Outlook für Windows - Signieren und Verschlüsseln von E-Mails

Es ist zwingend erforderlich, als Browser den Firefox zu verwenden.

Für den Zeitraum, vom Stellen des Antrags bis zum Download der P12-Datei ist es wichtig, den Browser-Verlauf und -Cache nicht zu leeren. Dazu gehen Sie bitte in der Firefox-Menüleiste auf Extras Einstellungen Datenschutz & Sicherheit 1. *Cookies und Website-Daten* bei "Cookies und Website-Daten beim Beenden von Firefox löschen" das Häkchen herausnehmen und 2. *Chronik* "Firefox wird eine Chronik ..." bitte "anlegen" auswählen. Sollte ein Hacken grau hinterlegt sein und somit nicht verändert werden können, kann die Portable Variante des Firefox eine Alternative für die Beantragung darstellen.

Allgemeines zum Zertifikat

Jeder E-Mail Client möchte seine Zertifikate an einem anderen Speicherort haben. Outlook verwendet den Zertifikatsspeicher des Betriebssystems (=Internet Explorer). Thunderbird hingegen hat einen in die Anwendung integrierten Zertifikatsspeicher.

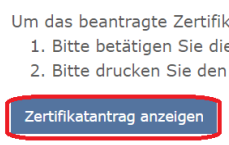
Für den erfolgreichen Import muss das Zertifikat als p12-Datei vorliegen. Sofern Sie bereits zuvor signierte und verschlüsselte E-Mails via Thunderbird versendet habe, können Sie das Zertifikat über diese Anleitung exportieren:

http://www.ku.de/fileadmin/1902/pdf/installation/Emails_verschluesseln_und_signieren_ik114.pdf (Seite 14: Sicherung des Zertifikats samt privatem Schlüssel und Export)

Antragstellung

- https://pki.pca.dfn.de/dfn-pki/dfn-ca-global-g2/3200 bitte unbedingt in Firefox anwenden
- Zertifikate
- Passwort festlegen und notieren (= Cache-Passwort)
- Neues Zertifikat beantragen
- die rot markierten Feld entsprechend ausfüllen - **keine Umlaute!**
- bei "Namensraum" auswählen zwischen ... L= Eichstaett ... und ... L= Ingolstadt ...

- es ist dringend angeraten, "Optional: Ich stimme der Veröffentlichung des Zertifikates ... zu" anzukreuzen. Wenn Sie der Veröffentlichung des Zertifikates nicht zustimmen, steht Ihr Zertifikat nicht im öffentlichen Verzeichnisdienst und Sie können selbst entscheiden, an wen Sie Ihren öffentlichen Schlüssel weitergeben möchten.
- Weiter
- auf der folgenden Seite werden Ihre Stammdaten angezeigt

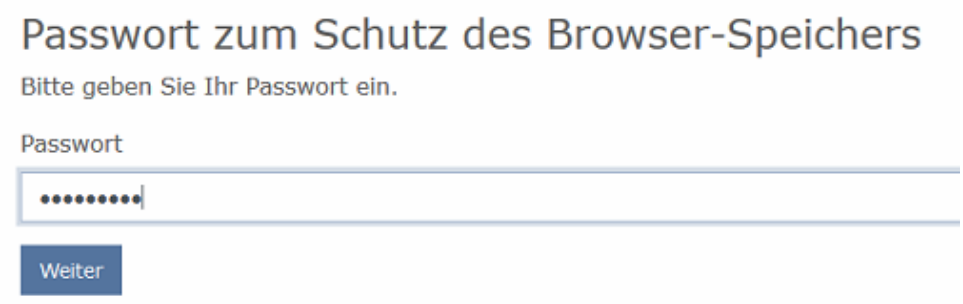


- über "Zertifikatantrag anzeigen" das nun erstellte PDF ausdrucken und mit Ihrem Personalausweis oder Reisepass persönlich beim Teilnehmerservice (= Sekretariat des URZ in Eichstätt, Zimmer eO-109 oder in Ingolstadt Herr Bernhard Brandel, Zimmer HB-204) nach vorheriger telefonischer Voranmeldung vorlegen.
- nachdem Ihr Antrag vom Teilnehmerservice geprüft und bewilligt wurde, erhalten Sie eine Mail vom DFN.

Zertifikat vom DFN herunterladen

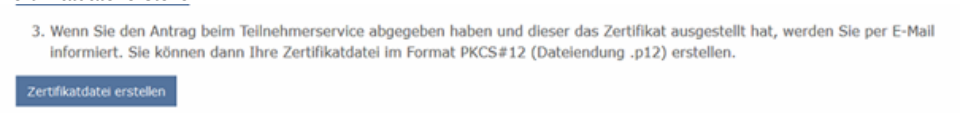
- aus der E-Mail vom DFN folgenden Link auswählen Nur im Firefox! Sollte am PC der Browser Firefox nicht standardmäßig eingerichtet sein, bitte den Link per Hand in den Firefox kopieren.

- Passwort der Antragstellung eingeben (Ihr Cache-Passwort, s. o.)

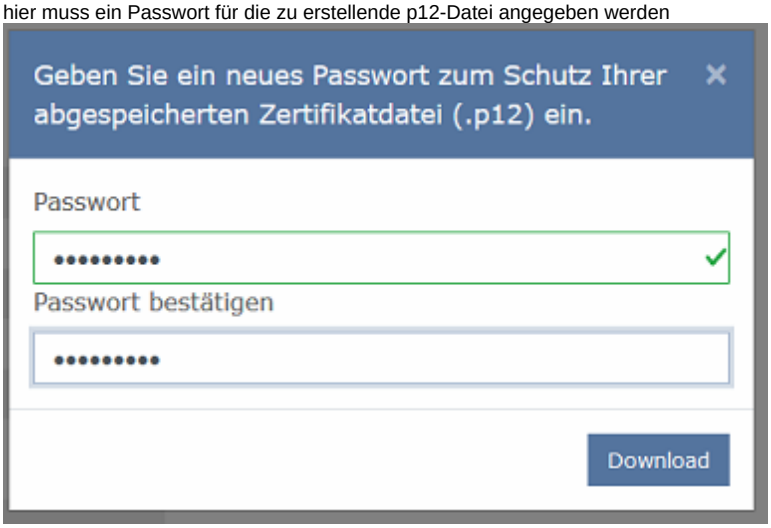


- neuesten Antrag auswählen

- Zertifikatdatei erstellen:



- hier muss ein Passwort für die zu erstellende p12-Datei angegeben werden

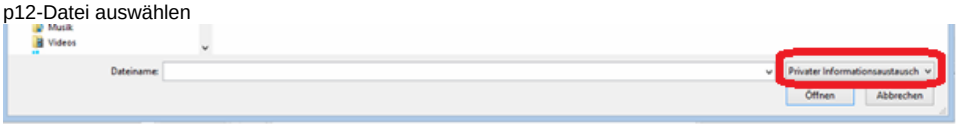


- Datei an einem sicheren Ort speichern und aufbewahren

Einbinden der Zertifikate in den Zertifikatspeicher von Windows

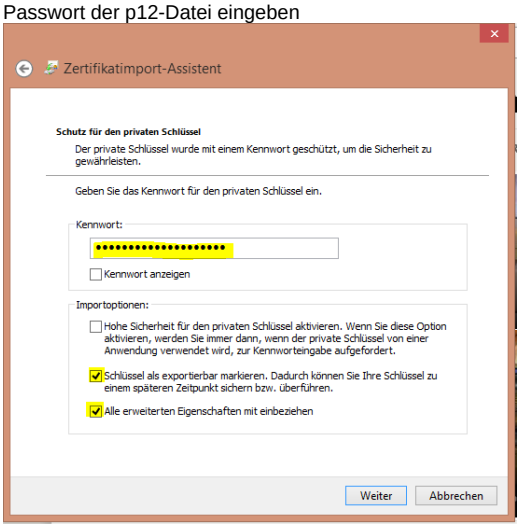
1. Internet Explorer
2. Extras
3. Internetoptionen
4. Inhalte

5. Zertifikate
6. unter dem Tab "Eigene Zertifikate" auf Importieren...
7. Weiter
8. Durchsuchen
9. p12-Datei auswählen

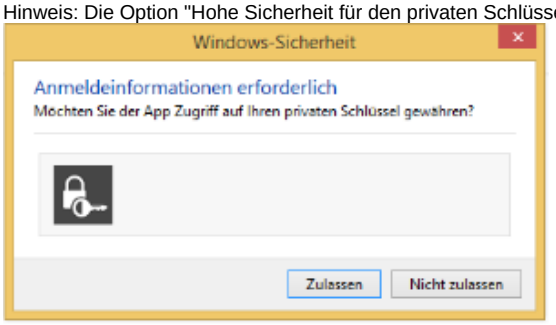


ggf. das Dateiformat auf p12 ändern

10. Passwort der p12-Datei eingeben



11. Hinweis: Die Option "Hohe Sicherheit für den privaten Schlüssel aktivieren..." hat folgende Meldung beim Versenden von Nachrichten zur Folge:



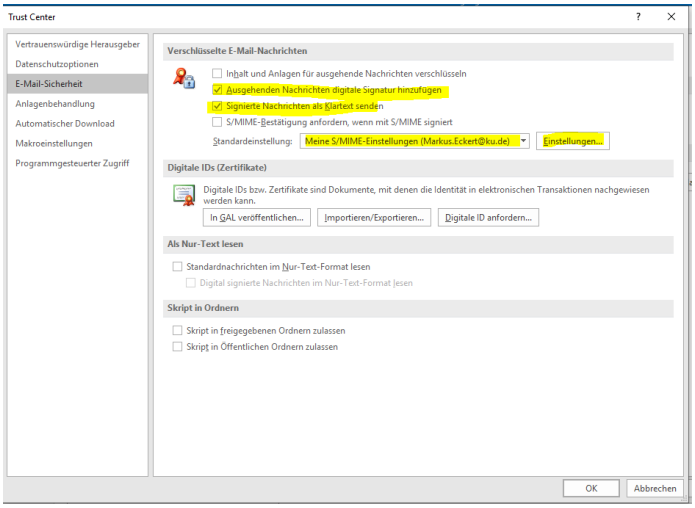
12. Weiter
13. Weiter
14. Fertig stellen

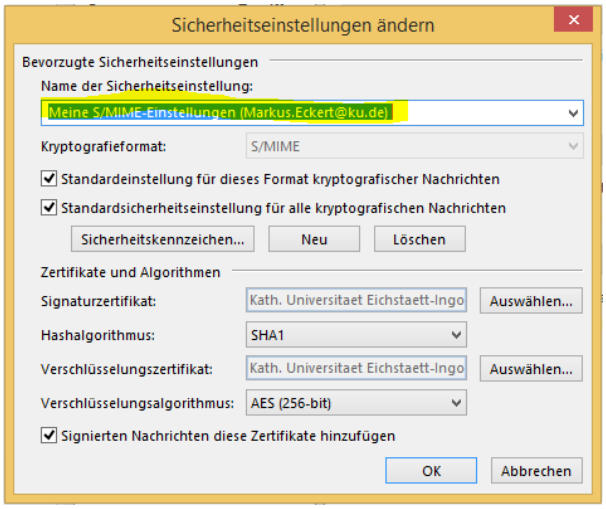
- OK - Fertig !
- Für eine erhöhte Sicherheit kann über die Schalfläche "Sicherheitsstufe... " diese von Mittel auf Hoch gestellt werden.

Konfiguration von Outlook

Globales hinterlegen des Zertikates

1. Datei
2. Optionen
3. Trust Center
4. Einstellungen für das Trust Center
5. E-Mail-Sicherheit

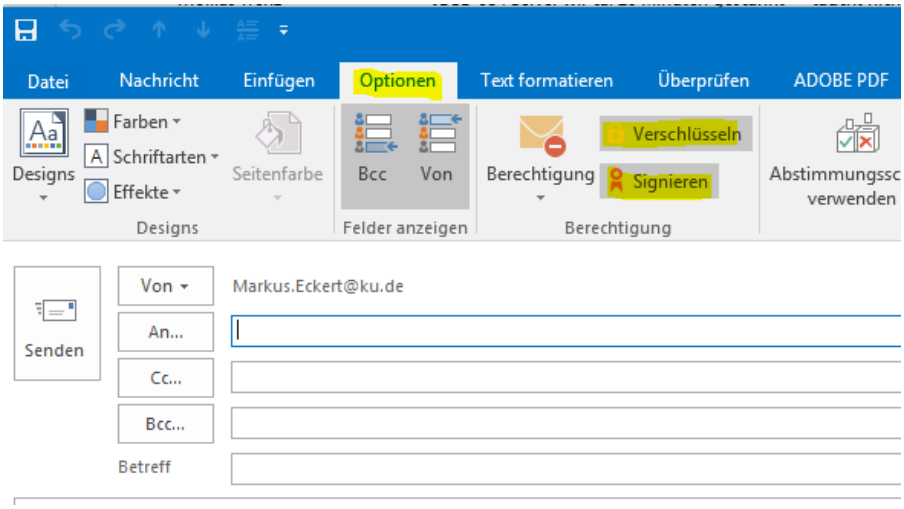
6. Einstellungen: 

prüfen ob beide Hacken gesetzt sind
7. Zertifikat auswählen: 

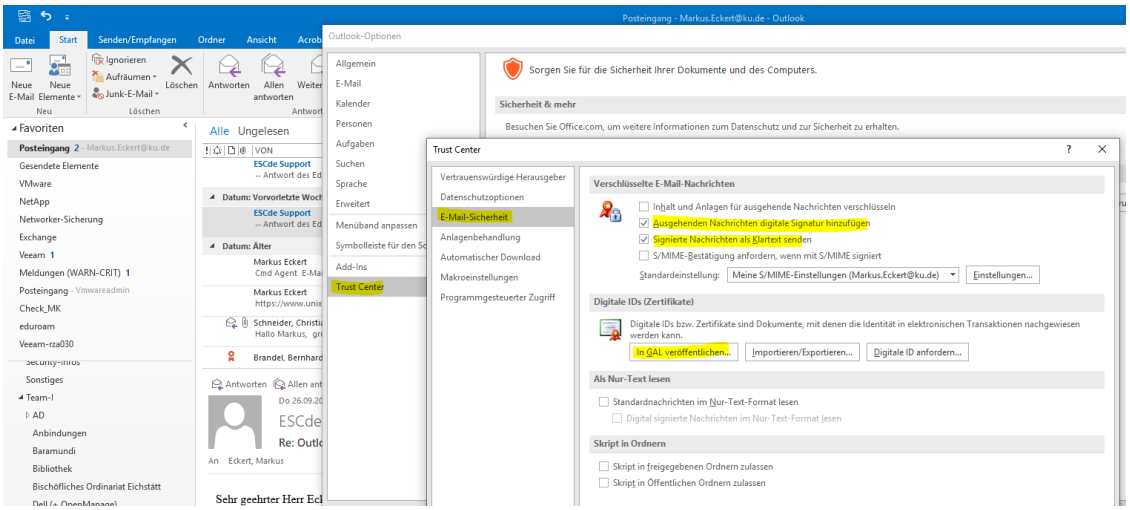
8. OK

Senden einer verschlüsselt und signierten E-Mail

Unter dem Tab "Optionen" (im Kontext einer neuen E-Mail) verbergen sich die Schaltflächen für das Verschlüsseln und Signieren von E-Mails:



Über den Punkt "Ausgehenden Nachrichten digitale Signatur hinzufügen" unter --- Datei - Optionen - Trust Center - Einstellungen für das Trust Center - E-Mail-Sicherheit --- wird jede E-Mail signiert, ohne es jedes mal separat zu aktivieren. Wenn viel von Shared-Mailboxen ohne Zertifikat versendet wird, kann es sinnvoll sein diese Funktion nur bei bedarf zu aktivieren. Durch die Option "In GAL veröffentlichen" wird der öffentliche Schlüssel im globalen Adressbuch abgelegt und vereinfacht somit die interne verschlüsselte Kommunikation.



Admin-Info:

Für die verschlüsselte Kommunikation via SMIME mit externen Empfängern sind serverseitig keine Konfigurationen notwendig.

Die ESCde-Anfrage gibt Hilfestellungen, wie geprüft werden kann, ob der öffentliche Schlüssel des externen am Client bekannt ist.