

---

## Nutzung von Zertifikaten mit Microsoft Outlook Express

---

### 1. Zertifikat beantragen und installieren

Vor der Nutzung eines FZJ-Zertifikats mit MS Outlook Express sind zunächst folgende Schritte erforderlich:

1. Mit dem MS Internet Explorer die Home-Page des **CA Servers** anwählen.  
**<http://www.fz-juelich.de/CA/x509/ca-home.htm>**
2. **DFN-PCA Zertifikat** anfordern und im Verzeichnis '**Vertrauenswürdige Stammzertifizierungsstellen**' installieren.
3. **FZJ-CA-Zertifikat** anfordern und im Verzeichnis '**Zwischenzertifizierungsstellen**' installieren.
4. Das **persönliche Zertifikat** anfordern und nach Erhalt einer entsprechenden E-Mail-Bestätigung importieren.

Die Gültigkeit des Zertifikats kann im Zertifikatsspeicher überprüft werden.

1. Im Menü **Extras** den Kontext '**Optionen...**' anwählen..
2. Im Register **Sicherheit** den Schaltfläche '**Digitale IDs...**' klicken.
3. Aus der Liste '**Eigene Zertifikate**' das entsprechende Zertifikat auswählen und anzeigen.

Bei korrekter Installation muß im Zertifikat der Hinweis '**Sie besitzen einen privaten Schlüssel für dieses Zertifikat**' enthalten sein und der **Zertifizierungspfad** sollte über die '**FZJ-CA**' auf die '**DFN Toplevel Certification Authority**' verweisen.

Bei MS Outlook Express hat der Benutzer lediglich bei der Installation bzw. beim Import eines neuen Zertifikates die Möglichkeit zu entscheiden, ob bei jeder Verwendung des privaten Schlüssels ein Kennwort verlangt werden soll (hohe Sicherheitsstufe) oder nicht (Standard). Sobald das Zertifikat einmal installiert ist, kann diese Option nicht mehr geändert werden.

Soll nachträglich die Sicherheitsstufe geändert werden, so ist

1. das Zertifikat mit dem zugehörigen privaten Schlüssel zu **exportieren**,
2. das entsprechende Zertifikat aus dem Zertifikatsspeicher zu **löschen**,

3. das Zertifikat mit den Optionen '**Verstärkte Sicherheit für den privaten Schlüssel aktivieren**' und '**Privaten Schlüssel als exportierbar markieren**' neu zu importieren.

## 2. Nachrichten digital signieren und/oder verschlüsseln

Bei einer digital signierten E-Mail kann der Empfänger die Identität des Absenders überprüfen. Das Verschlüsseln einer E-Mail verhindert, daß andere Personen sie während der Übertragung lesen können.

Die Funktionen '**Nachricht digital signieren**' und '**Nachricht verschlüsseln**' werden während der Erstellung einer Nachricht über eindeutige Symbole in der Symbolleiste des Bearbeitungsfensters angeboten.

Die gewünschte Standardeinstellung kann voreingestellt werden:

1. Im Menü **Extras** den Kontext '**Optionen...**' anwählen.
2. Das Register **Sicherheit** auswählen.
3. Die Kontrollkästchen im Bereich '**Sichere E-Mail**' aktivieren bzw. deaktivieren.

Bei der Nutzung verschiedener Zertifikate kann MS Outlook Express so eingerichtet werden, daß sowohl für verschiedene E-Mail Konten, als auch für das Signieren und Verschlüsseln der Nachricht jeweils ein anderes Zertifikat verwendet wird.

1. Im Menü **Extras** den Kontext '**Konten...**' anwählen.
2. Die **Eigenschaften** des Kontos abfragen, bei dem das Zertifikat verwendet werden soll.
3. Im Register **Sicherheit** das gewünschte Zertifikat auswählen.

Falls für verschiedene Zertifikate eine Namensgleichheit besteht und somit bei der Auswahl nicht ohne weiteres unterscheidbar sind, sollte der Name in der Details-Ansicht des Zertifikats über '**Eigenschaften bearbeiten...**' / '**Angezeigter Name:**' geändert werden. Das Zertifikat selbst bleibt von dieser Änderung unberührt.

## 3. Vertrauenswürdige Zertifikate erhalten und speichern

Der Import vertrauenswürdiger Zertifikate kann auf zweierlei Art erfolgen:

1. Die meist gebräuchliche Methode ist, daß der E-Mail Partner eine mit seinem öffentlichen Schlüssel signierte Nachricht sendet und der Empfänger diesen assistentgesteuert in die Rubrik '*Andere Personen*' des Zertifikatsspeichers importiert.
2. Die Zertifizierungsstelle des E-Mail Partners ist bekannt und man erfragt dort den öffentlichen Schlüssel des für ihn ausgestellten Zertifikats.

Die Zertifikate der auf dem FZJ-CA Server registrierten FZJ-Mitarbeiter können unter '<https://ca.fz-juelich.de/fzj-html/suche.html>' abgefragt werden. Der öffentlichen Schlüssel befindet sich im Abschnitt '*Base 64 encoded certificate*' und kann über den Umweg einer .cer-Datei in die Rubrik '*Andere Personen*' des Zertifikatsspeichers importiert werden.

## 4. Signierte und verschlüsselte E-Mail

Das Versenden einer verschlüsselten E-Mail setzt den Besitz des Empfängerzertifikats voraus, d.h. der öffentliche Schlüssel des Empfängers muß vorhanden und im Adressbuch mit seinem Namen verknüpft ist.

Beispiel: Herr Müller aus Jülich und Frau Meyer aus Berlin möchten sichere E-Mail austauschen.

1. Herr Müller sendet eine signierte E-Mail an Frau Meyer.
2. Frau Meyer erhält beim Öffnen der E-Mail von Herrn Müller einen Hinweis, daß es sich um eine signierte E-Mail handelt. Gleichzeitig wird in der rechten oberen Ecke der geöffneten Nachricht ein rotes Siegel eingeblendet über das die Eigenschaften der Signatur abgefragt werden können.

Hinweis: Im Feld '*Status der Überprüfung*' wird bei den von der FZJ-CA ausgestellten Zertifikaten die Meldung angezeigt, daß die digitale ID nicht überprüft werden kann, weil die Liste der zurückgezogener IDs unerhältlich sei. Dieser Hinweis hat keine Auswirkungen auf die Verwendbarkeit des Zertifikats und muß z.Z. leider noch ignoriert werden. Ein Link zur Liste der zurückgezogenen Zertifikate steht jedoch auf der Home-Page des CA Servers zur Verfügung.

Frau Meyer kann nun das Zertifikat dem Adressbucheintrag des Herrn Müller hinzufügen. Ob dieser Vorgang automatisch (Standard) oder manuell erfolgen soll, ist über eine entsprechende Option einstellbar:

- Menü **Extras** - Kontext **Optionen...** - Register **Sicherheit**
- Schaltfläche '**Weitere Einstellungen...**'
- Kontrollkästchen '**Absenderzertifikat automatisch dem Adressbuch hinzufügen**'

Falls diese Option ausgeschaltet ist, muß das Zertifikat dem Adressbuch manuell hinzugefügt werden:

- Öffnen der digital signierte Nachricht
- Menü **Datei** auf **Eigenschaften**
- Registerkarte **Sicherheit**
- Schaltfläche '**Digitale ID zum Adressbuch hinzufügen**'

3. Frau Meyer verfaßt eine Antwort, signiert diese mit ihrem eigenen Zertifikat und verschlüsselt sie mit dem Zertifikat des Herrn Müller.
4. Herr Müller vollzieht nun die gleichen Schritte wie unter Punkt 2. für Frau Meyer beschrieben.

Nach Abarbeitung der o.g. Punkte können Herr Müller und Frau Meyer die verschlüsselten Nachrichten auf die gleiche Weise lesen wie normale (unverschlüsselte) Nachrichten.

Weitere Informationen zur Nutzung von Zertifikaten bietet die Online Hilfe von MS Outlook Express (F1) unter dem Stichwort 'Digitale ID'.

## **5. Hinweis zur Sicherheit und Vertraulichkeit des privaten Schlüssels**

Da das Zertifikat den 'Beweis' für die Identität des Senders der E-Mail darstellen soll, darf keine andere Person in den Besitz des privaten (geheimen) Teils des Zertifikats (den privaten Schlüssel) gelangen. Der PC und der private Schlüssel müssen also zwingend vor unbefugtem Zugriff geschützt werden. Das bedeutet insbesondere, daß sichergestellt werden muß, daß keine 'Trojanischen Pferde' von Hackern heimlich auf dem PC installiert werden. Solche böartigen Programme sind in der Lage, durch Ablesen der Tastaturanschläge eingegebene Kennwörter auszuspähen, sie über das Internet an den Hacker zu versenden, um diesem dann

die Möglichkeit zu geben, unter Verwendung des fremden Zertifikats die Identität des eigentlichen Besitzers vorzutäuschen. Es ist also absolut unerlässlich, den PC vor solchen schädlichen Programmen zu schützen und einen aktuellen Viren-Scanner (siehe FZJ-ZAM-TKI-0355) zu nutzen.