

Zertifikat der TUD / Digitale Signatur

[Beantragung](#)

[Installation in Windows / Management](#)

[Konfiguration in Outlook](#)

[Konfiguration in Thunderbird](#)

[Nutzung als Digitale Signatur in PDFs](#)

[Anpassung der Digitalen Signatur in PDFs](#)

[Einbindung des DFN LDAP Adressbuches](#)

Mit den digitalen Zertifikaten der TUD vom DFN ist es möglich E-Mails zu signieren und zu verschlüsseln und ebenso das Zertifikat für PDF-Dokumente (mindestens Adobe Acrobat Reader empfohlen) zum Signieren als Digitale Signatur zu verwenden.

Beantragung

Die Ausstellung erfolgt über das neue EVAZert Verfahren im SAP. Hierzu ist eine **Identitätsprüfung** beim zuständigen IT-Personal (bei cfaed der IT-Referent bzw. dessen Vertreter) mit:

- Personalnummer (diese kann im <https://selfservice.zih.tu-dresden.de> der TUD unter „Mein Profil“ nachgeschaut werden bzw. wird für neue Mitarbeiter von der Personalstelle ausgehändigt)
- Ausweisnummer eines gültigen Lichtbildausweises
- Gültigkeit des Lichtbildausweises

Nach erfolgter Identitätsprüfung erhält der Nutzer eine Beantragung-PIN, mit der über das <https://selfservice.zih.tu-dresden.de> auf der linken Seite unter **Zertifikats-Management -> Zertifikats-Beantragung** das Zertifikat beantragt werden kann (hierzu PIN eingeben und auf Prüfen klicken).

The screenshot shows the 'SELF SERVICE PORTAL' interface. On the left is a navigation menu with options like 'Startseite', 'Zugangsvoraussetzung', 'Coupon einlösen', 'Mein Profil', 'Passwortverwaltung', 'Zertifikats-Management' (selected), 'Zertifikats-Übersicht', 'Zertifikats-Beantragung', and 'Login Antrag'. The main content area is titled 'ZERTIFIKATS-BEANTRAGUNG'. It contains the text 'Die PIN wurde Ihnen bei der Identitätsprüfung bzw. bei der Eir', a 'PIN:' label followed by an input field and a 'Zeige PIN' checkbox, and a 'Prüfen' button. At the bottom, it shows the date and time 'Stand 19.05.2020 11:02'.

Nach einer Weile bekommt man eine E-Mail, dass das neue Zertifikat im <https://selfservice.zih.tu-dresden.de> auf der linken Seite unter **Zertifikats-Management -> Zertifikats-Übersicht** innerhalb von 30 Tagen heruntergeladen werden kann.

Startseite » ... » Self Service Portal » Zertifikats-Management » Zertifikats-Übersicht

SELF SERVICE PORTAL:

- ☐ Startseite
- ☐ **Zugangsvoraussetzung**
 - ☐ Coupon einlösen
 - ☐ Mein Profil
 - ☐ Passwortverwaltung
 - ☐ Zertifikats-Management
 - ☒ Zertifikats-Übersicht
 - ☐ Zertifikats-Beantragung
 - ☐ Login Antrag

ZERTIFIKATS-ÜBERSICHT

In der Tabelle werden alle Zertifikate angezeigt, die Sie über das Self-Service Portal beantragt haben. Es besteht die Möglichkeit des Downl

Hinweis: Ihr Zertifikat steht nach Beantragung nur für 12 Wochen zum Download bereit.

Identität geprüft: Ja (2020-05-05 11:05:16)

AKTIVE ZERTIFIKATE

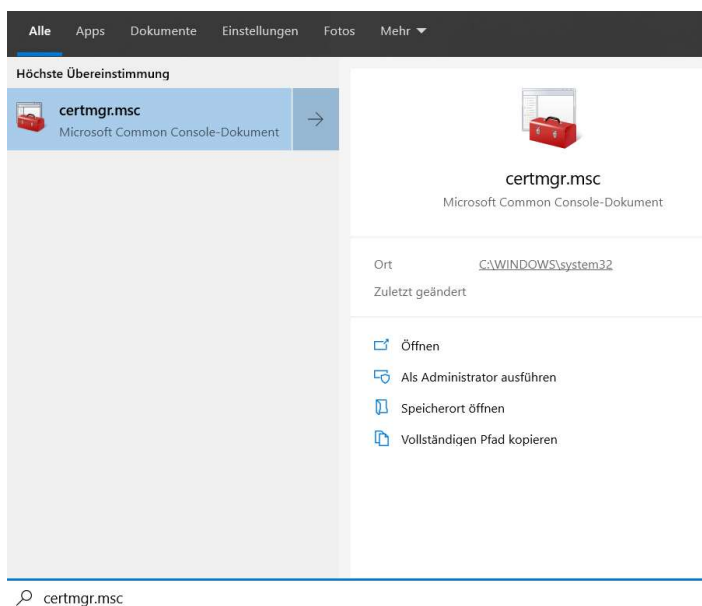
Seriennummer	E-Mail	Beantragt am	Gültig Bis	Sperrung	Download
10774751263786236134143950521	uwe.pretzsch@tu-dresden.de	2020-05-05	2023-05-05	Sperrung	Download

Hierfür auf Download klicken und das Zertifikat sicher ablegen (z.B. auf dem persönlichen ZIH Netzlaufwerk)! Ein sprechender Name z.B. <Name> TUD-Zertifikat <Jahr>.p12 wird empfohlen.

Installation in Windows / Management

Die Installation in Windows kann einfach durch einen Doppelklick mit der linken Maustaste ausgelöst werden. Es öffnet sich ein Assistent der weitgehend durchgeklickt werden kann. Nur in folgendem Dialog wird empfohlen „Schlüssel als Exportierbar...“ einzustellen -> damit kann das Zertifikat erneut vom Rechner gesichert werden, falls es an anderer Stelle verloren geht. Als Kennwort muss man hier das vorher vergebene Kennwort eingeben (dieses unbedingt merken und sichern, ansonsten ist das Zertifikat später nicht mehr nutzbar)!

Verwalten kann man die Zertifikate in Windows unter der Zertifikatsverwaltung, dazu folgendes starten (certmgr.msc):



Hier sieht man unter **Eigene Zertifikate** -> **Zertifikate** seine installierten Zertifikate (ältere Zertifikate müssen installiert bleiben, sonst sind früher verschlüsselte Emails unter Umständen nicht lesbar).

Datei	Aktion	Ansicht	?
Zertifikate - Aktueller Benutzer Eigene Zertifikate Zertifikate Vertrauenswürdige Stammzertifikate Organisationsvertrauen Zwischenzertifizierungsstellen Active Directory-Benutzerobjekte Vertrauenswürdige Herausgeber			
Ausgestellt für	Ausgestellt von	Ablaufdatum	Beabsichtigte Zwecke
23194a95cf0e09d1	Token Signing Public Key	14.05.2020	Clientauthentifizierung...
7386E284-8054-4A43-AB0E-F834...	Apple iPhone Device CA	12.12.2020	Serverauthentifizierung...
easy.box	easy.box	24.08.2021	<Alle>
Uwe Pretzsch	TU Dresden CA	31.05.2020	Clientauthentifizierung...
Uwe Pretzsch	TU Dresden CA	05.05.2023	Clientauthentifizierung...
Anzeigenname	St		
<Keine>			
APNS certificate Dire...			
<Keine>			
Uwe Pretzsch's Tech...			
<Keine>			

Zum Sichern von Zertifikate dieses mit der **rechten Maustaste** anklicken -> **Alle Aufgaben** -> **Exportieren** (es öffnet sich ein Assistent zum exportieren).

Ausgestellt für	Ausgestellt von	Ablaufdatum	Beabsichtigt
23194a95cf0e09d1	Token Signing Public Key	14.05.2020	Clientauthen
7386E284-8054-4A43-AB0E-F834...	Apple iPhone Device CA	12.12.2020	Serverauthen
easy.box	easy.box	24.08.2021	<Alle>
Uwe Pretzsch	TU Dresden CA	31.05.2020	Clientauthen
Uwe Pretzsch	TU Dresden CA	05.05.2023	Clientauthen

Öffnen

Alle Aufgaben

Ausschneiden

Kopieren

Löschen

Eigenschaften

Hilfe

Öffnen

Zertifikat mit neuem Schlüssel anfordern...

Zertifikat mit neuem Schlüssel erneuern...

Erweiterte Vorgänge

Exportieren...

Unbedingt den Privaten Schlüssel mit exportieren, sonst ist das Zertifikat unvollständig!

← Zertifikatexport-Assistent

Privaten Schlüssel exportieren

Sie können den privaten Schlüssel mit dem Zertifikat exportieren.

Private Schlüssel sind kennwortgeschützt. Wenn Sie den privaten Schlüssel mit dem ausgewählten Zertifikat exportieren möchten, müssen Sie auf einer der folgenden Seiten ein Kennwort eingeben.

Möchten Sie mit dem Zertifikat auch den privaten Schlüssel exportieren?

- ☒ Ja, privaten Schlüssel exportieren
 ☐ Nein, privaten Schlüssel nicht exportieren

Alle erweiterten Eigenschaften mit auswählen!

Format der zu exportierenden Datei

Zertifikate können in verschiedenen Dateiformaten exportiert werden.

Wählen Sie das gewünschte Format:

- ☐ DER-codiert-binär X.509 (.CER)
- ☐ Base-64-codiert X.509 (.CER)
- ☐ Syntaxstandard kryptografischer Meldungen - "PKCS #7"-Zertifikate (.P7B)
 - ☐ Wenn möglich, alle Zertifikate im Zertifizierungspfad einbeziehen
- ☒ Privater Informationsaustausch - PKCS #12 (.PFX)
 - ☒ Wenn möglich, alle Zertifikate im Zertifizierungspfad einbeziehen
 - ☐ Privaten Schlüssel nach erfolgreichem Export löschen
 - ☒ Alle erweiterten Eigenschaften exportieren
 - ☒ Zertifikatdatenschutz aktivieren
- ☐ Microsoft Serieller Zertifikatspeicher (.SST)

Kennwort vergeben!

Sicherheit

Zur Gewährleistung der Sicherheit müssen Sie den privaten Schlüssel mit einem Sicherheitsprinzipal oder mithilfe eines Kennworts schützen.

☐ Gruppen- oder Benutzernamen (empfohlen)

Hinzufügen

Entfernen

☐ Kennwort:

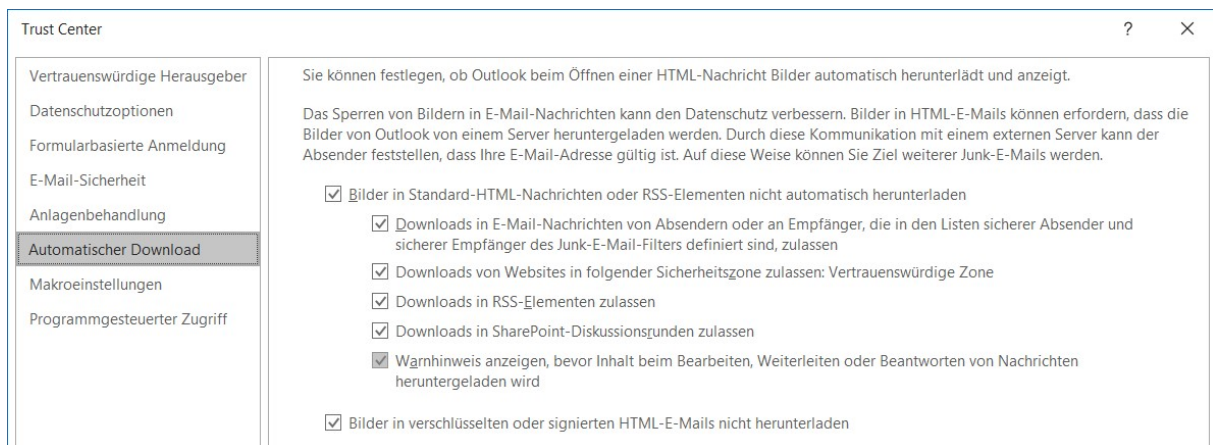
Kennwort bestätigen:

Verschlüsselung: TripleDES-SHA1 ▾

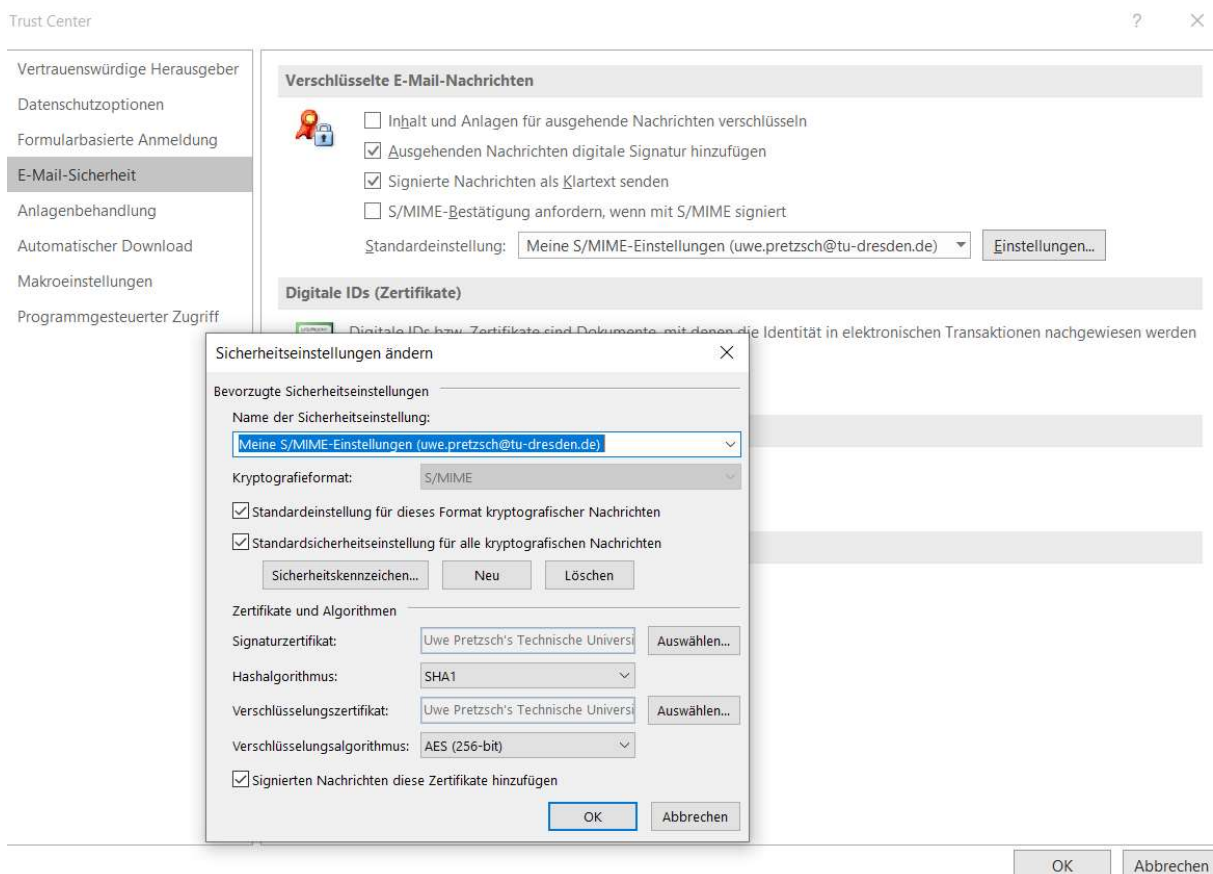
Der Rest ist selbsterklärend...

Konfiguration in Outlook

Um ein Zertifikat in Outlook zum Signieren oder Verschlüsseln zu verwenden, im Outlook nach **Datei -> Optionen -> Trust Center -> Einstellungen für das Trust Center** gehen:



Hier zu **E-Mail-Sicherheit -> Einstellungen** wechseln!



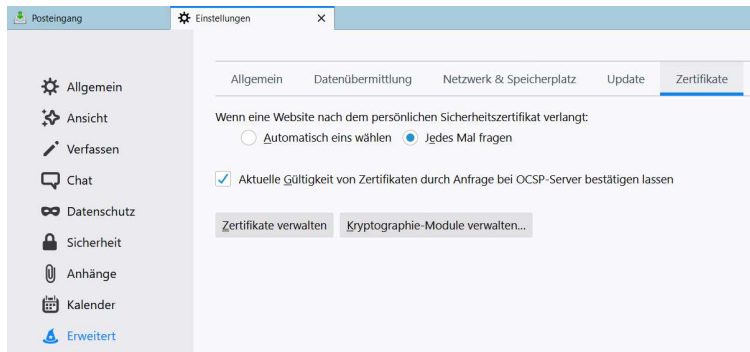
Auf **Auswählen** klicken und das richtige Zertifikat (Ablaufdatum beachten) wählen! Unter **E-Mail-Sicherheit** das Häkchen „Ausgehende Nachrichten digitale Signaturen hinzufügen“ anwählen. Fertig!

Zur Sicherheit sich selbst eine Testmail schicken, diese sollte ein Signatursymbol enthalten. Wenn man dieses anklickt erhält man weitere Informationen zum Zertifikat.

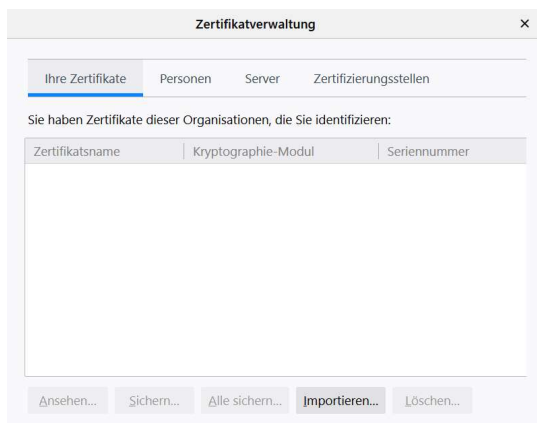


Konfiguration in Thunderbird

Für die Konfiguration in Thunderbird muss das Zertifikat zuerst in den Mozilla Zertifikatsspeicher importiert werden. Hierfür in Thunderbird zu **Einstellungen -> Einstellungen -> Erweitert -> Zertifikate** gehen.

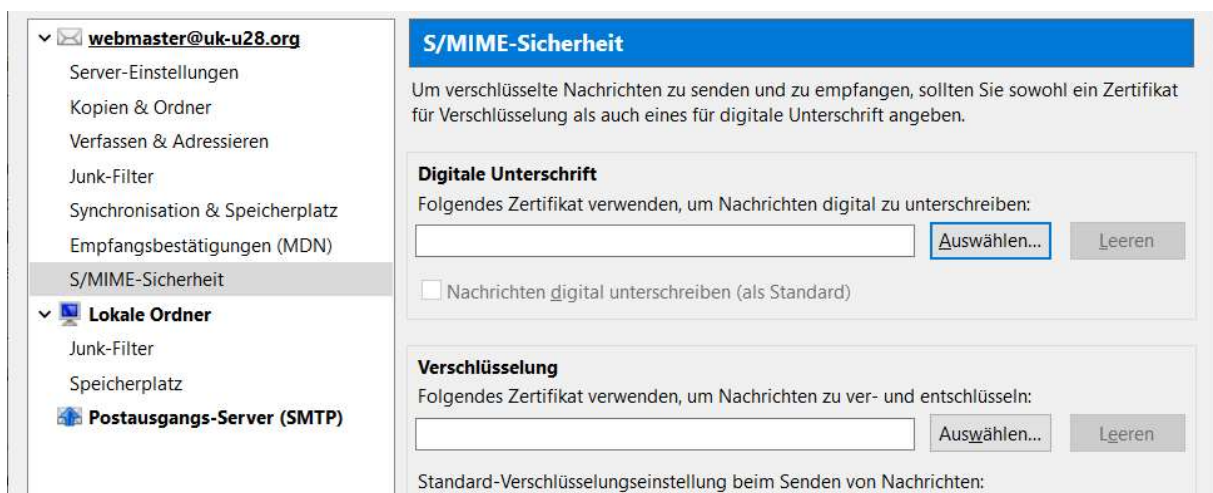


Dort auf **Zertifikate verwalten** klicken. **Ihre Zertifikate** auswählen und **Importieren** wählen. Mit dem sich öffnenden Assistenten das Zertifikat importieren.



Zur Einrichtung für signierte und verschlüsselte Emails in Thunderbird zu **Einstellungen -> Konten-Einstellungen -> (beim TUD Postfach) S/Mime-Sicherheit**

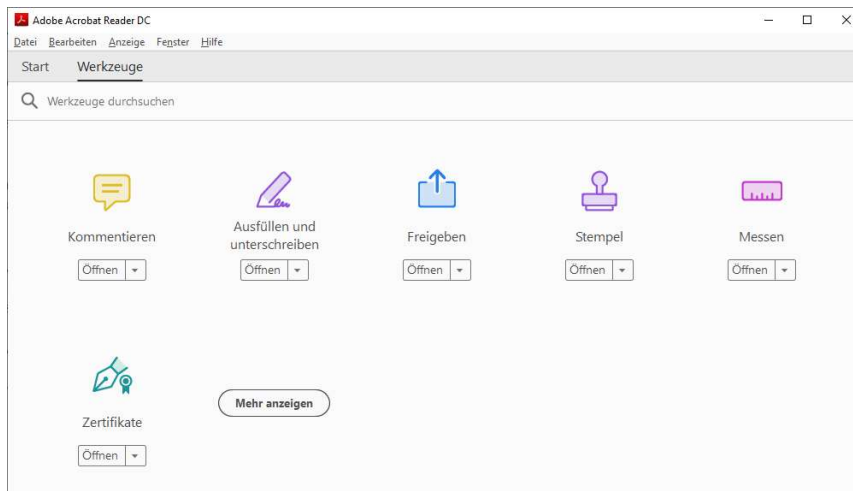
Bei **Digitale Unterschrift** das Zertifikat **Auswählen** (ist hier keines sichtbar, liegt das daran, das unter dem Postfach die E-Mail-Adresse falsch ist. Hier geht nur die, auf die das Zertifikat ausgestellt ist, ansonsten ist kein Zertifikat auswählbar!



Nutzung als Digitale Signatur in PDFs

Die Nutzung als Digitale Signatur in PDFs kann sofort nach der Installation in Windows erfolgen. Empfohlen wird hier Adobe Reader oder Adobe Acrobat, in anderen PDF Programmen kann nicht garantiert werden, das eine Unterstützung der Digitalen Signatur vorhanden ist.

Die Digitale Signatur sollte in Adobe Programmen *NICHT* mit der Funktion „**Ausfüllen und Unterschreiben**“ verwechselt werden. Klickt man in Adobe Programmen auf Werkzeuge, muss hier „**Zertifikate**“ verwendet werden.



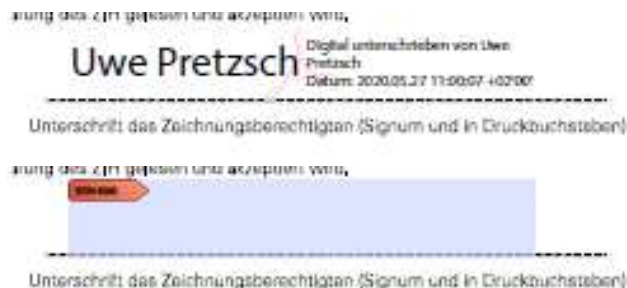
In bereits als Formular generierten kann nicht digital signiert werden, falls kein Signaturfeld vorhanden ist. Formulare sind meistens gegen Änderungen gesperrt und das Anlegen eines Signaturfeldes ist eine Änderung am PDF (ein Workaround ist hier das erneute Drucken als Microsoft PDF -> damit verliert das Formular aber alle Eingabefelder).

Das Menü „Digital unterschreiben“ muss auswählbar sein. Zum digitalen signieren, dieses Menü auswählen und einen Rahmen auf dem Unterschriftsfeld ziehen.

Signatur auswählen und speichern der PDF (es empfiehlt sich nicht direkt aus Mailprogrammen zu arbeiten, da die PDF immer gespeichert werden muss und Mailprogramme in der Regel einen versteckten temporären Speicherort für Ihre Anhänge verwenden).

Löscht man jetzt mit der rechten Maustaste die Digitale Signatur und speichert erneut ab, bleibt der Signaturrahmen bestehen. So kann man eigene PDF Dokumente bereits mit einem Signaturrahmen versehen.

Haben PDF-Dokumente bereits einen Signaturrahmen, genügt es diesen anzuklicken, Signatur auswählen, speichern.



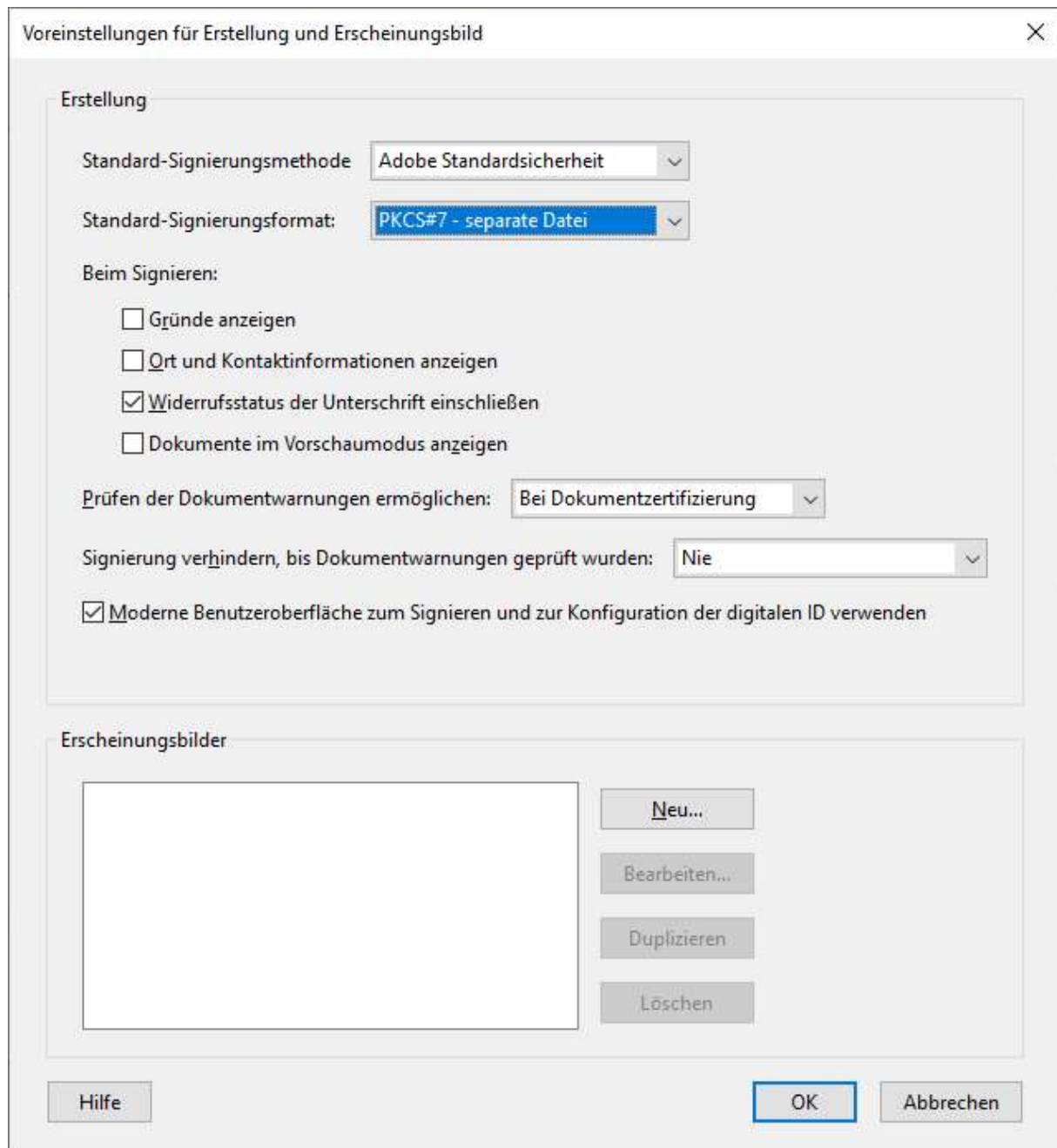
In Adobe Reader oder Adobe Acrobat kann über **Bearbeiten -> Einstellungen -> Unterschriften** die Digitale Signatur angepasst werden.

In Adobe Reader oder Adobe Acrobat kann über **Bearbeiten -> Einstellungen -> Unterschriften** die Digitale Signatur angepasst werden.

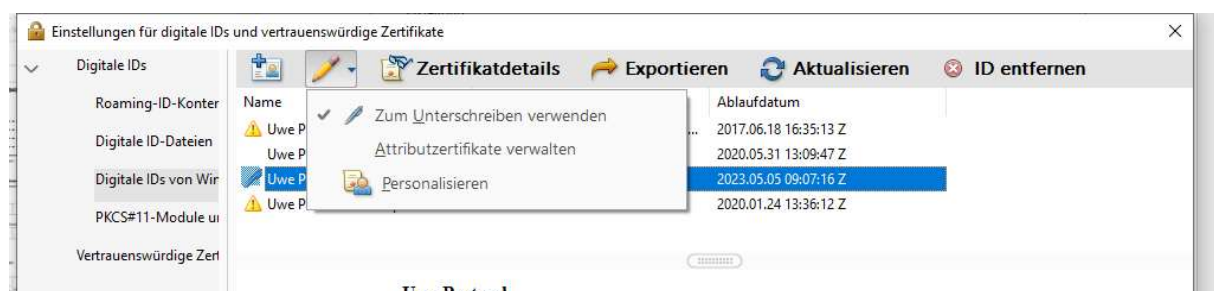
The screenshot shows the 'Einstellungen' (Settings) window in Adobe Acrobat. The left sidebar lists various categories, with 'Unterschriften' (Signatures) selected and highlighted. The main content area is titled 'Digitale Unterschriften' (Digital Signatures) and contains four sub-sections, each with a 'Weitere...' (More...) button:

- Erstellung und Erscheinungsbild** (Creation and Appearance):
 - Steuerungsoptionen für die Erstellung einer Unterschrift
 - Festlegen des Erscheinungsbilds von Unterschriften innerhalb eines Dokuments
- Überprüfung** (Verification):
 - Festlegen, wie und wann Unterschriften geprüft werden
- Identitäten und vertrauenswürdige Zertifikate** (Identities and Trusted Certificates):
 - Erstellen und Verwalten von Identitäten für die Unterzeichnung
 - Verwalten von Anmeldeinformationen für die Vertrauenswürdigkeit von Dokumenten
- Zeitstempel für Dokumente** (Timestamps for Documents):
 - Konfigurierung der Servereinstellungen für Zeitstempel

At the bottom right of the window are 'OK' and 'Abbrechen' (Cancel) buttons.



Um bei mehreren Zertifikaten das richtige automatisch zu wählen zu **Bearbeiten** -> **Einstellungen** -> **Unterschriften** -> **Identitäten...Weitere** -> **Digitale IDs von Windows** gehen. Zertifikat markieren und oben bei dem Stift im Menü „Zum Unterschreiben verwenden“ auswählen.

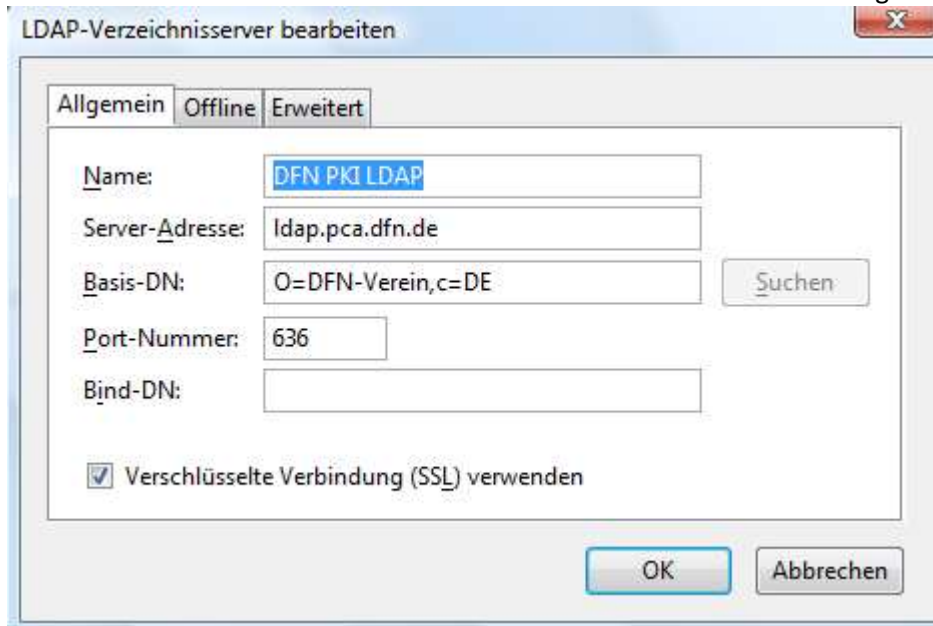


Einbindung des DFN LDAP Adressbuches

MOZILLA Thunderbird

Konfigurieren Sie das DFN PKI Verzeichnis als neues Adressbuch. Öffnen Sie dazu das Adressbuch über den Menüeintrag **Extras->Adressbuch**. Wählen Sie dann bitte oben im Menü **Datei->Neu->LDAP-Verzeichnis**. Bitte fügen Sie einen neuen LDAP-Verzeichnis hinzu mit folgenden Angaben:

Klicken Sie dann bitte auf **OK**. Damit wird der LDAP-Verzeichnisserver eingetragen.



LDAP-Verzeichnisserver bearbeiten

Allgemein Offline Erweitert

Name: DFN PKI LDAP

Server-Adresse: ldap.pca.dfn.de

Basis-DN: O=DFN-Verein,c=DE Suchen

Port-Nummer: 636

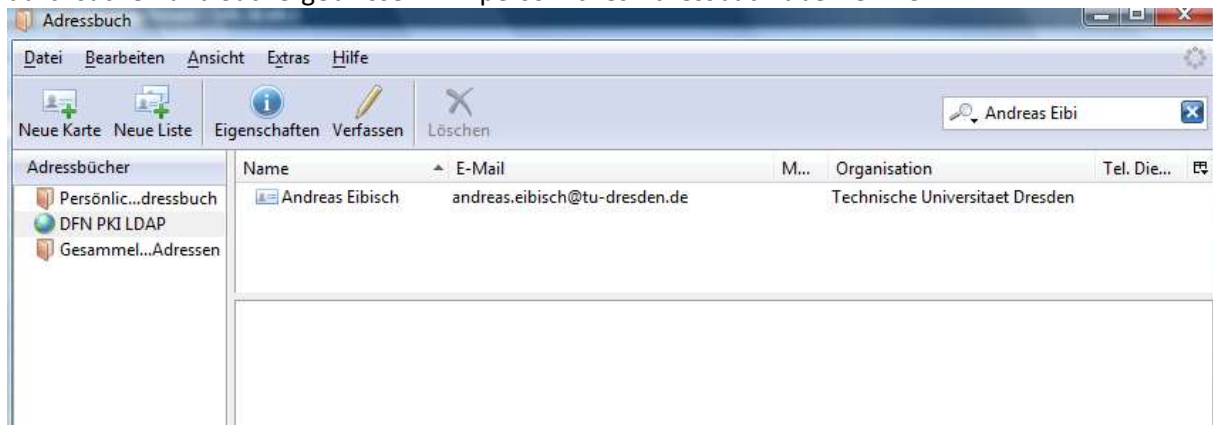
Bind-DN:

☒ Verschlüsselte Verbindung (SSL) verwenden

OK Abbrechen

Name: DFN PKI LDAP
Server-Adresse: ldap.pca.dfn.de
Basis-DN: O=DFN-Verein,c=DE
Port-Nummer: 636
Verschlüsselte Verbindung (SSL) verwenden
alle weiteren Optionen können beibehalten werden

Sie können nun im Adressbuch das DFN PKI LDAP Verzeichnis nach Personen bzw. E-Mail-Adressen durchsuchen und Suchergebnisse in ihr persönliches Adressbuch übernehmen.



Adressbuch

Datei Bearbeiten Ansicht Extras Hilfe

Neue Karte Neue Liste Eigenschaften Verfassen Löschen

Adressbücher

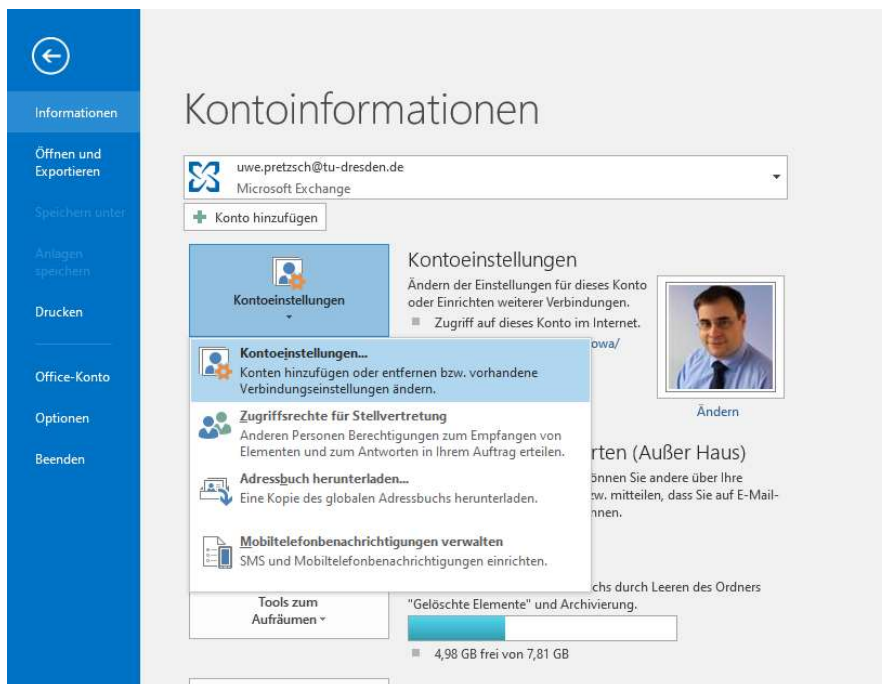
- Persönlic...dressbuch
- DFN PKI LDAP
- Gesammel...Adressen

Name E-Mail M... Organisation Tel. Die...

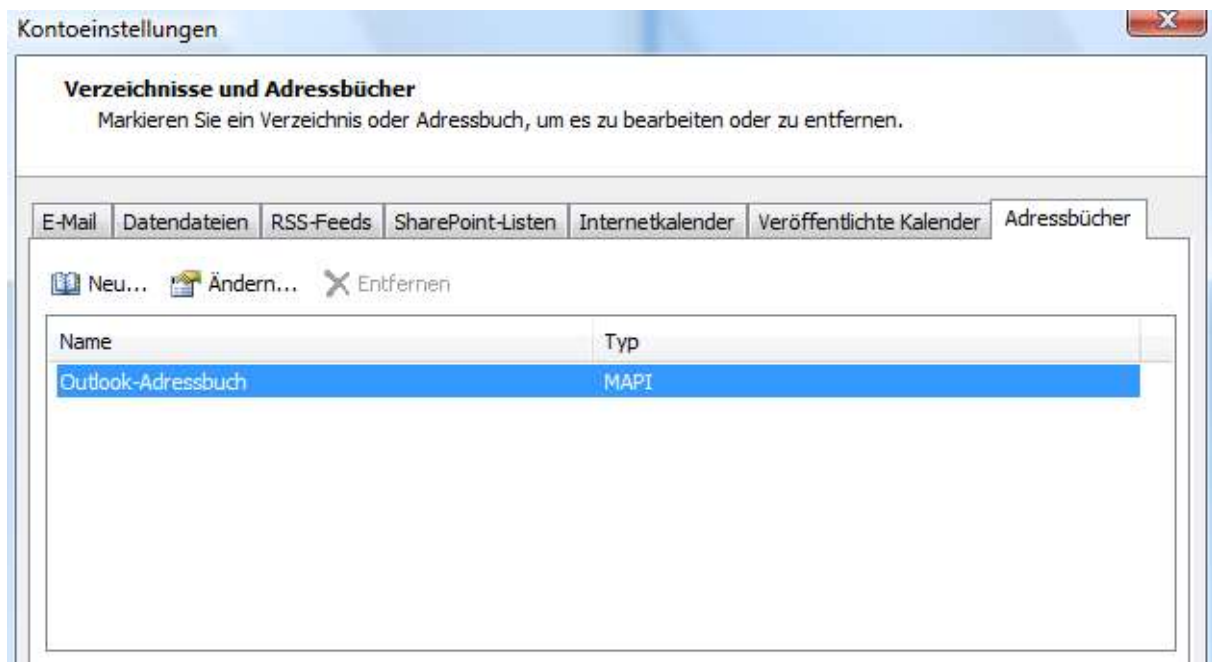
Andreas Eibisch	andreas.eibisch@tu-dresden.de		Technische Universitaet Dresden	
-----------------	-------------------------------	--	---------------------------------	--

Microsoft Outlook

Wählen Sie in MS Outlook die Registerkarte "Datei" -> "Kontoeinstellungen" -> "Kontoeinstellungen"



Wechseln Sie anschließend auf das Tab **Adressbücher** und klicken Sie auf **Neu...**



Wählen Sie bitte als **Verzeichnis- oder Adressbuchtyp** Internetverzeichnisdienst (LDAP) aus und klicken Sie auf **Weiter**.

Neues E-Mail-Konto hinzufügen

Verzeichnis- oder Adressbuchtyp
Sie können wählen, welchen Verzeichnis- oder Adressbuchtyp Sie hinzufügen möchten.

☒ **Internetverzeichnisdienst (LDAP)**
Verbindung zu einem LDAP-Server herstellen, um E-Mail-Adressen und weitere Informationen zu suchen und zu überprüfen.

☐ **Zusätzliche Adressbücher**
Verbindung zu einem Adressbuch herstellen, um E-Mail-Adressen und weitere Informationen zu suchen und zu überprüfen.

< Zurück Weiter > Abbrechen

Tragen Sie unter **Servername** ldap.pca.dfn.de ein und klicken Sie dann auf **Weitere Einstellungen....**
Outlook weist Sie darauf hin, dass Sie nach Abschluß der Konfiguration Outlook beenden und neu starten müssen.

Neues E-Mail-Konto hinzufügen

Einstellungen für den Verzeichnisdienst (LDAP)
Geben Sie die Einstellungen ein, die für den Zugriff auf Informationen eines Verzeichnisdiensts erforderlich sind.

Serverinformationen
Geben Sie den Namen des Verzeichnisservers ein, den Sie von Ihrem Internetdienstanbieter oder Systemadministrator erhalten haben.

Servername:

Anmeldeinformationen

☐ Server erfordert Anmeldung

Benutzername:

Kennwort:

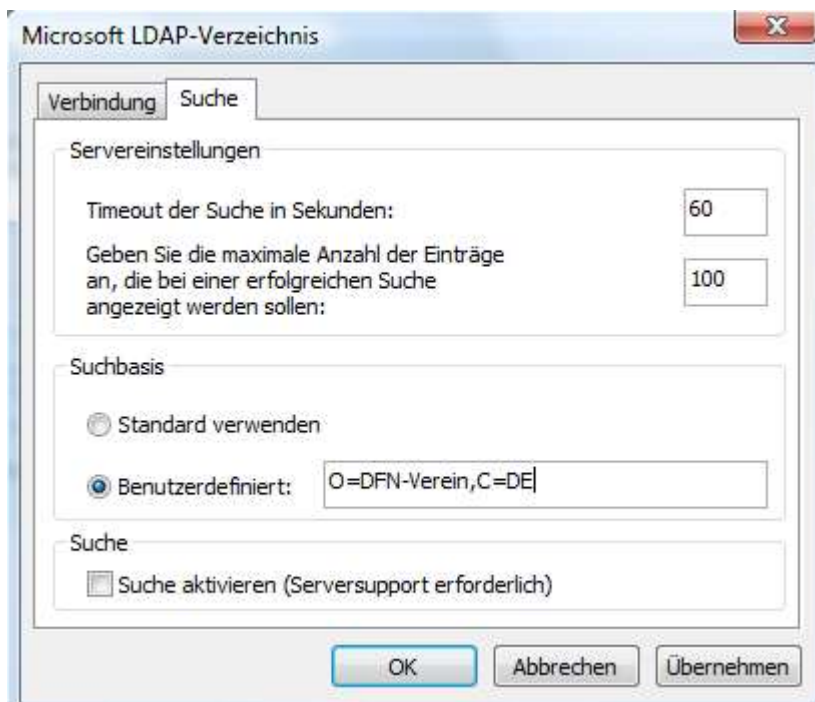
☐ Gesicherte Kennwortauthentifizierung (SPA) erforderlich

Weitere Einstellungen...

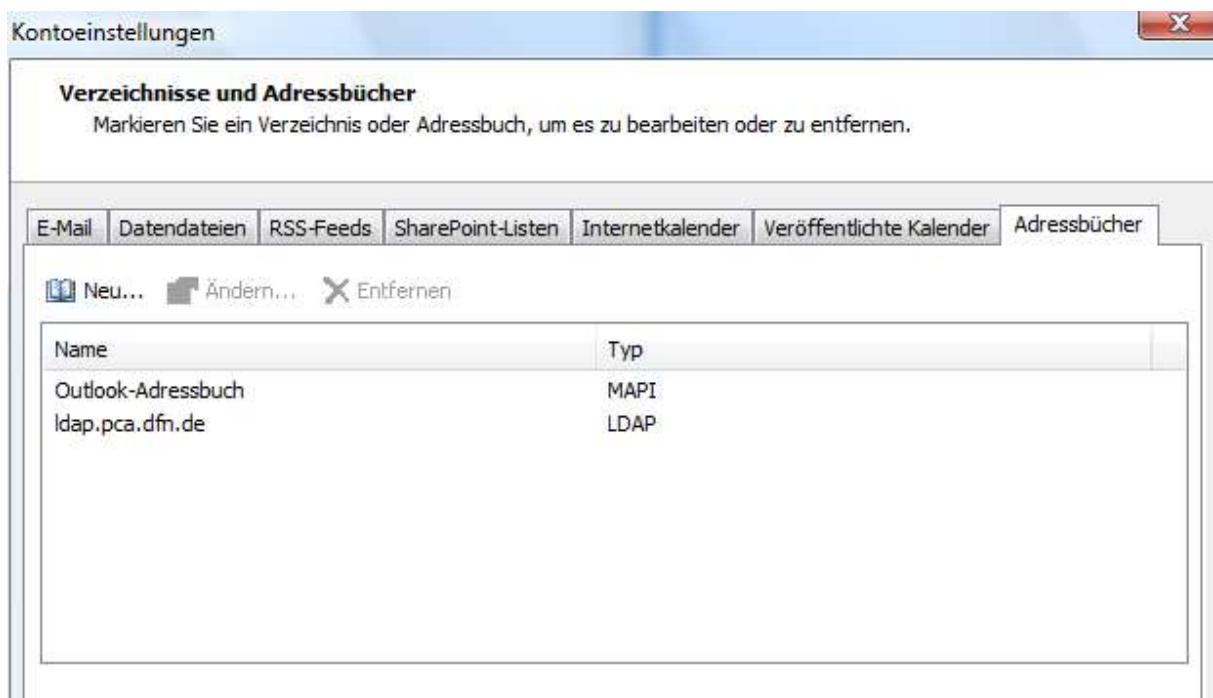
< Zurück Weiter > Abbrechen

Tragen Sie bitte im Tab **Verbindung** als Anzeigenname ldap.pca.dfn.de und unter Anschluss 636 ein.
Wählen Sie "Secure Sockets Layer verwenden" aus.

Tragen Sie im Tab **Suche** unter Suchbasis Benutzerdefiniert: **O=DFN-Verein,C=DE** ein. Klicken Sie dann auf OK.



Sie befinden Sie nun wieder im Fenster **Einstellungen für Verzeichnisdienste (LDAP)**. Klicken Sie auf **Weiter** und danach auf **Fertig stellen**. Damit haben Sie die Konfiguration erfolgreich abgeschlossen.



Sie können nun über das Adressbuch das LDAP Verzeichnis nach Personen und E-Mail-Adressen durchsuchen. Outlook bietet ihnen sehr umfangreiche Suchoptionen an, insbesondere, wenn Sie auf **Erweiterte Suche** klicken.

Namen auswählen: ldap.pca.dfn.de

Suchen: ☐ Nur Name ☒ Mehr Spalten **Adressbuch**

ldap.pca.dfn.de

Geben Sie die Schlüsselwörter für die Suche ein, und klicken Sie auf 'OK', um einen Such...

An ->

Cc ->

Bcc ->

Wenn Sie eine verschlüsselte E-Mail schicken wollen, klicken Sie bitte auf das blaue Schloss-Symbol im Fenster der neuen Nachricht. Beim Versenden durchsucht Outlook automatisch den DFN PKI LDAP-Verzeichnisdienst nach einem passenden Zertifikat und verschlüsselt die E-Mail, wenn ein Zertifikat zur E-Mail-Adresse vorhanden ist.