, wie auch die Hinweise zur Veröffentlichung des Zertifikates gelesen haben. Klicken Sie nun auf „Weiter“ .:

Hochschule für Angewandte Wissenschaften Hamburg
Hamburg University of Applied Sciences

DFN
Deutsches
Forschungsnetz

Zertifikate CA-Zertifikate Gesperrte Zertifikate Policies Hilfe Beenden

Nutzerzertifikat Serverzertifikat Zertifikat sperren Zertifikat suchen

Nutzerzertifikat beantragen

Bitte geben Sie Ihre Daten ein. Felder mit einem Stern (*) müssen ausgefüllt werden.

Zertifikatdaten

E-Mail * max.mustermann@haw-hamburg.de

Name * Max Mustermann

Geben Sie hier Ihren Vor- und Nachnamen ein. Für Gruppenzertifikate stellen Sie das Kürzel "GRP:"
voran. Verwenden Sie keine Umlaute.

Abteilung

Wenn Sie hier eine Abteilung angeben, wird diese in den Zertifikatnamen aufgenommen.

Weitere Angaben

Diese Angaben werden nicht in das Zertifikat übernommen.

PIN (Mindestens 8 beliebige Zeichen) *

Nochmalige Eingabe der PIN zur Bestätigung *

Die PIN wird von Ihnen benötigt, wenn Sie Ihr Zertifikat sperren wollen. Bitte notieren Sie sich die PIN.

Ich verpflichte mich, die in den Informationen für Zertifikatinhaber aufgeführten
Regelungen einzuhalten. *

Ich stimme der Veröffentlichung des Zertifikats mit meinem darin enthaltenen Namen
und der E-Mail-Adresse zu. *

Sie können diese Einwilligung jederzeit mit Wirkung für die Zukunft durch eine E-Mail an pki@dfn.de
widerrufen.

Weiter

Impressum

4. Sie werden aufgefordert Ihre Daten nochmals zu überprüfen. Sind die Daten korrekt klicken Sie auf „Bestätigen“,, andernfalls auf „ändern“. Stimmt Ihre Mail-Adresse nicht überein, wird das Zertifikat später nicht funktionieren!

Hochschule für Angewandte Wissenschaften Hamburg
Hamburg University of Applied Sciences

DFN
Deutsches
Forschungsnetz

Zertifikate CA-Zertifikate Gesperrte Zertifikate Policies Hilfe Beenden

Nutzerzertifikat Serverzertifikat Zertifikat sperren Zertifikat suchen

Nutzerzertifikat beantragen - Bestätigen

Bitte überprüfen Sie die Daten.

Zertifikatdaten

E-Mail max.mustermann@haw-hamburg.de

Name Max Mustermann

Abteilung

Weitere Angaben

Veröffentlichen Ja

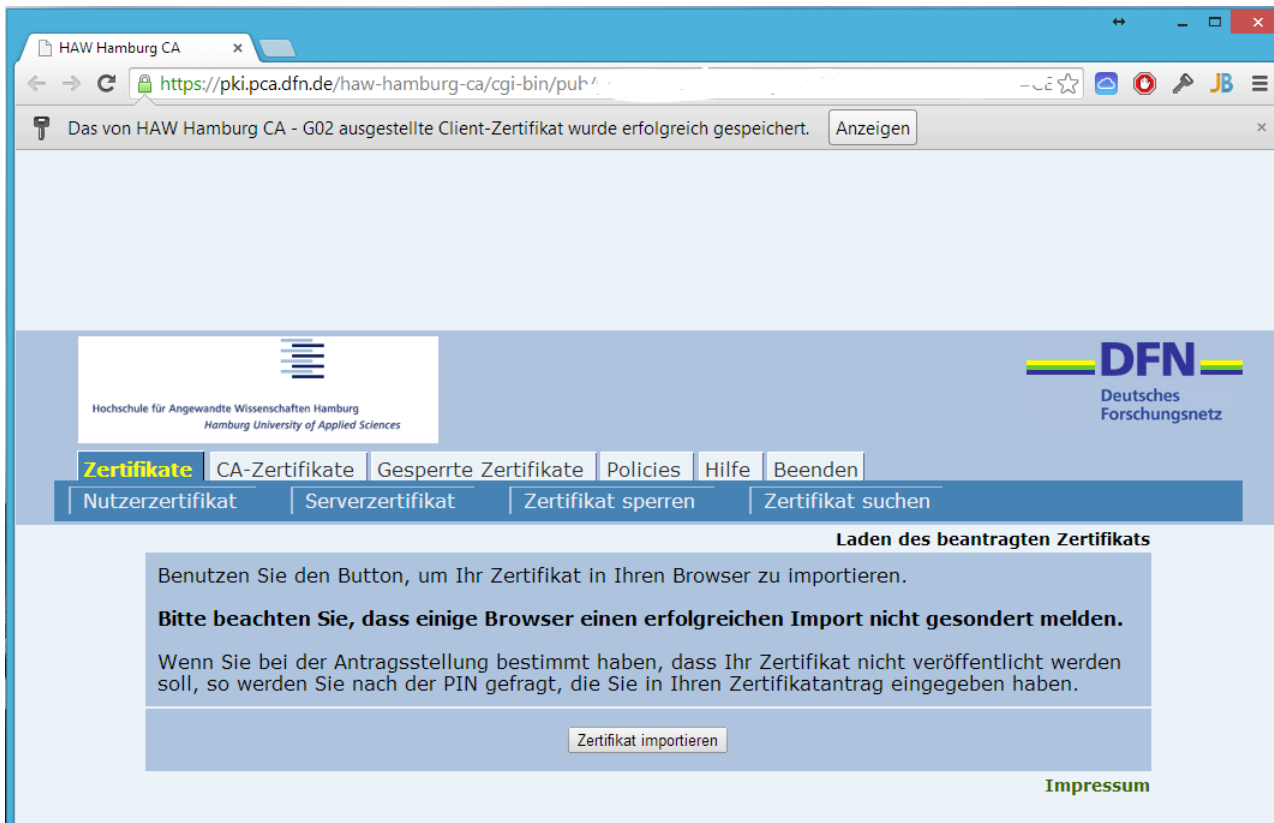
Ändern Bestätigen

Impressum

5. Sie werden nun aufgefordert Ihren Antrag auszudrucken. Mit einem Klick auf „Zertifikatantrag anzeigen“,, lädt Ihr Browser eine PDF Datei herunter bzw. öffnet diese im Browser oder dem jeweils installierten PDF Betrachter. Drucken Sie diesen Antrag aus.:

6. Schreiben Sie nun eine E-Mail an die Adresse [pki\(@\)haw-hamburg.de](mailto:pki(@)haw-hamburg.de) um einen Termin mit Jörg Kottusch, Olaf Boneß oder Alexander Oswald zu vereinbaren. Bringen Sie zu diesem Termin Ihren Zertifikatsantrag sowie Ihren Personalausweis mit. Einer der drei Herren wird Ihre Identität verifizieren, den Antrag bestätigen und Sie haben Ihr Zertifikat erfolgreich beantragt.
7. Nachdem Sie Ihr Zertifikat erfolgreich beantragt haben, erhalten Sie eine E-Mail von der Adresse [zertifikate\(@\)haw-hamburg.de](mailto:zertifikate(@)haw-hamburg.de). Diese enthält unter 2. einen Link über welchen Sie Ihr eigenes Zertifikat herunterladen können:

8. Der Link führt Sie wieder zur DFN Seite, auf der Sie bitte auf „Zertifikat importieren“ klicken. :



9. Es öffnet sich nun je nach Browser ein Fenster (im Bild oben ist das Verhalten von Chrome zu sehen), in welchem Ihnen mitgeteilt wird, dass das Zertifikat in Ihren Browser bzw. in Ihr System importiert wurde.

Hinweis

Je nach verwendetem Browser und Betriebssystem, wird das Zertifikat an dieser Stelle verschiedentlich behandelt. Nachfolgend eine Tabelle zum Speicherort des Zertifikates für die jeweilige Browser / System Kombination:

	Windows	Mac OS X	Linux
Firefox	Interner Browserspeicher	Interner Browserspeicher	TBA
Chrome	Windows Zertifikatspeicher	Schlüsselbundverwaltung	TBA
Internet Explorer	Windows Zertifikatspeicher	-	-
Safari	-	Schlüsselbundverwaltung	-

Zertifikate importieren

Mac - in Schlüsselbundverwaltung importieren

Um Ihr Zertifikat in Mac OS X benutzen zu können, müssen Sie dieses in die „Schlüsselbundverwaltung“ importieren.

1. Starten Sie die Anwendung „Schlüsselbundverwaltung“, in dem Sie sie über Spotlight suchen:



2. Klicken Sie im Menü „Ablage“ auf den Punkt „Objekt importieren“. Wählen Sie Ihr privates Zertifikat (.pfx Datei) und klicken Sie auf „Öffnen“. Als Ziel-Schlüsselbund können Sie „Anmeldung“ eingestellt lassen.
3. Geben Sie nun das Kennwort für Ihren privaten Schlüssel ein und bestätigen Sie mit Klick auf „Ok“.
4. Das Zertifikat ist nun erfolgreich importiert. Das Programm Apple Mail sollte das Zertifikat automatisch finden. Für eine Verwendung in Outlook 2011, folgen Sie bitte dem entsprechenden Dokument.

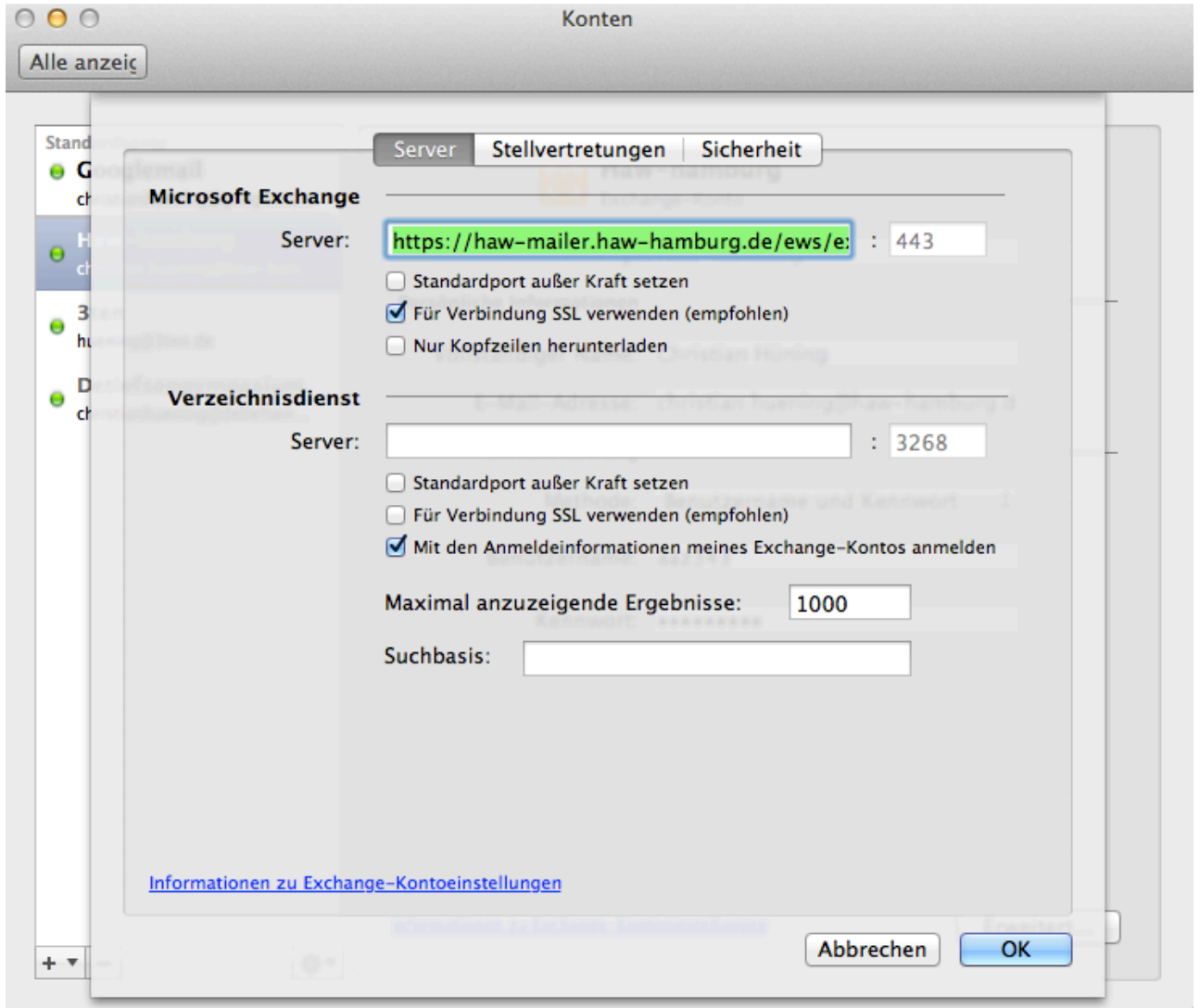
Apple Mail

Ist das Zertifikate erfolgreich in der [Schlüsselbundverwaltung importiert](#) worden, nutzt Apple Mail dieses automatisch. Es sind keine weiteren Schritte erforderlich.

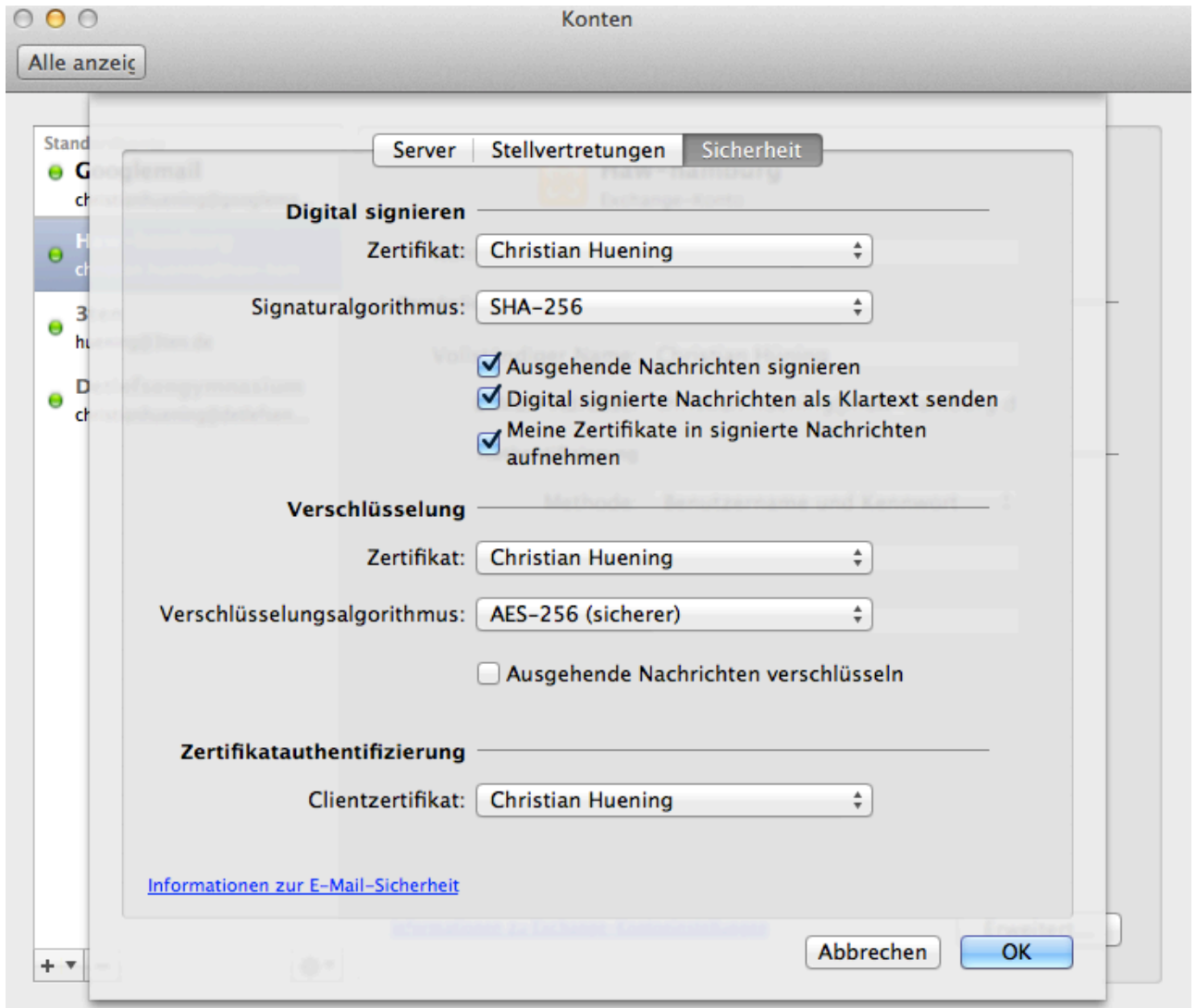
Outlook / Mac

Zunächst muss das Zertifikat in die [Schlüsselbundverwaltung importiert](#) importiert werden. Beachten Sie dazu die entsprechende Anleitung. Ist dies geschehen, gehen Sie wie folgt vor um Ihr Zertifikat in Outlook 2011 for Mac zu installieren:

1. Nummerierter ListenpunktWählen Sie „Konten“ in den Outlook Einstellungen
2. Wählen Sie hier Ihr HAW Konto aus und klicken Sie auf den Button „Erweitert“



3. Wählen Sie den Tab „Sicherheit“ aus

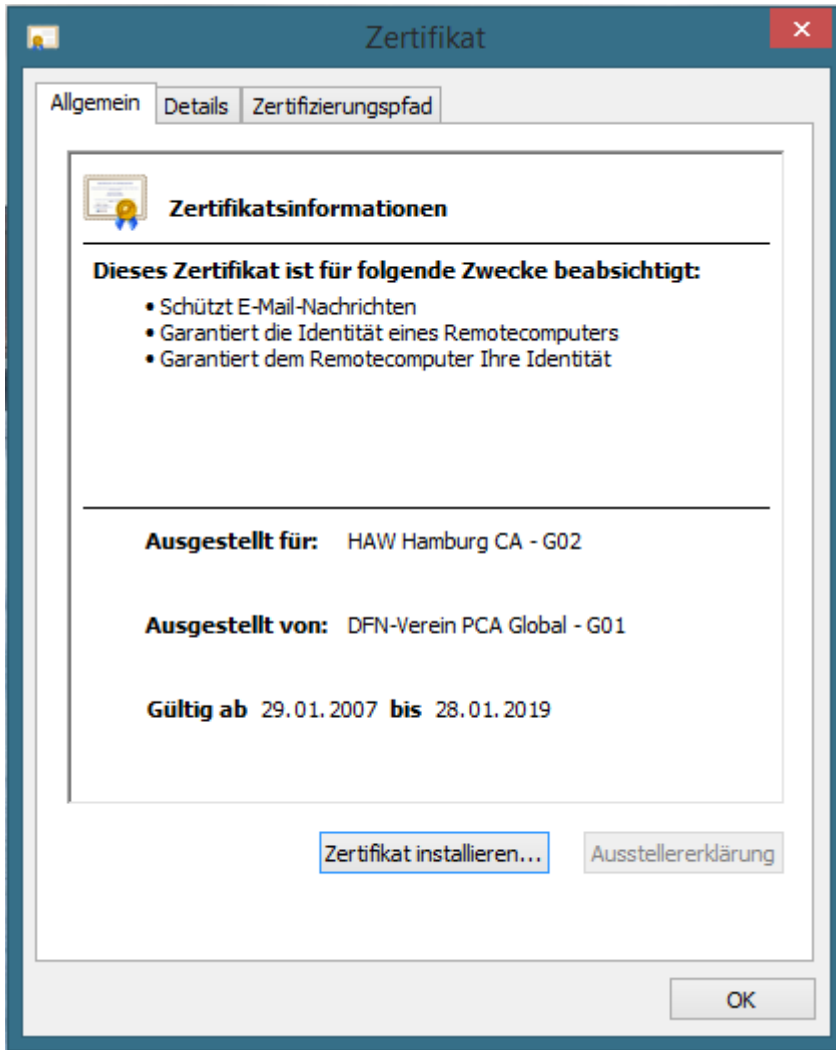


4. Wählen Sie in den Auswahllisten der Option "Zertifikat" bei „Digital signieren“ und „Verschlüsselung“ Ihren Namen aus. Dahinter verbirgt sich Ihr Zertifikat aus der Schlüsselbundverwaltung
5. Verfahren Sie ebenso für die Option „Clientzertifikat“ unter „Zertifikatauthentifizierung“.
6. Fertig! Sie haben Ihr DFN Zertifikat erfolgreich in Ihrem Outlook hinterlegt. Ausgehende E-Mail werden nun digital signiert und ggf. auch verschlüsselt

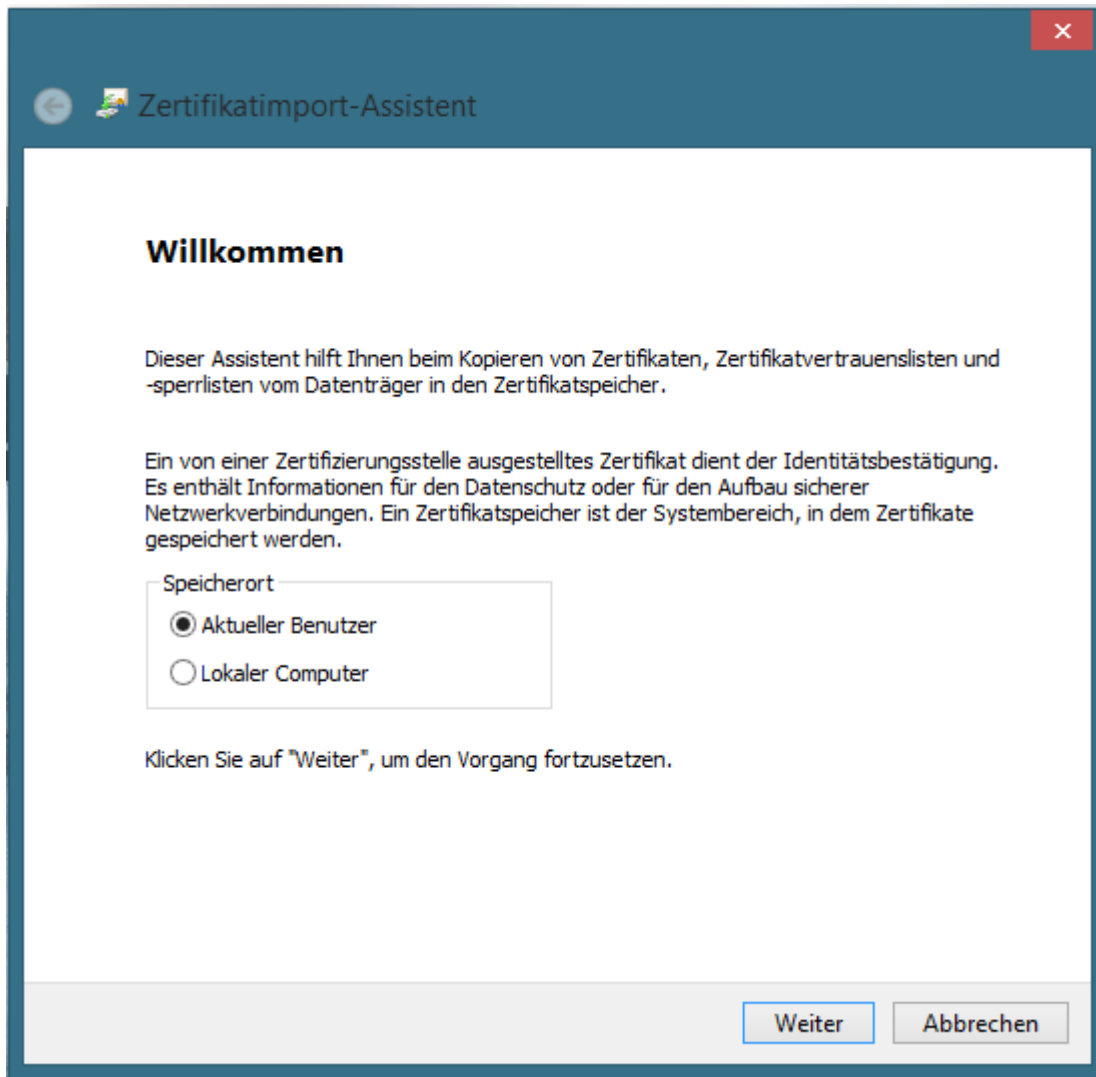
Windows 7 & 8 - in Zertifikatsspeicher importieren

Um Ihr Zertifikat in Windows benutzen zu können, müssen Sie dieses in den Zertifikatsspeicher von Windows importieren.

1. Doppelklicken Sie auf die Datei mit Ihrem persönlichen Zertifikat. Das Zertifikat öffnet sich. Klicken Sie nun auf „Zertifikat installieren“



2. Der „Zertifikatimport-Assistent“ öffnet sich. Klicken Sie auf „Weiter“.



3. Bestätigen Sie die Auswahl der Datei im nächsten Fenster mit „Ok“.
4. Geben Sie im nächsten Schritt das Kennwort zu Ihrem Zertifikat ein und setzen die Haken, wie im Bild ersichtlich.
5. Belassen Sie im nächsten Fenster die Voreinstellung und bestätigen Sie die Abfrage nach dem Speicherort per Klick auf „Ok“.
6. Abschließend klicken Sie noch auf „Fertigstellen“ und auf „Ok“ und somit haben Sie Ihr Zertifikat erfolgreich in den Windows-Zertifikatespeicher importiert.

From:

<https://userdoc.informatik.haw-hamburg.de/> - **Dokumentations-Wiki des Departments Informatik der HAW Hamburg**

Permanent link:

https://userdoc.informatik.haw-hamburg.de/doku.php?id=docu:dfn_zertifikat

Last update: **2017/07/19 08:33**

