

PKI Konfigurationshilfe – Kurzübersicht 1/2

Zertifikat installieren	Windows	Linux	iOS	DFN LDAP Einrichten	
Zertifikatsspeicher	Systemsteuerung ↳ Internetoptionen ↳ Inhalte ↳ Zertifikate		Schlüsselbund	Thunderbird	Extras ↳ Adressbuch ↳ Datei ↳ Neu ↳ LDAP-Verzeichnis 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 Extras ↳ Einstellungen ↳ Verfassen ↳ Adressieren ↳ LDAP-Verzeichnis markieren und PKI-Adressbuch auswählen In den Kontoeinstellungen muss "Globale LDAP-Verzeichniseinstellungen verwenden" markiert sein
Firefox	Extras ↳ Einstellungen ↳ Erweitert ↳ Zertifikate				
Internet Explorer	Extras ↳ Internetoptionen ↳ Inhalte ↳ Zertifikate				
Thunderbird	Zertifikat importieren Extras ↳ Einstellungen ↳ Erweitert ↳ Zertifikate Zertifikat dem Konto zuordnen Kontoeinstellungen ↳ S/MIME ↳ Verfassen + LDAP des DFN einrichten (neues Adressbuch und Aktivieren bei Verfassen)			Outlook	Datei Kontoeinstellungen Adressbücher Neu LDAP Reiter "Verbindung" Servervname: ldap.pca.dfn.de Anzeigenname: ldap.pca.dfn.de Anschluss: 389 Reiter "Suche" Benutzerdefiniert: "O=DFN-Verein, C=DE"
Outlook	Zertifikat dem Konto zuordnen (Outlook 2010/2013) Datei ↳ Optionen ↳ Trust Center ↳ Einstellungen für das Trust Center ↳ E-Mail-Sicherheit ⇔ Stichwort: Verschlüsselte E-Mail Nachrichten Outlook 2007 Extras / Optionen ↳ Einstellungen Vertrauenszentrum ⇔ weiter wie oben + LDAP des DFN einrichten (Kontoeinstellungen => Adressbücher => neues Adressbuch)			Mac	Bisher kann Apple Mail noch nicht automatisch auf die Zertifikate aus dem LDAP Verzeichnis zugreifen. Lassen Sie sich deshalb von Ihrem E-Mail-Partner eine signierte E-Mail schicken. Dann wird automatisch das Zertifikat mittels der Schlüsselbundverwaltung gespeichert.

PKI Konfigurationshilfe – Kurzübersicht 2/2

Adobe einrichten	Windows	Linux	iOS
Grundeinstellungen	Bearbeiten ↳ Voreinstellungen ↳ Bei Kategorien: Unterschriften ⇒ Identitäten und vertrauenswürdige Zertifikate ↳ Prüfen, ob DTAG Root CA 2 vorhanden, bei nein: Wurzelzertifikat beim DFN herunterladen und als vertrauenswürdiges Zertifikat importieren ↳ Einstellungen für Vertrauenswürdigkeit bearbeiten: Aktivierung "vertrauenswürdiger Stamm" und "Zertifizierte Dokumente" ↳ Bei Kategorien: Sicherheit ⇒ Sicherheitseinstellungen ↳ Aktivieren "Sicherheitseinstellungen vom Server laden" und URL* eintragen ↳ Einstellungen herunterladen und Update einspielen		
Standardzertifikat für Unterschriften setzen	Bearbeiten ↳ Voreinstellungen ↳ Bei Kategorien: Unterschriften ==> Identitäten und vertrauenswürdige Zertifikate ↳ Unter Digitale IDs nach gewünschtem Zertifikat suchen und markieren ↳ Verwendungsoptionen => zum Unterschreiben verwenden anklicken		

* http://tu-dresden.de/die_tu_dresden/zentrale_einrichtungen/zih/dienste/datennetz_dienste/pki/tu_dresden_adobe_security

PKI aus Sicht des Nutzers - Anwendungsfälle

● Digitale Signatur

- E-Mails
 - Nach Installation im benötigten Zertifikatsspeicher und Konfiguration der Mail-Programme nutzbar
- PDF-Formulare
 - greift aus Zertifikatsspeicher des Betriebssystems zu
 - Auswahl des korrekten Zertifikats bei jeder Unterschrift notwendig

● Verschlüsselung / Entschlüsselung

- E-Mails
 - Nach Einrichtung des DFN-LDAP verschlüsselte Nachrichten verschicken
 - Nach Installation des eigenen Zertifikats verschlüsselte Nachrichten lesbar

● Authentifizierung

- Anmeldung an Web-Anwendungen
 - Nach Installation im benötigten Zertifikatsspeicher (Betriebssystem und/oder Webbrowser)