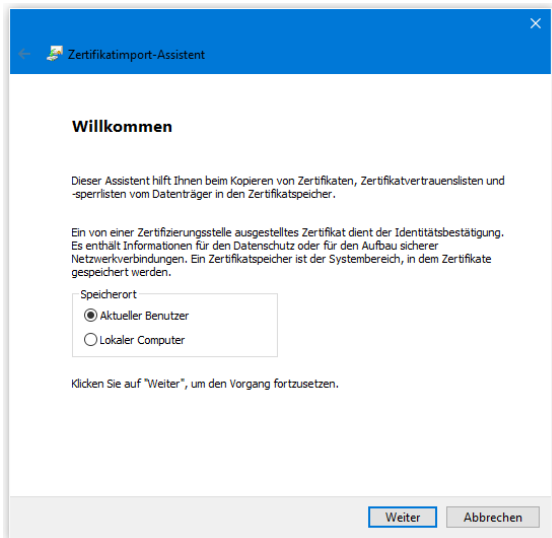
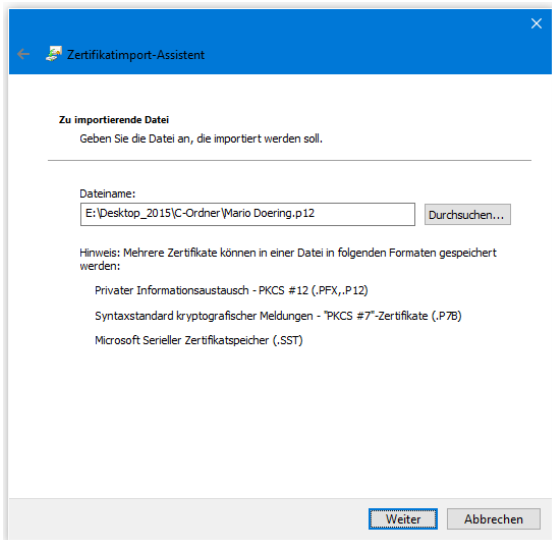


Beispielhaft - anhand von Windows 10 - beschreibt diese Anleitung den Import eines persönlichen SSL-Zertifikates (*.p12-Datei) in den internen Zertifikatsspeicher des Betriebssystems, um es anschließend im Internet Explorer wie auch in Outlook verwenden zu können.

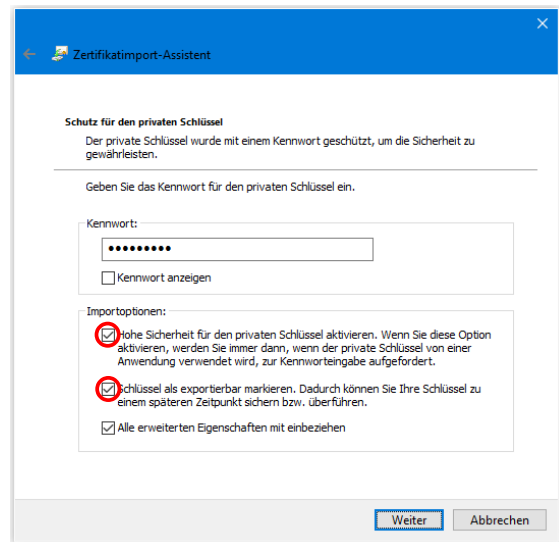
Als Erstes muss die bei der Zertifikatsausstellung in Empfang genommene *.p12-Datei auf den Windows-Rechner kopiert und der Installationsvorgang mit einem Doppelklick auf diese Datei gestartet werden.



Folgen Sie den Anweisungen des Zertifikatimport-Assistenten und klicken auf **Weiter**.

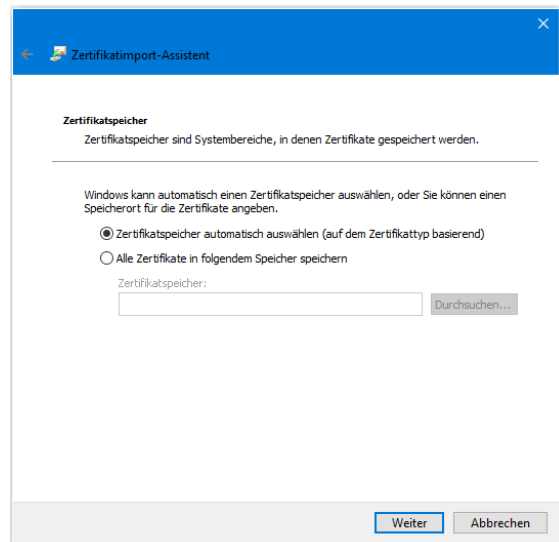


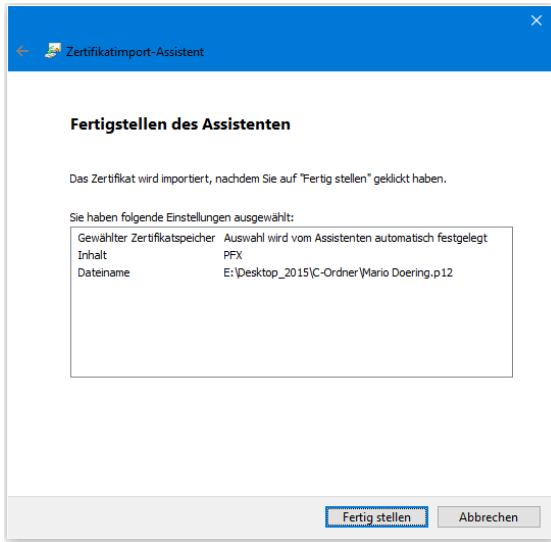
Als **Kennwort** für den privaten Schlüssel muss das Kennwort eingegeben werden, mit dem die *.p12-Datei geschützt wurde. Bei neu ausgestellt Zertifikaten sollte das die PIN sein, die



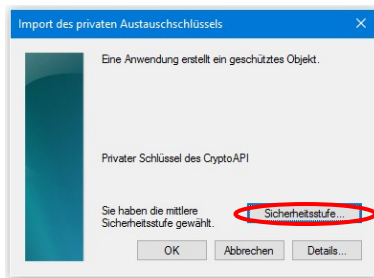
Ihnen im geschwärzten PIN-Brief gemeinsam mit Ihrer *.p12-Datei ausgehändigt wurde.

Mit der Option **Hohe Sicherheit** kann und sollte der Passwortschutz für den auf Ihrem Rechner zu importierenden privaten Schlüsselteil aktiviert werden.

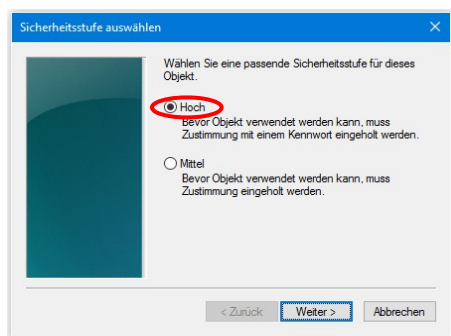




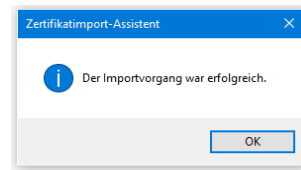
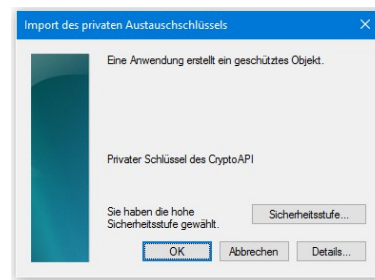
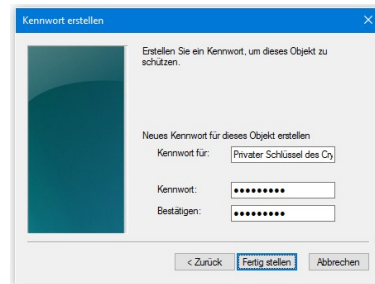
Um den Passwortschutz für den privaten Schlüsselanteil zu aktivieren, muss die **Sicherheitsstufe** im Fenster **Import des privaten Austauschschlüssels** konfiguriert



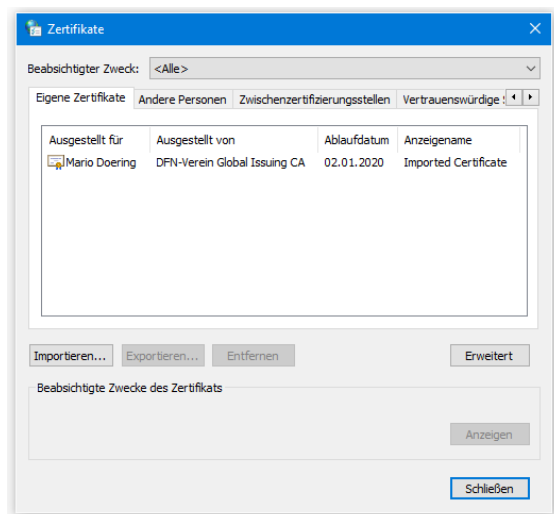
und im Fenster **Sicherheitsstufe auswählen** auf dem Wert **Hoch** gesetzt werden.



Im Fenster **Kennwort erstellen**, wird das Kennwort für den Schutz des privaten Schlüsselanteils auf Ihrem Rechner festgelegt.



Unter **Systemsteuerung => Internetoptionen => Inhalte => Zertifikate => Eigene Zertifikate** wird nun das importierte Zertifikat angezeigt und kann dort später – wenn es nicht mehr benötigt wird – auch wieder gelöscht werden.



Bitte richten Sie Fragen und Hinweise direkt per E-Mail an ca-btu@b-tu.de