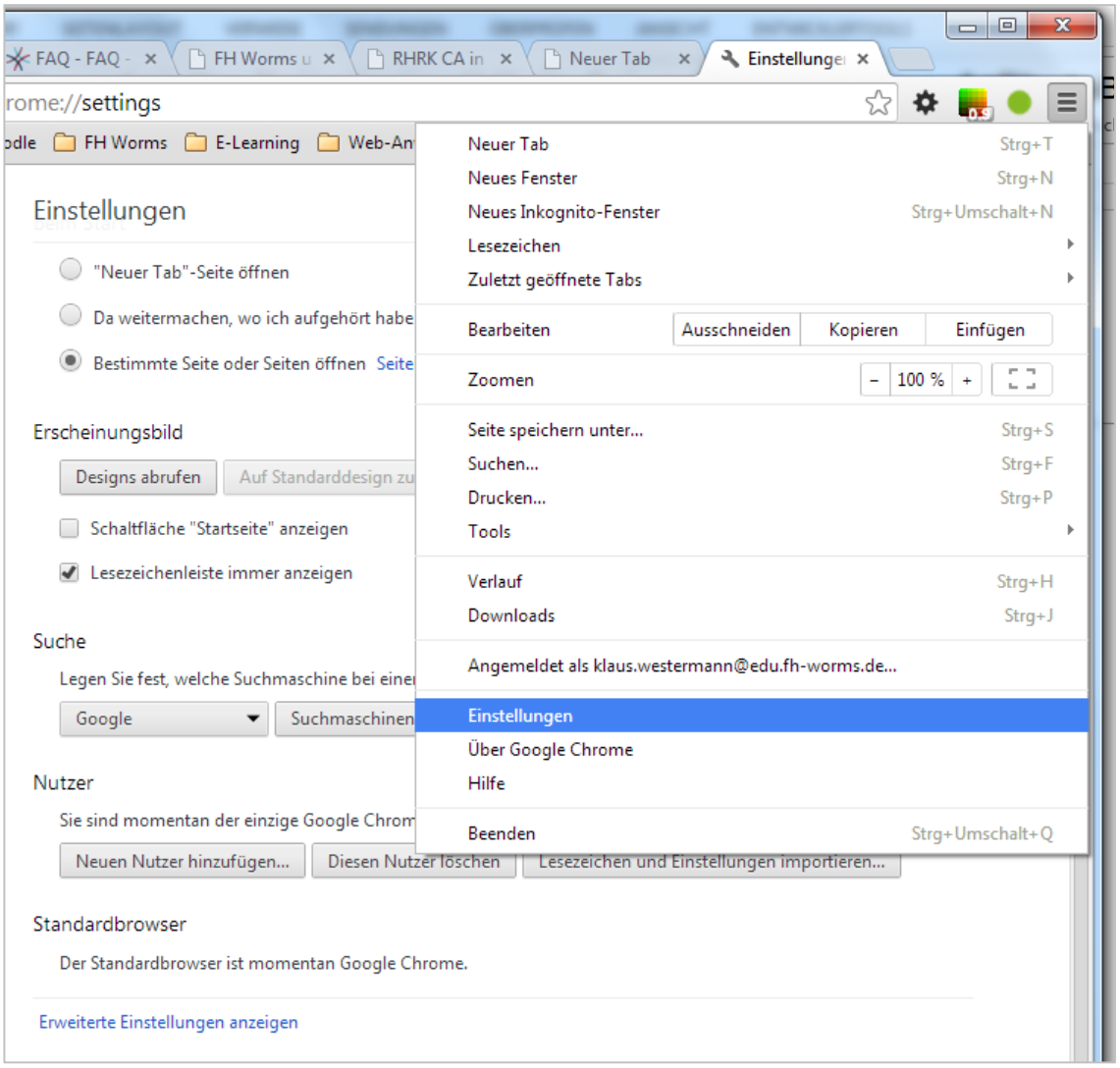
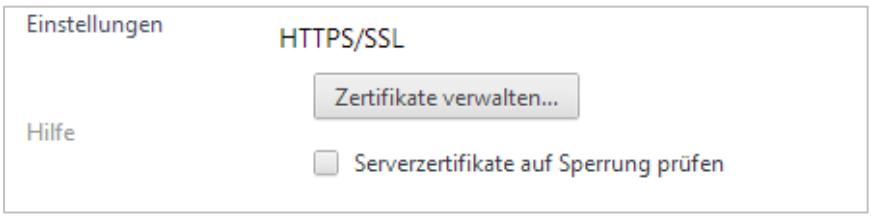
PKI-Zertifikate verwenden

Zertifikat implementieren und exportieren

Im Google-Chrome-Browser finden Sie Ihre Zertifikate unter EINSTELLUNGEN (rechts oben) → E-WEITERTE EINSTELLUNGEN (unten) → HTTPS/SSL → Zertifikate verwalten



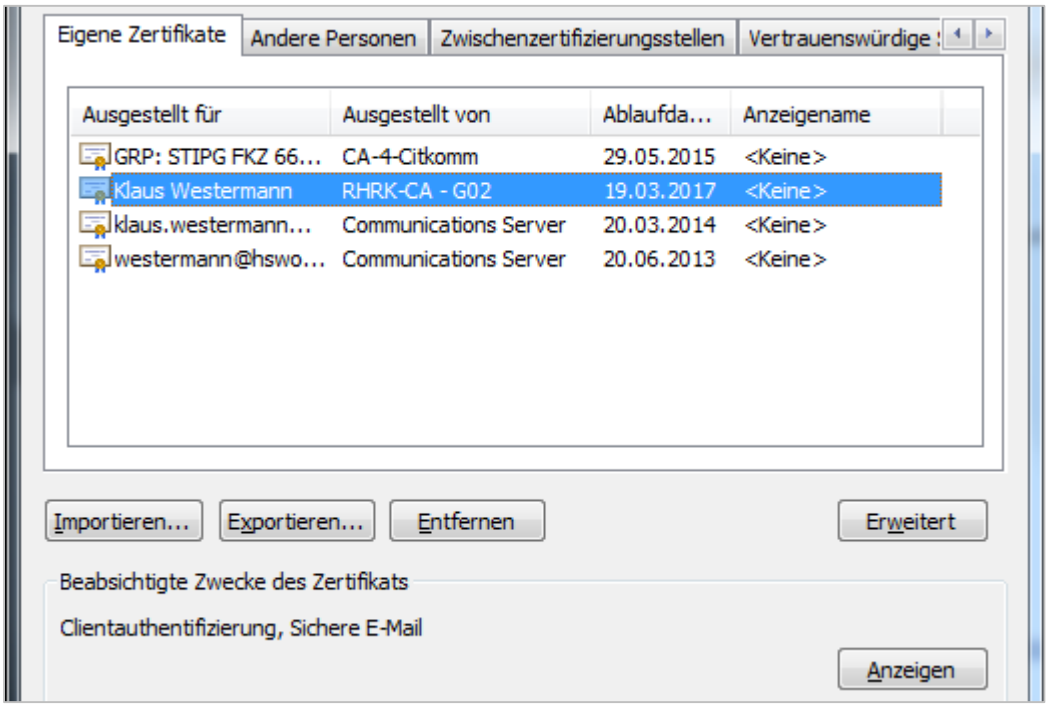


Das Zertifikat mit der Dateinamensendung .PEM kann exportiert werden, um es in anderen Browsern (z.B. Firefox) und in E-Mail-Programmen (z.B. Thunderbird) zu verwenden.

Beim Export wird das .PEM Zertifikat zu einem .PFX.

Wählen Sie dazu EIGENE ZERTIFIKATE → (Das Zertifikat mit dem neuen Ablaufdatum) → EXPORT

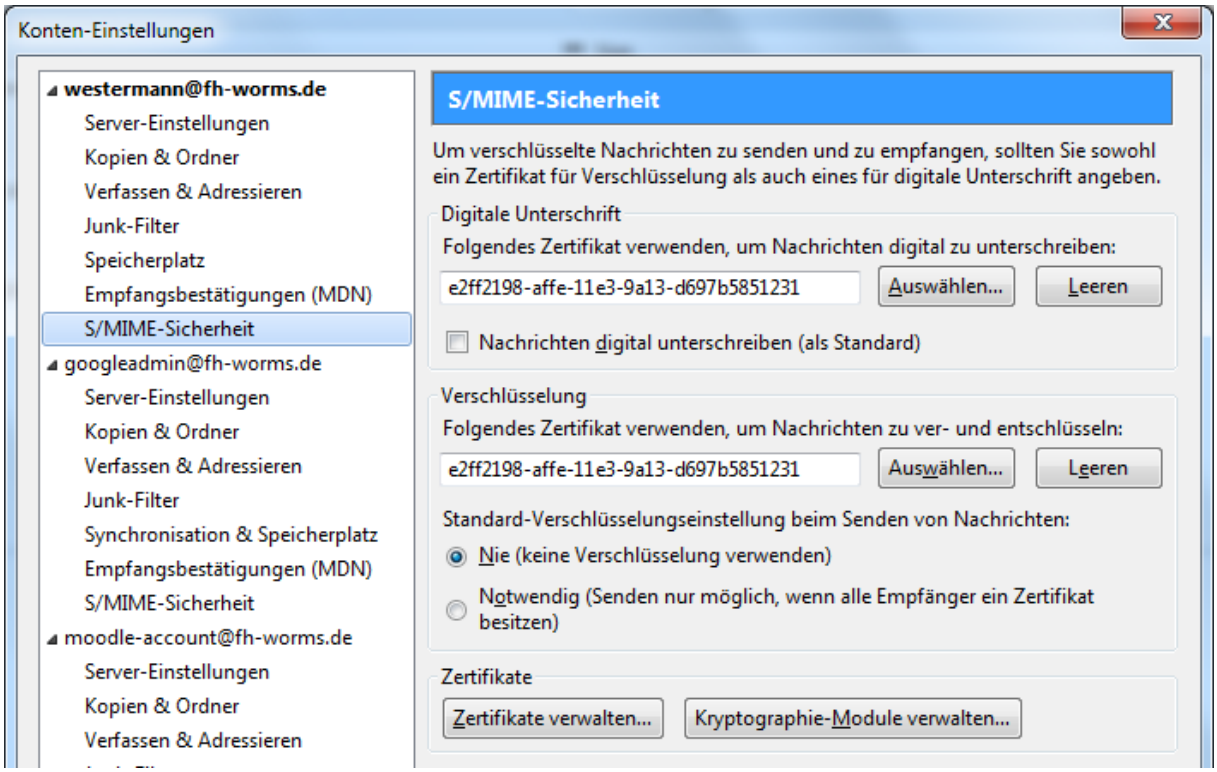
Unter ERWEITERT können Sie noch den Zweck näher festlegen.



Zertifikat importieren, Beispiel Thunderbird

Das exportierte Zertifikat kann nun in beliebige Anwendungen importiert werden. Beispiel „Thunderbird“ E-Mail-Client:

Unter EXTRAS → KONTENEINSTELLUNGEN → S/MIME-Sicherheit wählen Sie das exportierte Zertifikat für Signierung und Verschlüsselung.



Auf ähnliche Weise können Sie das Zertifikat auch in andere Webanwendungen importieren.

Kommentar des DFN

Die PEM-Datei kann nicht in eine P12-Datei konvertiert werden. Das PKCS#12-Format enthält den privaten *und* den öffentlichen Schlüssel.

Das Zertifikat kann nur in genau dem Browser auf genau dem Rechner installiert werden, mit dem auch der Antrag gestellt wurde. Denn nur dort befindet sich der zugehörige private Schlüssel (sofern am System keine gravierenden Änderungen vorgenommen wurden).

Installiert werden kann das Zertifikat nur ein einziges Mal über den angegebenen Link in der Zertifikats-Auslieferungsmail.

Dadurch wird ein Skript ausgeführt, das in dem verwendeten Browser nach dem zugehörigen privaten Schlüssel sucht. Wird dieser gefunden, dann wird das Zertifikat erfolgreich installiert und steht zur Verfügung.

Das Schlüsselpaar (= privater Schlüssel + Zertifikat) ist danach in der Schlüsselverwaltung unter "Eigene Zertifikate" zu sehen. Von dort können Sie es als P12-Datei exportieren und in eine Windows-Anwendung importieren. Windows verwendet gewöhnlich die Extension PFX, kann aber auch mit P12 umgehen.

Wenn es geschafft haben, Ihren Schlüssel als P12-Datei zu exportieren, dann können Sie diese Datei in beliebige Anwendungen (Browser, Mailclients) importieren. Das PKCS#12-Format ist universell.

Allerdings können Sie das Zertifikat nur für Mailadressen verwenden, die auch im Zertifikat enthalten sind. Für andere Mailadressen benötigen Sie weitere Zertifikate, oder ein Zertifikat mit mehreren Mailadressen.

Verschlüsseln können Sie Ihre E-Mails nur dann, wenn auch der Empfänger ein Zertifikat besitzt und wenn dieses Zertifikat in Ihrer Schlüsselverwaltung vorhanden ist, bzw. im Adressbuch dem Empfänger zugeordnet ist.

Das Ganze funktioniert asymmetrisch: mit Ihrem Schlüssel können Sie ausgehende E-Mails signieren und verschlüsselte E-Mails empfangen, d.h. andere können an Sie verschlüsseln, aber nicht umgekehrt.