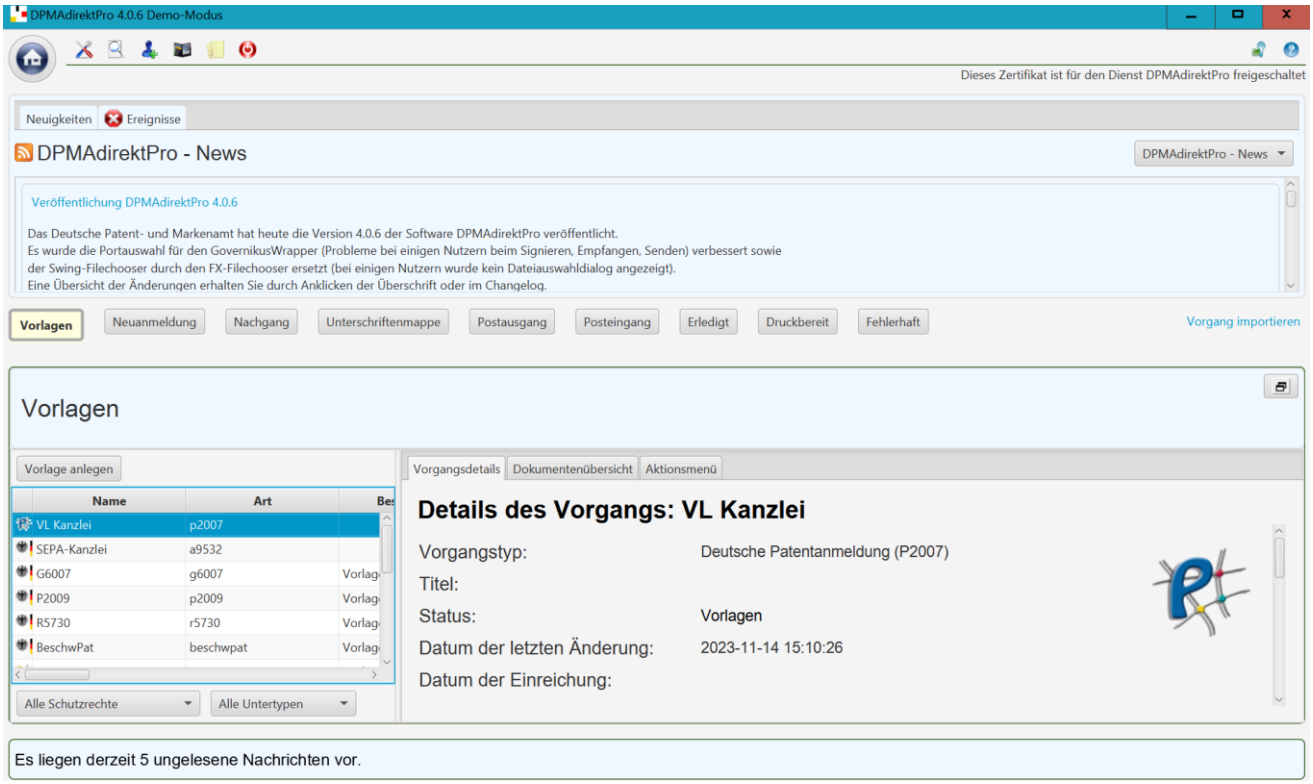
Deutsches
Patent- und Markenamt

# DPMAdirektPro

# Administratorhandbuch




Deutsches Patent- und Markenamt

Referat 2.4.3.a

80297 München

**Versionsverwaltung**

| Datum | Beschreibung |
|---|---|
| 01.06.2021 | Integration der Rechte- und Benutzerverwaltung;<br>Zugriff mehrerer Nutzer auf einem Client auf einem (Terminal-) Server |
| 24.08.2022 | Entfernung der Nutzung eines Clients auf Terminalserver (die dort beschriebenen Einstellungen erfolgen jetzt im Programm automatisch)<br>Anpassung: Vollzugriffsrechte werden nur für das integrierte Updatetool benötigt |
| 11.07.2023 | Kleinere Text Korrekturen.<br>Abbildungen mit Alternativtext versehen |
| 17.07.2024 | Aktion „Amtspost empfangen“ hinzugefügt<br>EPA-Karte nur noch bis max. 31.12.2024 |

**Ansprechpartner**

Deutsches Patent- und Markenamt
Referat 2.4.3
80297 München
E-Mail: DPMAdirekt@dpma.de

# Inhaltsverzeichnis:


**1 Zusammenfassung ..... 6**

**2 Voraussetzungen für die Nutzung von DPMAdirektPro ..... 7**

**3 Installation der Software, Datensicherungen ..... 8**

3.1 Entscheidung Single-User- oder Multi-User-Version ..... 8

3.1.1 Single-User (DPMAdirektPro – Desktop) ..... 8

3.1.2 Multi-User (Client – Server) ..... 8

3.2 Installation ..... 9

3.2.1 Installation der Single-User-Version (DPMAdirektPro – Desktop) ..... 9

3.2.2 Installation der Multi-User-Version (Client und Server) ..... 11

3.2.3 Mehrere Clients installieren bzw. mehrere Nutzer einrichten ..... 13

3.2.4 Unbeaufsichtigte Installation ..... 13

3.2.5 Deinstallation von DPMAdirektPro ..... 14

3.3 Der erste Programmstart von DPMAdirektPro ..... 16

3.4 Die Erstkonfiguration ..... 16

3.5 Ein neues Zertifikat erzeugen ..... 18

3.6 Datensicherung und Rücksicherung ..... 19

3.6.1 Datensicherung ..... 19

3.6.2 Rücksicherung ..... 20

3.7 Ersatz des Servers ..... 21

3.8 Wechsel von einer Einzelplatz- in eine Multi-User-Version ..... 21

**4 Das AdminTool ..... 22**

4.1 Das integrierte AdminTool ..... 22

4.1.1 Taskmenüpunkt „Einstellungen“ ..... 23

4.1.2 Taskmenüpunkt „Passwort für das AdminTool ändern“ ..... 23

4.1.3 Taskmenüpunkt „aktuelle Zertifikatszuordnung ändern“ ..... 23

4.1.4 Meldung „Benutzerzertifikat ist abgelaufen“ bzw. „Benutzerzertifikat wird ablaufen“ 25

4.2 Die Schnellstartleiste ..... 25

4.2.1 Das Menü „Aktionen“ ..... 26

4.2.2 Das Menü „Vorgangsverwaltung“ ..... 28

4.2.3 Das Menü „Zertifikatsverwaltung“ ..... 29

4.2.4 Das Menü „DB-Diagnostik“ ..... 29

**5 Rechte- und Benutzerverwaltung im AdminTool ..... 31**

5.1 Grundlagen der Rechte- und Benutzerverwaltung ..... 31

5.1.1 Aktivierung/Deaktivierung des Rechte- und Benutzerverwaltungssystems ..... 31

5.1.2 Benutzerverwaltung ..... 33

5.1.3 Rechtvergabe ..... 35

5.1.4 Programm-Login bei aktivierter Rechteverwaltung ..... 36

5.2 Die Passwort Verwaltung ..... 37

5.2.1 Passwort ändern ..... 37

5.2.2 Passwortsicherheit ..... 37

5.2.3 Das initiales Passwort ..... 38

5.2.4 Das Master Passwort ..... 38

5.2.5 Benutzer wechseln oder Passwort ändern ..... 38

5.3 Vorgänge und Aktionen ..... 39

5.4 Voreingestellte Rechte der Standard-Benutzerrollen ..... 40

**6 Nutzung der Zertifikate ..... 42**

6.1 Meldung: Gültigkeit des Zertifikats ist abgelaufen ..... 42

6.2 Das Verschlüsselungszertifikat ..... 42

6.2.1 Zugriffssteuerung auf die Vorgänge anhand eines Beispiels ..... 42

6.2.2 Sicherung (Backup) des Verschlüsselungszertifikats ..... 43

6.3 Das Signaturzertifikat (die Signaturkarte) ..... 43

**7 Fehlersuche und –behebung ..... 45**

7.1 Bekannte Probleme ..... 45

7.2 Fehlersuche im Debugmodus ..... 46

**8 Abbildungsverzeichnis: ..... 47**

Dieses Dokument beschreibt die Installation und Administrierung der Software DPMAdirektPro zur Erzeugung, Überprüfung und Versendung von elektronischen Schutzrechtsanmeldungen.
Eine Bedienungsanleitung finden Sie im Anwenderhandbuch.

## Verwendete Konventionen:

| Konvention | Bedeutung |
|---|---|
| ***Fett*** | auszuwählendes Menü oder Befehl |
| ***Menü→Befehl*** | Abfolge von Menüs und Befehlen, von links beginnend |
| ***Befehl\Befehl*** | Abfolge von Befehlen, von links beginnend |
| <Taste> | zu betätigende Taste auf der Tastatur |
| Doppelklicken | schnelles zweimaliges Klicken mit der linken Maustaste |
| Linksklicken | einmaliges Klicken mit der linken Maustaste |
| Rechtsklicken | einmaliges Klicken mit der rechten Maustaste |

## Copyrights

In der Dokumentation werden eingetragene Warenzeichen, Handelsnamen und Gebrauchsnamen verwendet. Auch wenn diese nicht als solche gekennzeichnet sind, gelten die entsprechenden Schutzbestimmungen.

## Fehler, Verbesserungsvorschläge

Sollten Ihnen Fehler auffallen, ist etwas unklar beschrieben oder haben Sie Verbesserungsvorschläge würden wir uns über eine Nachricht freuen.

# 1 Zusammenfassung

DPMAdirektPro ist ein kostenloses Computerprogramm des Deutschen Patent- und Markenamtes (DPMA) das es ermöglicht, eine rechtswirksame Schutzrechtsanmeldung online vorzunehmen und elektronische Dokumente zu Anmeldungen online nachzureichen. Neben einem PC mit Internetanschluss und der darauf installierten Software DPMAdirektPro wird eine qualifizierte Signaturkarte oder die Smartcard des Europäischen Patentamtes (EPA-Karte nur noch max. bis zum 31.12.2024) als Unterschriftsersatz benötigt.
Zusätzlich kann der elektronische Empfang der Dokumente vom DPMA beantragt werden.

**Die Anmeldung eines Schutzrechts erfolgt in sechs Schritten:**
**1. Antrag:** Der Anmelder füllt mit DPMAdirektPro einen elektronischen Antrag aus und fügt bei Bedarf Anlagen hinzu.

**2. Komprimierung und Überprüfung:** Das Programm fügt alle Dateien des Antrags zu einer komprimierten ZIP-Datei zusammen, dem elektronischen Antrag. Die Daten werden auf Vollständigkeit geprüft.

**3. Signatur:** Der Anmelder versieht im Programm den Antrag mit einer elektronischen Signatur nach dem Signaturgesetz ( = Unterschriftsersatz).

**4. Versenden:** Der Antrag wird in verschlüsselter Form über das Internet an das DPMA versendet. Das Verschlüsselungs-Protokoll OSCI und die dazu notwendigen Softwarebibliotheken wurden vom Bundesamt für Sicherheit in der Informationstechnik (BSI) zertifiziert.

**5. Signaturprüfung:** Das DPMA prüft die qualifizierte elektronische Signatur des eingegangenen Antrags mittels automatischen Abgleich mit der Datenbank des Trustcenters, das die qualifizierte Signaturkarte des Unterzeichners ausgestellt hat.

**6. Abschluss**: Bei erfolgreicher Eingangsprüfung erhält der Anmelder im Programm eine Benachrichtigung über den Empfang des Antrags. Das Prüfprotokoll, welches die qualifizierte elektronische Signatur bestätigt, kommt in die Schutzrechtsakte. Falls die Prüfung fehlschlägt, erhält der Anmelder eine Benachrichtigung über den bei der Prüfung aufgetretenen Fehler. Der Antrag gilt in diesem Fall als nicht eingereicht.

# 2 Voraussetzungen für die Nutzung von DPMAdirektPro

An die Hardware werden folgende Anforderungen gestellt:
Standard PC mit mindestens:

* mind. 4 GB RAM
* 1 GB freier Festplattenspeicher (Client-Version)
* mind. 2 GB freier Festplattenspeicher (Einzelplatz-Version)
* Grafik-Auflösung: 1280 x 1024 Pixel oder höher
* Breitband-Internetzugang (DSL oder vergleichbar)
* qualifizierte Signaturkarte oder Karte des Europäischen Patentamtes mit Kartenlesegerät und installierten Treibern

Folgende Betriebssysteme werden zurzeit unterstützt:

* Windows Server: alle aktuellen Versionen (64 bit)
* Windows: alle aktuellen Versionen (64 bit)

In der Multi-User-Version ist DPMAdirektPro ist eine klassische Client-Server-Anwendung.

Die Ausführung auf Terminalservern wird derzeit offiziell nicht unterstützt und erfolgt auf eigenes Risiko. Support kann in diesem Fall nur für den Betrieb und die Bedienung von DPMAdirektPro geleistet werden.

# 3 Installation der Software, Datensicherungen

Die jeweils neueste Version von DPMAdirektPro können Sie sich auf der Internetseite des DPMA herunterladen. Nutzen Sie dazu folgenden Link:
https://www.dpma.de/service/elektronische_anmeldung/dpmadirekt/downloads/index.html
Bevor Sie DPMAdirektPro installieren, müssen Sie sich entscheiden, mit welcher Version Sie arbeiten wollen. Eine Entscheidungshilfe dazu erhalten Sie im nächsten Abschnitt.

## 3.1 Entscheidung Single-User- oder Multi-User-Version

DPMAdirektPro wird in zwei verschiedenen Versionen angeboten. Die richtige Verwendung soll im Folgenden erklärt werden.

### 3.1.1 Single-User (DPMAdirektPro – Desktop)

Diese Version ist für den Einzelanmelder oder kleinere Kanzleien sinnvoll. Der Vorgang wird an einem Rechner komplett vom Entwurf bis zum Erhalt der Anmeldebenachrichtigung bearbeitet. Die Übertragung der Daten von einem Rechner zum anderen ist nur über die Export-/Importfunktion möglich. Auf dem Installationsrechner wird sowohl das Programm DPMAdirektPro als auch die für die Datenhaltung notwendige Datenbank installiert. Die Datenbank wird zusammen mit DPMAdirektPro gestartet und auch beim Schließen von DPMAdirektPro wieder beendet. So werden keine Systemressourcen unnötig beansprucht.

### 3.1.2 Multi-User (Client – Server)

Wenn mehrere Personen aufgabenverteilt an einem Vorgang arbeiten sollen, wird der Einsatz der Multi-User-Version empfohlen. Diese Version ist eine typische Client-Server-Anwendung, d. h. auf einen zentralen Server greifen mehrere Anwender mit ihren Clients zu. Die Daten zu den einzelnen Vorgängen werden zentral auf dem Server in einer Datenbank verwaltet. Jeder Client muss über das Intranet Zugang zu diesem Server haben. Der Server muss mindestens zu den Arbeitszeiten betriebsbereit sein, weil die einzelnen Clients Zugriff auf den Server benötigen. Sollte eine Firewall vor dem Server installiert sein, muss der Zugriff der Clients auf den Port 1527 freigeschalten werden. Auf den einzelnen Clients werden keine Daten gespeichert. Der Datenaustausch mit den Clients erfolgt über den Server. Ein mögliches Anwendungsszenario finden Sie im Abschnitt 5 und dort unter dem Punkt 6.2.1 Zugriffssteuerung auf die Vorgänge anhand eines Beispiels.
Es ist auch möglich, die Client- und Serverkomponenten zusammen auf einen Rechner zu installieren.

## 3.2 Installation

Im Folgenden wird die Installation von DPMAdirektPro beschrieben.

Bei der Installation des Treibers für den Kartenleser verfahren Sie bitte nach der Anleitung des Herstellers.

Das Installationsprogramm von DPMAdirektPro benötigt Administrator-Rechte. Die Installation startet durch Ausführen der Datei „DPMAdirektProxxx_Setup“ wobei xxx für die jeweilige Version steht. Wird beim Start festgestellt, dass keine Admin-Rechte vorliegen, bricht der Installer mit einer entsprechenden Fehlermeldung ab. Folgen Sie im Weiteren den Anweisungen auf dem Bildschirm und nehmen Sie die Lizenzbestimmungen an. Im dann folgenden Dialog (siehe Abbildung) müssen Sie bestimmen, welche Version installiert werden soll.

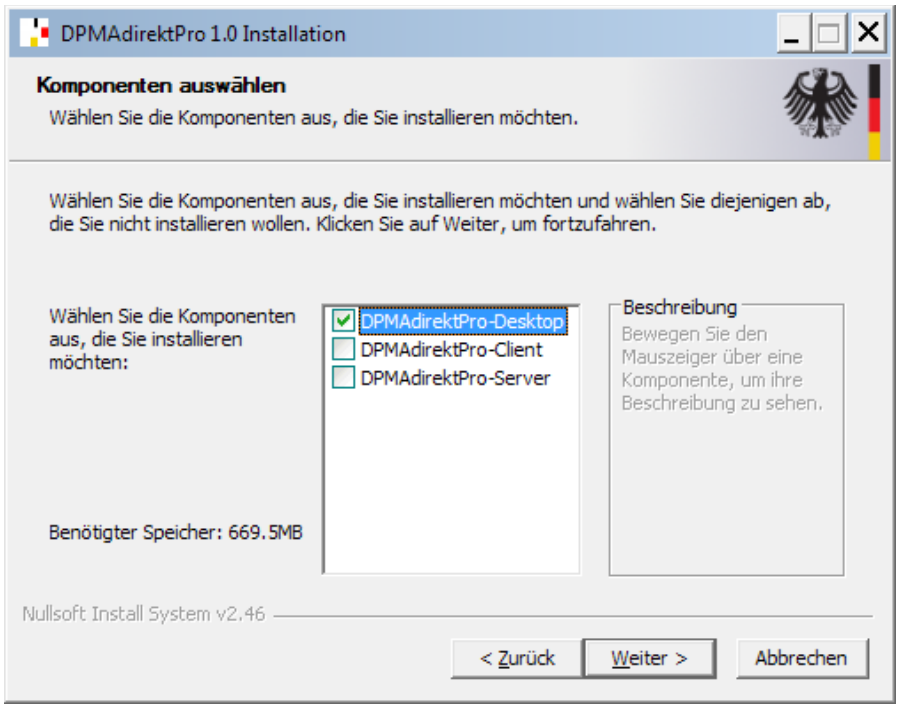



**Abbildung 1: Auswahl der Einzelplatzversion**

Je nach Auswahl lesen Sie bitte im entsprechenden Abschnitt weiter.

### 3.2.1 Installation der Single-User-Version (DPMAdirektPro – Desktop)

Soll die Einzelplatzversion installiert werden, wählen Sie bitte das oberste Kästchen aus. Im folgenden Fenster muss das Installationsverzeichnis ausgewählt werden. Sie können den Vorschlag übernehmen oder ein anderes Verzeichnis bestimmen. Folgen Sie den weiteren Anweisungen. Die Entscheidungen, die Sie noch treffen können sind in den einzelnen Fenstern erklärt.

Im letzten Fenster starten Sie durch ***Installieren*** den Installationsprozess.

**Beachten Sie:** Nutzer, die DPMAdirektPro auf diesem Rechner über das integrierte Updatetool aktualisieren wollen, benötigen Vollzugriff auf das Installationsverzeichnis. Dazu Rechtsklicken Sie im Explorer auf das Installationsverzeichnis (z.B.: C:\Programme\DPMAdirektPro) und wählen den Eintrag ***Eigenschaften*** und im sich öffnenden Fenster den Punkt ***Sicherheit*** aus. Jetzt wählen Sie im oberen Fenster den Nutzer ***Benutzer*** aus. Im unteren Fenster klicken Sie das Kästchen ***Vollzugriff*** in der Spalte ***Zulassen*** an.
Mit einem Klick auf ***OK*** werden die Einstellungen übernommen.
Alternativ können Sie jedem Nutzer, der mit DPMAdirektPro arbeiten soll den ***Vollzugriff*** gewähren.
Damit ist DPMAdirektPro installiert. Ein Neustart des Rechners ist nicht erforderlich.

### 3.2.2 Installation der Multi-User-Version (Client und Server)

Bei dieser Version müssen Sie festlegen, ob Sie nur die Client- oder Serverkomponente installieren wollen oder beide Komponenten auf einen Rechner. In einer größeren Arbeitsumgebung ist es sinnvoll, die Serverkomponente auch wirklich auf einen Server zu installieren.

**Serverinstallation:**

Für die Serverinstallation markieren Sie das entsprechende Feld (siehe Abbildung)

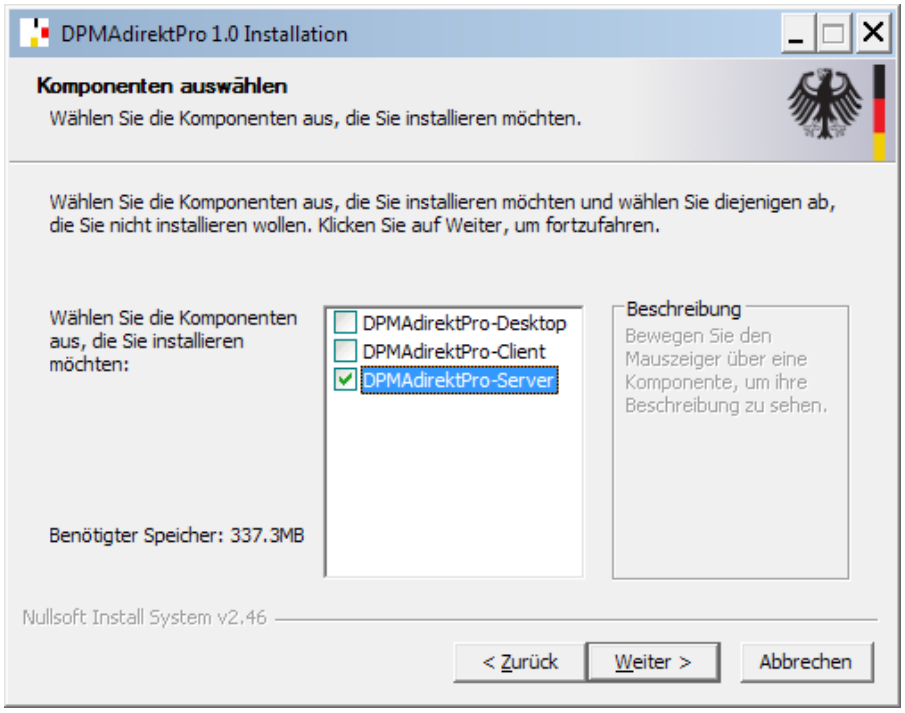



**Abbildung 2: Auswahl der Serverinstallation**

Im folgenden Fenster muss das Installationsverzeichnis ausgewählt werden. Sie können den Vorschlag übernehmen oder ein anderes Verzeichnis bestimmen. Im letzten Fenster starten Sie durch ***Installieren*** den Installationsprozess. Nach der Installation müssen Sie den Server (Rechner) neu starten. Die Datenbank wird beim Neustart als Dienst eingerichtet. Beachten Sie, dass für die Zugriffe der Clients auf diesen (internen) Datenbankdienst der Port 1527 zugänglich sein muss (Firewall, Routerkonfiguration, usw.).

Wurde der Dienst (DPMAdirektServicePro64) ordnungsgemäß gestartet, enthält es im Verzeichnis ***Installationsverzeichnis\Server*** die Dateien „DPMAdirektService.log“ und „derby.log“ jeweils mit etwa folgendem Inhalt:

*Apache Derby Network Server 10.2.2.0 - (485682) wurde gestartet und ist seit 2018-04-03 09:12:17.187 GMT bereit, Verbindungen am Port 1527 zu akzeptieren.*

**Abbildung 3: DPMAdirektService.log**

Zur Kontrolle können Sie in der Kommandozeile den Befehl ***netstat –a*** eingeben. In der Ausgabe muss der Port 1527 mit dem Status „Abhören“ aufgeführt sein.

```
C:\>netstat –a
Aktive Verbindungen
  Proto  Lokale Adresse        Remoteadresse        Status
  TCP    server:1527           server:0             ABHÖREN
```

**Abbildung 4: Den Datenbankport prüfen**

**Clientinstallation:**

Es wird empfohlen, vor der Installation des/der Clients den Server wie oben beschrieben zu installieren.

Wählen Sie im Auswahlfenster (siehe Abbildung 2: Auswahl der Serverinstallation) ***DPMAdirektPro-Client*** aus. Im Weiteren muss wieder das Installationsverzeichnis bestimmt werden. Folgen Sie den weiteren Anweisungen. Die Entscheidungen, die Sie noch treffen können sind in den einzelnen Fenstern erklärt. Im letzten Fenster (siehe Abbildung) muss auf der rechten Seite die Serveradresse eingetragen werden.

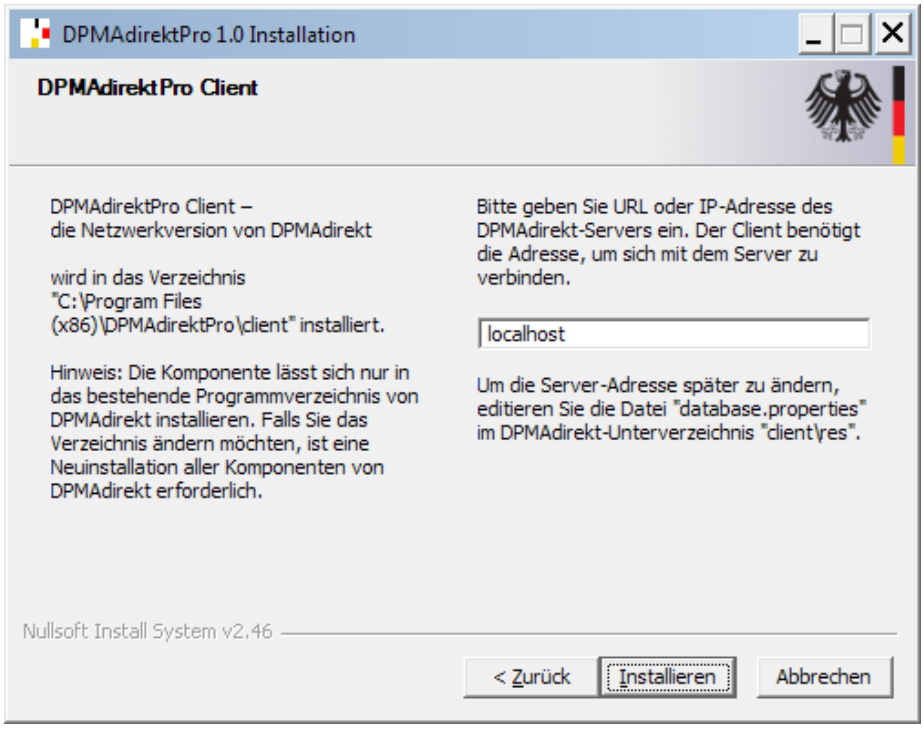



**Abbildung 5: Serveradresse auswählen**

Wenn Server und Client auf dem gleichen Rechner installiert werden, können Sie den Eintrag ***localhost*** übernehmen. Ansonsten muss hier die Adresse des Servers eingetragen werden. Bei funktionierender Namensauflösung im Netzwerk kann der Servername eingetragen werden, ansonsten verwenden Sie die IP-Adresse des Servers (z.B.: 192.168.140.100).
Anschließend startet ***Installieren*** wieder den Installationsprozess.
**Beachten Sie:** Nutzer, die DPMAdirektPro auf diesem Rechner über das integrierte Updatetool aktualisieren wollen, benötigen Vollzugriff auf das Installationsverzeichnis. Dazu Rechtsklicken Sie im Explorer auf das Installationsverzeichnis (z.B.: C:\Programme\DPMAdirektPro) und wählen den Eintrag ***Eigenschaften*** und im sich öffnenden Fenster den Punkt ***Sicherheit*** aus. Jetzt wählen Sie im oberen Fenster den Nutzer ***Benutzer*** aus. Im unteren Fenster klicken Sie das Kästchen ***Vollzugriff*** in der Spalte ***Zulassen*** an.
Mit einem Klick auf ***OK*** werden die Einstellungen übernommen.
Alternativ können Sie jedem Nutzer, der mit DPMAdirektPro arbeiten soll den ***Vollzugriff*** gewähren.
Damit ist DPMAdirektPro installiert. Ein Neustart des Rechners ist nicht erforderlich.

### 3.2.3 Mehrere Clients installieren bzw. mehrere Nutzer einrichten

Für die Installation mehrerer Clients kann der Installationsablauf vereinfacht werden.
Installieren Sie dazu wie oben beschrieben einen Client und starten Sie diesen. Dabei wird unter „c:\Dokumente und Einstellungen\nutzername“ das Verzeichnis „DPMA“ und dort „DPMAdirekt“ angelegt, wobei „nutzername“ der aktuelle Nutzer ist. Dieses „DPMA“-Verzeichnis brauchen Sie nur in das persönliche Verzeichnis der Nutzer kopieren, die mit DPMAdirekt auf diesem Rechner arbeiten sollen. Anschließend müssen noch in diesem Verzeichnis in der Datei \DPMAdirekt\UserConfig.properties die Pfade an den neuen Benutzernamen anpasst werden. Natürlich könnte diese Anpassung auch ein Kopierscript übernehmen. Dadurch entfällt die Konfiguration beim ersten Start von DPMAdirektPro. Sollen für einen Benutzer andere Einstellungen oder ein anderes Zertifikat gelten, kann dies nach dem Programmstart über die Programmkonfiguration (bitte an entsprechender Stelle nachlesen) geändert werden.
Bei einer Installation auf anderen Rechnern (Clients) brauchen Sie nur vor der Installation das Verzeichnis in die Nutzerverzeichnisse zu kopieren.

### 3.2.4 Unbeaufsichtigte Installation

Wird das Setup-Programm mit dem Schalter /S und weiteren Steuerparametern aufgerufen, so wird eine unbeaufsichtigte Installation (silent installation) durchgeführt. Wird nur der Schalter angegeben (z.B. DPMAdirektPro_Setup_1.0.exe /S), so wird ein Informationsdialog (siehe Abbildung) angezeigt:

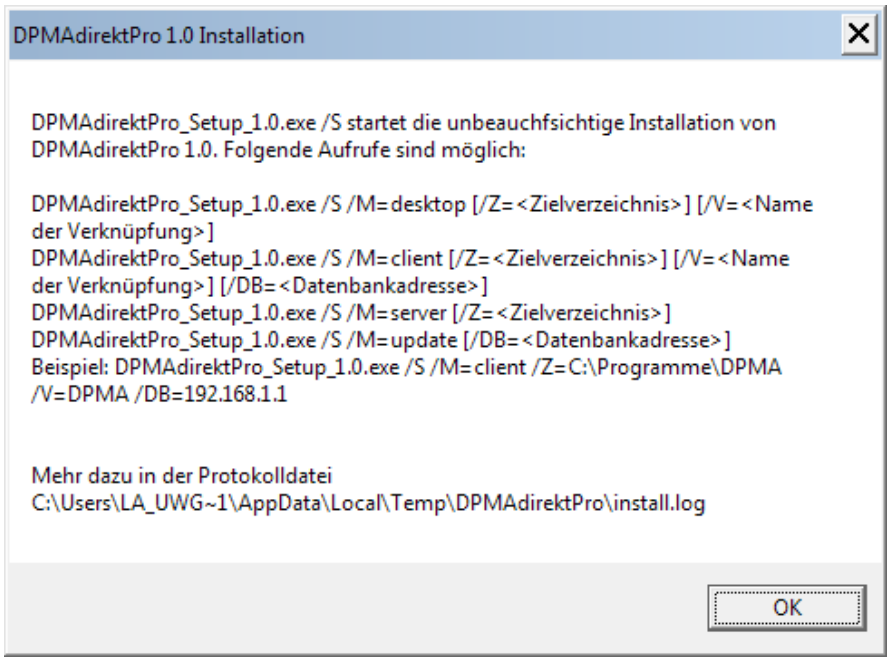



**Abbildung 6: Infodialog zur unbeaufsichtigten Installation**

Folgende Parameter sind möglich (bitte große Buchstaben verwenden!):

- /S obligatorisch — Aufruf der unbeaufsichtigten Installation
- /M obligatorisch — Installationsmodul (Art der Installation)
  - desktop — Einzelplatzversion
  - client — Client der Multi-User-Version
  - server — Server der Multi-User-Version
  - update — ein Update der installierten Module
- /Z fakultativ — Zielverzeichnis (default: c:\Programme\DPMAdirektPro)
- /V fakultativ — Verknüpfungsname (default: DPMAdirektPro)
- /DB fakultativ — Datenbankadresse (default: localhost)

### 3.2.5 Deinstallation von DPMAdirektPro

Für das Deinstallieren von DPMAdirekt müssen Sie wieder Administratorrechte besitzen. Das Deinstallieren kann wie in Windows üblich über ***Einstellungen->Systemsteuerung->Software*** oder über den direkten Aufruf des Installationsprogramms erfolgen. Im erscheinenden Fenster (siehe Abbildung) können Sie die zu deinstallierende Komponente auswählen. Haben Sie Client und Server installiert und wollen Sie beides deinstallieren, können Sie beides zusammen auswählen.

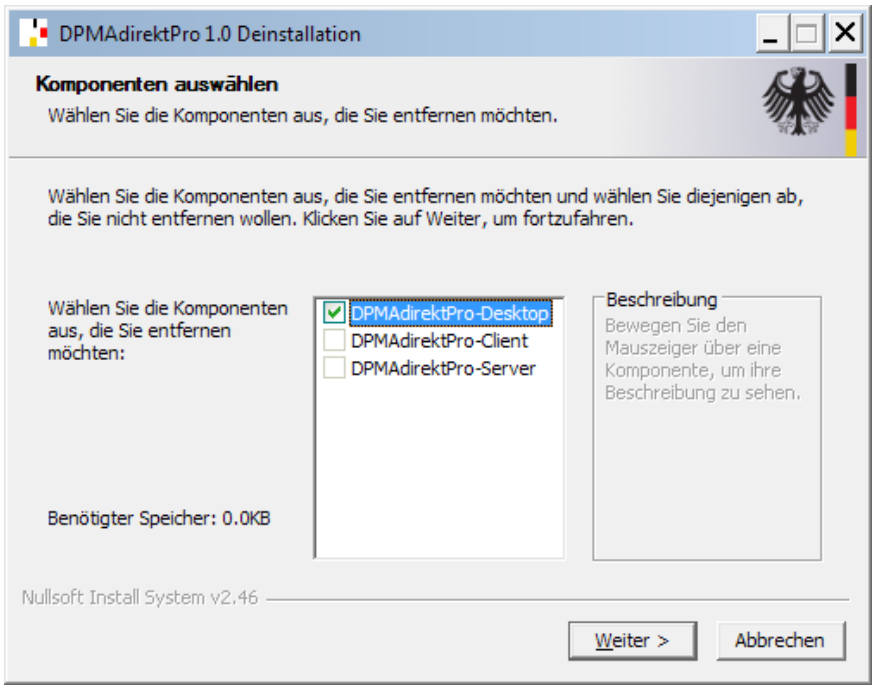



**Abbildung 7: Auswahl der zu deinstallierenden Komponenten**

Im Verlauf der Deinstallation müssen Sie angeben, ob die verwendete Datenbank für eine spätere Verwendung erhalten werden soll. In diesem Fall wird diese nicht gelöscht. Sollten im Dateisystem noch Dateien oder Verzeichnisse nicht automatisch gelöscht worden sein, werden diese beim nächsten Rechnerneustart entfernt. Bei der Deinstallation des Servers wird der Dienst „DPMAdirektServicePro64“ erst beim nächsten Serverneustart entfernt. Daher muss bei der Serverversion der Server nicht unbedingt während des Deinstallationsprozesses gebootet werden (wie vom Deinstallationsprogramm vorgeschlagen).

## 3.3 Der erste Programmstart von DPMAdirektPro

Durch den Installationsprozess wurde eine Verknüpfung auf dem Bildschirm abgelegt und ein Eintrag unter ***Start->Programme*** angelegt. Sie können DPMAdirektPro über die Verknüpfung oder über den Startmenüeintrag öffnen.
Beim ersten Programmstart muss DPMAdirektPro konfiguriert werden. Dazu startet ein graphisches Hilfsprogramm (siehe nächster Abschnitt). Nach erfolgreicher Erstkonfiguration startet DPMAdirekt-Pro und Sie sehen die Programmoberfläche.
Hilfe für die Vereinfachung bei der Installation mehrerer Clients erhalten Sie im Abschnitt 3.2.3 Mehrere Clients installieren.

## 3.4 Die Erstkonfiguration

Wurde beim Programmstart keine gültige Nutzerkonfiguration (C:\Dokumente und Einstellungen\userLogin\Dpma\DPMAdirekt) gefunden, wird ein graphisches Hilfsprogramm gestartet.

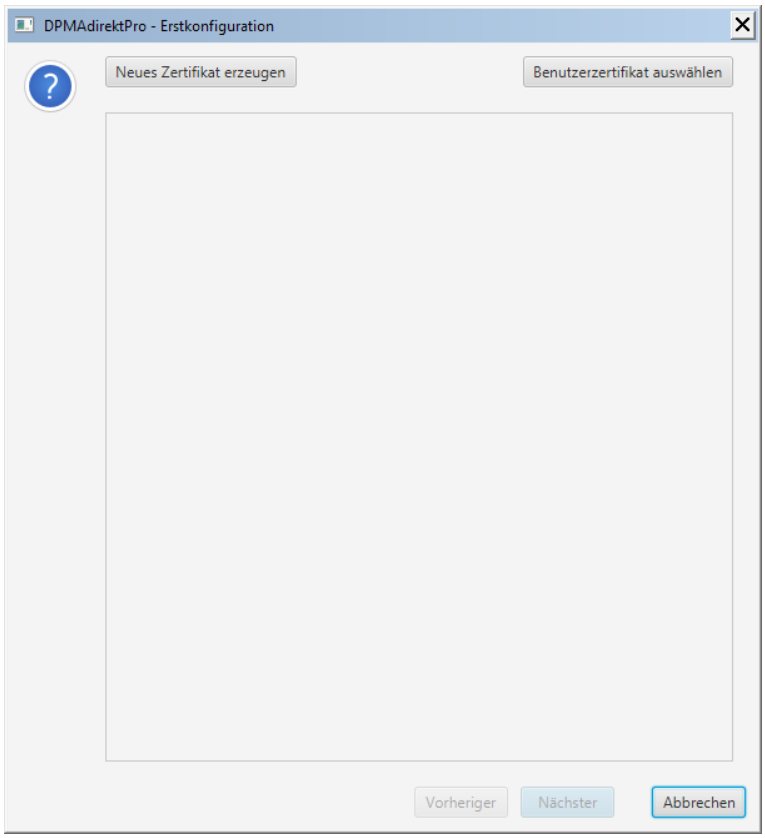



**Abbildung 8: Erstkonfiguration – Zertifikatsauswahl**

Im ersten Dialog haben Sie die Möglichkeit ein neues (Benutzer-) Zertifikat zu erzeugen oder ein schon vorhandenes auszuwählen. Soll ein schon vorhandenes Zertifikat genutzt werden, so kann man dieses über entsprechende Schaltfläche auswählen. Es öffnet sich ein Dialog, in dem Sie entweder ein

Zertifikat aus der Datenbank auswählen oder mittels Dateiauswahldialog ein Zertifikat aus dem Dateisystem laden können.
Wenn das in DPMAdirektPro zu nutzende Zertifikat ausgewählt wurde, muss die PIN für das gewählte Zertifikat eingegeben werden. Anschließend werden auf der Konfigurationsseite die Zertifikatsinformationen angezeigt. Die Auswahl des Zertifikats kann beliebig oft wiederholt werden. Wenn ein neues Zertifikat erzeugt werden soll, so klicken Sie auf die entsprechende Schaltfläche. Das Erzeugen eines Zertifikats ist im Abschnitt 3.5 Ein neues Zertifikat erzeugen beschrieben.
Ist die Zertifikatsauswahl beendet, wird mit ***Weiter*** auf die nächste Seite gewechselt.

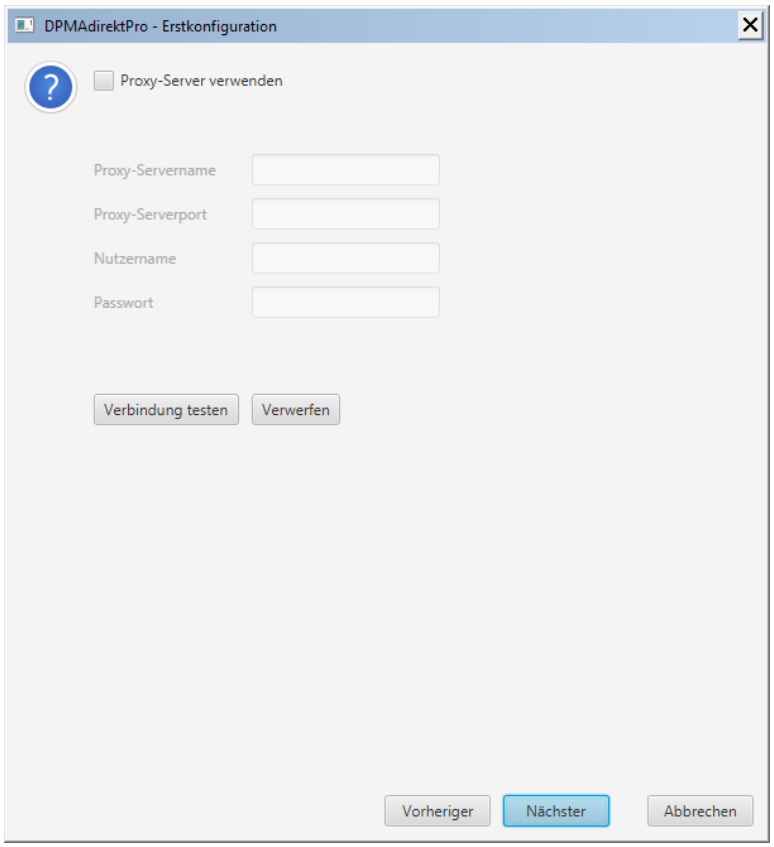



**Abbildung 9: Erstkonfiguration – Proxy-Konfiguration**

Hier können die notwendigen Angaben für einen Proxyserver gemacht werden. Ein Proxyserver ist ein „Vermittlungsrechner“ zwischen dem internen Intranet und dem Internet und dient vor allem dem Schutz des internen Netzes. Er wird in der Regel in größeren Firmen oder Kanzleien verwendet. Ob Sie einen Proxy-Server verwenden müssen, können Sie mit einem Klick auf ***Verbindung testen*** prüfen. Wenn Sie eine Erfolgsmeldung erhalten, können Sie ohne weitere Eingaben auf ***Nächster*** klicken.
Wenn die Checkbox ***Proxy-Server verwenden*** aktiviert wurde, sind mindestens die Einträge ***Proxy-Servername*** und ***Proxy-Serverport*** notwendig. Mit der Schaltfläche ***Verbindung testen*** kann gleich die Richtigkeit der gemachten Angaben kontrolliert werden. Mit ***Nächster*** wird die Erstkonfiguration verlassen und das Programm DPMAdirektPro gestartet.

## 3.5 Ein neues Zertifikat erzeugen

Es ist hier möglich, ein neues Benutzerzertifikat für DPMAdirektPro zu erzeugen.

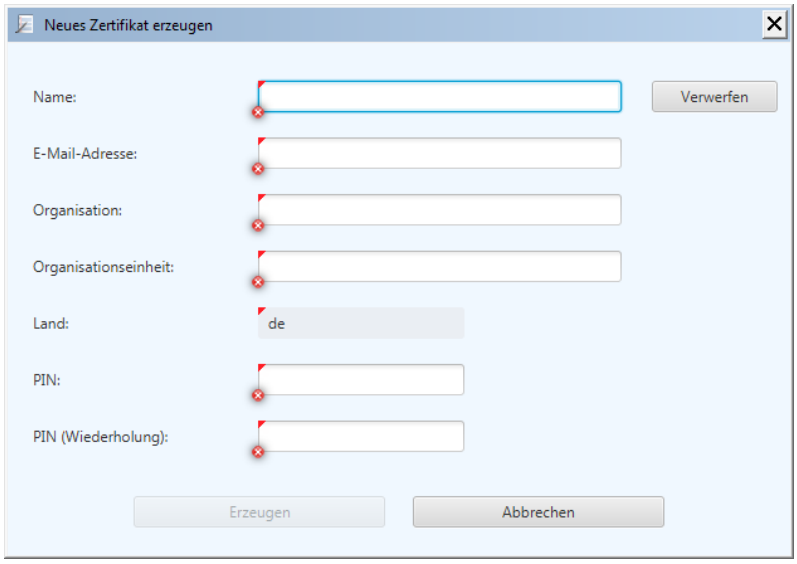



**Abbildung 10: Ein neues Benutzerzertifikat erzeugen**

Die Angaben sind frei wählbar. Als E-Mail-Adresse empfiehlt es sich, eine wirklich genutzte Adresse zu verwenden. Beachten Sie bei der PIN-Vergabe, dass die PIN für das spätere Anmelden am Programm benötigt wird.

Wenn alle Angaben den Anforderungen entsprechen, werden die roten Markierungen an den einzelnen Feldern entfernt und die Schaltfläche ***Erzeugen*** frei gegeben. Sind noch Fehler vorhanden, so sind die fehlerhaften Felder rot markiert. Durch ein Verweilen des Mauszeigers auf der Markierung erfolgt eine kurze Fehlerausgabe als so genannter Tooltip.

Mit ***Erzeugen*** wird das Zertifikat generiert und ein Dialog zur Verwendung des neuen Zertifikats angezeigt.

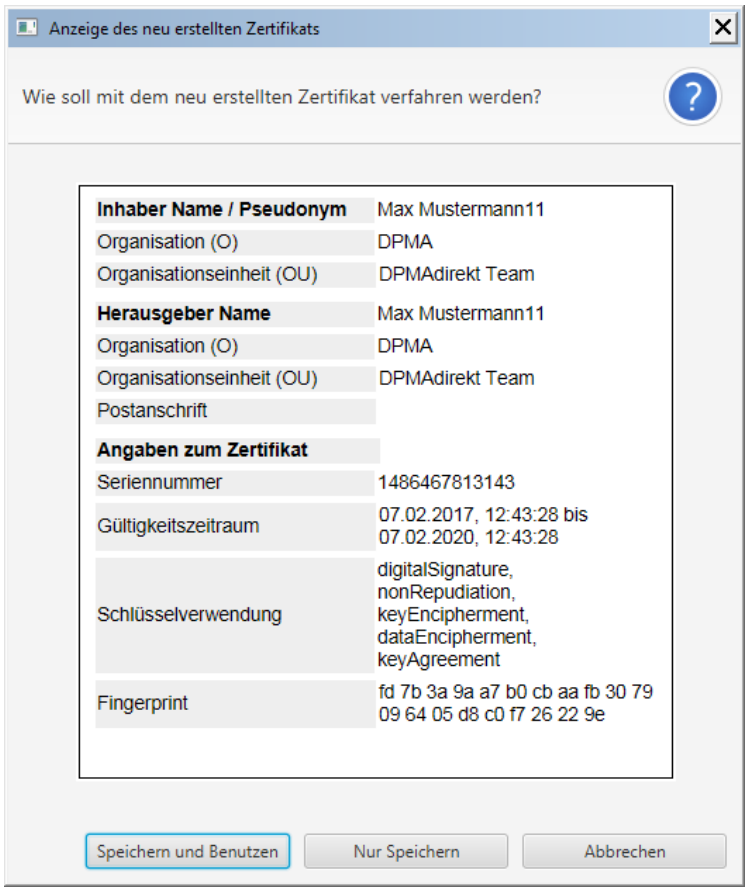



**Abbildung 11: Dialog zur Verwendung des neuen Zertifikats**

***Speichern und Benutzen*** speichert das neue Zertifikat in der Datenbank ab und setzt es in DPMAdirektPro als aktives Zertifikat.

**Achtung:** Nach dem Ändern werden die Vorgänge, die unter dem alten Zertifikat sichtbar waren, jetzt nicht mehr angezeigt!

***Nur Speichern*** speichert das neue Zertifikat in der Datenbank ab. Im Programm selbst wird weiter mit dem alten Benutzerzertifikat gearbeitet.

## 3.6 Datensicherung und Rücksicherung

### 3.6.1 Datensicherung

Sämtliche Daten (Anmeldungen, Adressbucheinträge, Zertifikate) werden bei DPMAdirektPro in einer Datenbank gespeichert. Diese befindet sich im kompletten Verzeichnis ***transactiondb***. Bei einer Einzelplatzversion (desktop) liegt dieses Verzeichnis auf dem Rechner im DPMAdirektPro-Installationsverzeichnis\desktop\transactiondb (z.B. C:\Programme\DPMAdirektPro\desktop\), bei einer Multiuserversion auf dem Server im DPMAdirektPro-Installationsverzeichnis\server\transactiondb (z.B. C:\Programme\DPMAdirektPro\server\).

Für eine Sicherung der Daten ist es ausreichend, in einer Zeit, in der möglichst keine Schreibzugriffe erfolgen, einfach das komplette Verzeichnis ***transactiondb*** zu kopieren.
Bei einer Multi-User-Version sollten Sie vor der Sicherung auf dem Server den Dienst ***DPMAdirekt-ProService64*** in der Dienstesteuerung anhalten und nach der Sicherung bitte wieder starten.

### 3.6.2 Rücksicherung

Voraussetzung für die Rücksicherung:

Einzelplatzversion: DPMAdirektPro wurde beendet

Multiuserversion: Auf dem Server wurde in der Dienstesteuerung der Dienst DPMAdirektService64 angehalten. Nach der Rücksicherung ist dieser wieder zu starten.

Bei einer Rücksicherung darf das aktuelle Verzeichnis ***transactiondb*** nicht durch die gesicherte Version überschrieben werden! Dabei kann es zu einem inkonsistenten Zustand der Datenbank kommen. Das aktuelle Verzeichnis sollte zuerst umbenannt werden (z.B. transactiondb.old). Jetzt wird die gesicherte Version in das Verzeichnis ***desktop*** bzw ***server*** kopiert. Somit gibt es dann die Verzeichnisse transactiondb und transactiondb.old.
War die Rücksicherung erfolgreich, kann anschließend das alte Verzeichnis (transactiondb.old) gelöscht werden.

## 3.7 Ersatz des Servers

Soll bei einer Multiuserversion der Server ersetzt werden, so können die Daten wie folgt „mitgenommen“ werden:

- Installieren Sie auf dem neuen Server den Serveranteil laut Anleitung.
- Sichern Sie auf dem alten Server die Datenbank wie im Punkt 3.6.1 Datensicherung beschrieben.
- Rücksichern Sie die Datenbank wir im Abschnitt 3.6.2 beschrieben.

Wenn der neue Server einen neuen Namen oder eine geänderte IP-Adresse erhalten hat, so muss diese Änderung auch auf den einzelnen Clients eingetragen werden.
Dies erfolgt in der Datei database.properties welche sich auf dem Client im DPMAdirektPro-Installationsverzeichnis\client\res\ befindet.
Beispiel:
url=jdbc:derby://192.168.101.63:1527/transactiondb;create=false;

Da der Eintrag auf allen Clients gleich ist, kann eine Datei angepasst und dann auf die anderen Clients verteilt werden.

## 3.8 Wechsel von einer Einzelplatz- in eine Multi-User-Version

- Installieren Sie auf dem Server den Serveranteil laut Anleitung.
- Sichern Sie die Datenbank der Einzelplatzversion, die Sie auf dem Server verwenden wollen wie im Punkt 3.6.1 Datensicherung beschrieben.
- Rücksichern Sie die Datenbank wir im Abschnitt 3.6.2 beschrieben.
- Installieren Sie auf den Rechnern mit dem Setup-Programm die Clients

# 4 Das AdminTool

In DPMAdirektPro wurde ein eigenes AdminTool integriert. Wir haben die Funktionalitäten des alten separaten AdminTools hierher übernommen und noch erweitert.
Das separate AdminTool wird daher nicht mehr zur Verfügung gestellt und auch nicht mehr unterstützt. Sollte es noch vorhanden sein, bitte verwenden Sie dieses nicht mehr!
Der Zugang zu diesem Bereich ist durch ein Passwort geschützt. Sollten Sie schon mit dem alten separaten AdminTool gearbeitet haben, so geben Sie hier das dort verwendete Passwort ein.

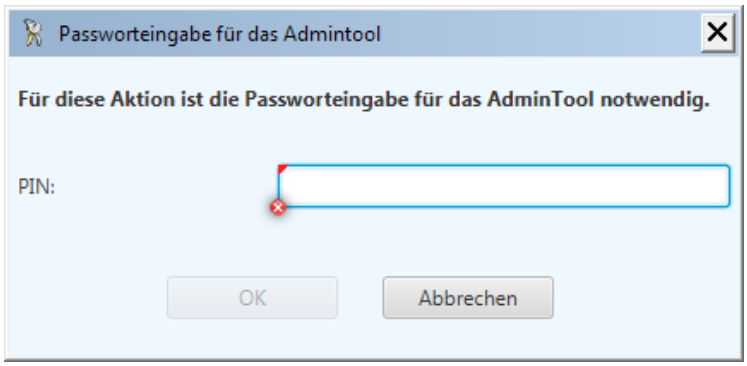



**Abbildung 12: Passworteingabe für das AdminTool**

Ist noch kein Passwort hinterlegt, so erscheint ein Dialog zur Passwort-Festlegung.
Aus Sicherheitsgründen empfehlen wir hier nicht das gleiche Passwort wie für das Login in das Programm zu wählen!
Die Funktionen des AdminTools werden im folgenden Abschnitt 4.1 erläutert.

## 4.1 Das integrierte AdminTool

Nach dem erfolgreichen Anmelden sehen Sie die Oberfläche des AdminTools.
Diese entspricht im Aufbau der Oberfläche des Hauptprogramms DPMAdirektPro und wird auch so bedient. In der folgenden Abbildung sind die aktuellen Möglichkeiten nach Klick auf das Häuschen links oben dargestellt.

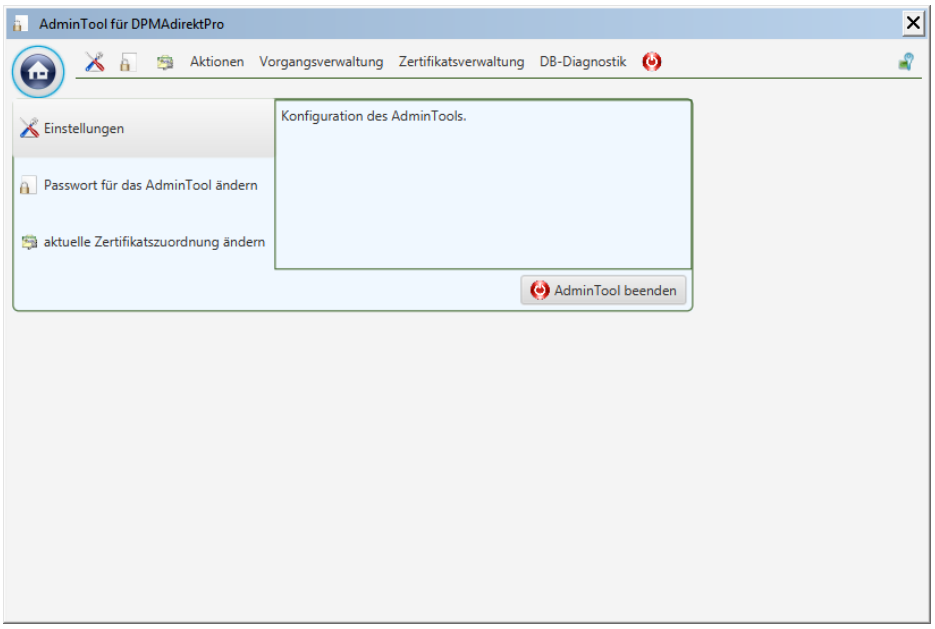



**Abbildung 13: Die Oberfläche des AdminTools**

### 4.1.1 Taskmenüpunkt „Einstellungen“

Momentan gibt es hier nur den folgenden Eintrag.

***Rechtesteuerung ermöglichen:*** Hier wird ab der DPMAdirektPro-Version 3.0 die integrierte Rechte- und Rollenverwaltung aktiviert bzw. deaktiviert (siehe auch Abschnitt 5 Rechte- und Benutzerverwaltung im AdminTool). Im deaktivierten Zustand darf jeder Benutzer alles.

Nach Aktivierung der Steuerung können sich in DPMAdirektPro nur noch Benutzer anmelden, denen in der Rechteverwaltung ein Zugriff gestattet wurde. Nutzer, die in der Rechteverwaltung nicht aufgeführt sind, haben dann keinen Zugriff mehr auf das Programm.

### 4.1.2 Taskmenüpunkt „Passwort für das AdminTool ändern“

Hier kann das Passwort für das AdminTool in der Datenbank geändert werden. Die Änderung dieses Passworts betrifft nur den Zugang zum AdminTool und nicht das Login des Programms DPMAdirektPro!

### 4.1.3 Taskmenüpunkt „aktuelle Zertifikatszuordnung ändern“

Hier kann ein neues Zertifikat erstellt und die Vorgänge des aktuellen Zertifikats diesem neuen zugeordnet werden.

**Hinweis:**

Ein Zertifikat, welches für den Pro-Dienst (elektronische Dokumentenzustellung des DPMA) benutzt wird, kann hier nicht geändert werden. Das geht nur im Registrierungsassistenten des Hauptprogramms (blaues Männchen).

Beim Anlegen eines Vorgangs wird dieser mit dem Zertifikat, das aktuell in DPMAdirektPro auf diesem PC verwendet wird, verknüpft (siehe auch 6.2.1 Zugriffssteuerung auf die Vorgänge anhand eines Beispiels).

Mit der Aktion ***aktuelle Zertifikatszuordnung ändern*** werden alle Vorgänge des aktuellen Zertifikats dem neuen Zertifikat in der Datenbank zugeordnet.

**Achtung:** Durch diese Zuordnungsänderung können alle Benutzer, die an DPMAdirektPro noch mit dem alten Zertifikat angemeldet sind, die Vorgänge solange nicht mehr sehen, bis sie ebenfalls auf das neue Zertifikat gewechselt haben.

Nach Aufruf dieses Punktes wird zuerst automatisch ein Abholen aller für das alte Zertifikat auf dem DPMA-Server hinterlegten Nachrichten durchgeführt.

Anschließend erscheint ein Dialog zur Zertifikatsauswahl.

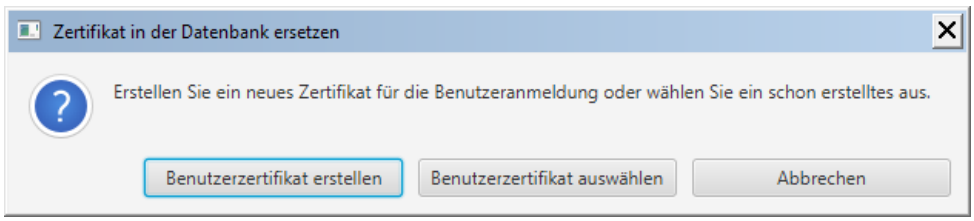



**Abbildung 14: Zertifikatsauswahl für das Ändern der Zuordnung**

***Benutzerzertifikat erstellen*** ruft den Dialog zur Erstellung eines neuen Zertifikats auf.

***Benutzerzertifikat auswählen*** ruft den Dialog zur Zertifikatsauswahl.

Nachdem das neue Zertifikat erstellt bzw. ausgewählt wurde, werden die Zertifikatsdaten nochmals in einem Informationsdialog angezeigt. Hier wird gegenübergestellt, welches aktuelle Zertifikat Sie durch das neue Zertifikat ersetzen wollen.

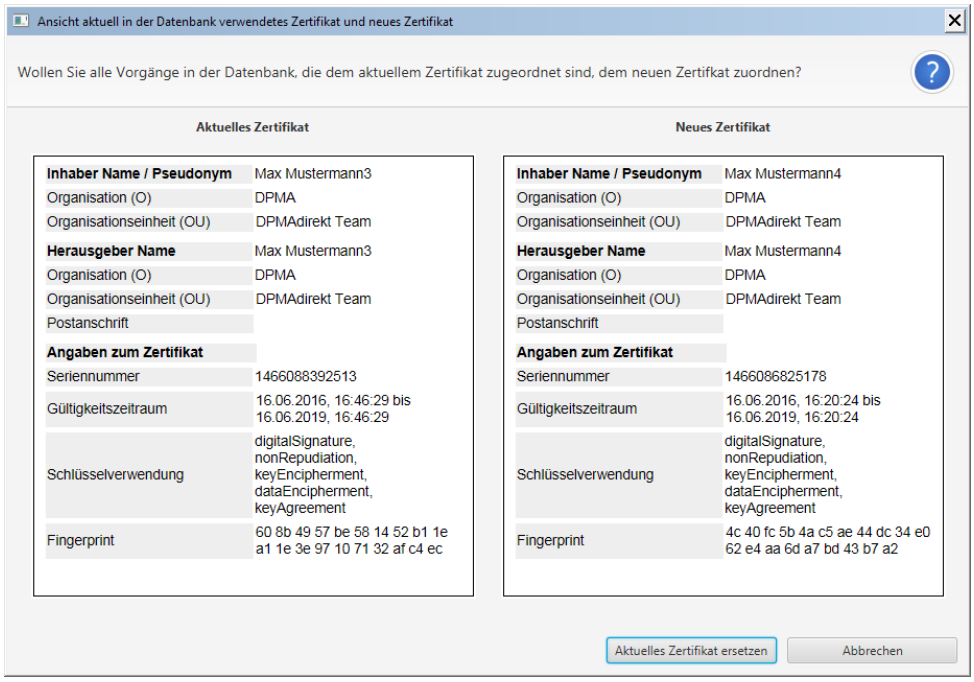



**Abbildung 15: Gegenüberstellungsdialog zum Zertifikatsersetzen**

Mit der Schaltfläche ***Aktuelles Zertifikat ersetzen*** wird dann das Ersetzen in der Datenbank durchgeführt. Anschließend wird die Anzahl der ersetzten Vorgänge angezeigt.

### 4.1.4 Meldung „Benutzerzertifikat ist abgelaufen“ bzw. „Benutzerzertifikat wird ablaufen“

Wenn das Zertifikat ist für den Pro-Dienst (elektronischer Dokumentenempfang) angemeldet ist, so müssen Sie es über den Pro-Assistenten wechseln (siehe DPMAdirektPro-Benutzerhandbuch Abschnitt 4.7.2.3 Zertifikat für den elektronischen Dokumentenempfang ändern.

Ansonsten verfahren Sie wie im vorherigen Abschnitt 4.1.3 Taskmenüpunkt „aktuelle Zertifikatszuordnung ändern“ beschrieben.

## 4.2 Die Schnellstartleiste

Wie beim Hauptprogramm befindet sich auch im AdminTool-Bereich oben eine Schnellstartleiste:

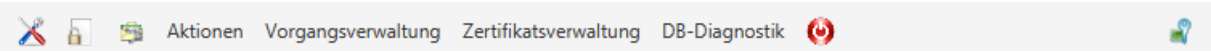



**Abbildung 16: Die Schnellstartleiste**

Sie können auf die Icons klicken um Aktionen auszuführen. Ein Klick auf einen Menüeintrag öffnet das entsprechende Menü. Zeigen Sie nur mit der Maus auf ein Icon oder einen Eintrag so wird eine kleine Hilfe als Tooltip ausgegeben.

Mit dem Klick auf ***Schraubendreher und Schraubenschlüssel*** ( ) haben Sie Zugriff auf die Einstellungen des AdminTools.

Das Icon rechts daneben ( ) ermöglicht das Ändern des Passworts für das Tool.

Mit dem nächsten Icon ( ) starten Sie den Assistenten zur Zuordnung eines neuen Zertifikats zu den Vorgängen.

Das Ausschalt-Icon ( ) beendet das AdminTool und der Benutzer kehrt zum Hauptprogramm zurück.

Das letzte Icon ( ) zeigt Informationen zum gerade verwendeten Zertifikat an.

### 4.2.1 Das Menü „Aktionen“

Im Aktionsmenü können folgende Aktionen ausgeführt werden:

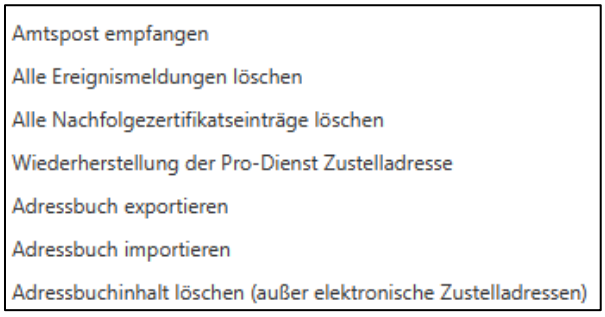



**Abbildung 17: Das Menü "Aktionen"**

**Hinweis:**

Die Aktionen der Zeilen 2, 3 und 4 sollten Sie nur verwenden, wenn es tatsächlich im Programm nicht behebbare Probleme mit den dort aufgeführten Punkten gibt. Sie sollten keinesfalls vorbeugend durchgeführt oder testweise ausprobiert werden!

***Amtspost empfangen:*** Hier können die Dokumente des elektronischen Dokumentenempfangs (Amtsdokumente) abgerufen werden. Dabei wird auch die Sperre, dass nur einmal am Tag abgeholt werden kann, umgangen.

***Alle Ereignismeldungen löschen:*** Löscht **alle** Ereignismeldungen, die im Hauptprogramm im Informationsfenster unter dem Tabulator Ereignisse angezeigt werden. Vor dem Löschen sollten Sie sich im Hauptprogramm überzeugen, dass diese Meldungen tatsächlich nicht durch normale Aktionen im Programm abgearbeitet werden können.

***Alle Nachfolgezertifikatseinträge löschen:*** Wenn im AdminTool eine Änderung der Zertifikatszuordnung zu den Vorgängen vorgenommen wird (siehe auch 4.1.3 Taskmenüpunkt „aktuelle Zertifikatszuordnung ändern“) so wird in der Datenbank der Nachfolger des gewechselten Zertifikats eingetragen. Beim Start bekommen alle Nutzer des alten Zertifikats eine entsprechende Meldung. In seltenen Fällen erscheint diese Meldung trotz Wechsel auf das neue Zertifikat immer wieder. In diesem Fall kann der Nachfolgeeintrag hier gelöscht werden.

***Wiederherstellung der Pro-Dienst Zustelladresse:*** Sollte die bei der Registrierung zum Pro-Dienst (elektronische Dokumentenzustellung des DPMA) angegebene Adresse beschädigt sein, kann hier versucht werden, diese wiederherzustellen.

***Adressbuch exportieren bzw. importieren:*** Hier kann das DPMAdirektPro-Adressbuch komplett für Sicherungszwecke exportiert bzw. importiert bzw. auf andere Datenbanken übertragen werden. Der Export ist nur im Programm DPMAdirektPro verwendbar. Adressen aus Outlook oder dem Online Filing des Europäischen Patentamtes lassen sich im Hauptprogramm in der Adressbuchverwaltung als csv-Dateien importieren.

***Adressbuchinhalt löschen:*** Hier können Sie den kompletten Inhalt des Adressbuches mit einem Klick löschen. Eine für den Pro-Dienst registrierte Zustelladresse wird dabei nicht gelöscht.

### 4.2.2 Das Menü „Vorgangsverwaltung“

Die folgende Abbildung zeigt das Menü der Vorgangsverwaltung.

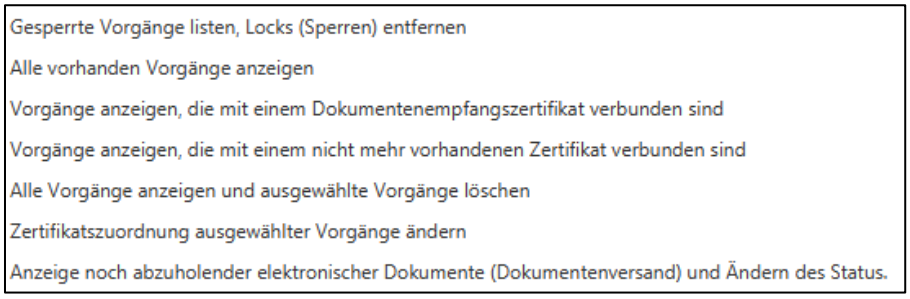



**Abbildung 18: Das Menü "Vorgangsverwaltung"**

Wählen Sie hier eine Aktion aus. Die Ergebnisse werden in einer Tabelle dargestellt. Über das Kontextmenü einer Ergebniszeile sind weitere Aktionen aufrufbar. Die üblichen Spaltensortierungen sind möglich.

***Gesperrte Vorgänge listen, Locks (Sperren) entfernen:*** Beim Bearbeiten eines Vorgangs durch einen Nutzer wird der Vorgang für die anderen Benutzer durch ein Lock in der Datenbank gesperrt. Beim Beenden des Bearbeitens wird das Lock normalerweise wieder entfernt. Bricht vorher die Verbindung zu Datenbank ab oder wird das Hauptprogramm nicht ordnungsgemäß beendet, kann das Lock nicht mehr entfernt werden und die Nutzer erhalten immer eine Sperrmeldung. Diese Sperre kann hier entfernt werden.

***Alle vorhandenen Vorgänge anzeigen:*** Es werden alle in der Datenbank vorhanden Vorgänge angezeigt. Zertifikatszuordnung und Betriebsmodus werden ignoriert. Diese Abfrage dient rein informativen Zwecken, Aktionen sind nicht möglich.

***Vorgänge anzeigen, die mit einem Dokumentenempfangs-Zertifikat verbunden sind:*** Es werden alle Vorgänge angezeigt, die mit einem Zertifikat verbunden sind, das für den elektronischen Dokumentenempfang (Pro-Dienst) registriert wurde. Auch dies ist nur eine informative Anzeige.

***Vorgänge anzeigen, die mit einem nicht mehr vorhandenen Zertifikat verbunden sind:*** Es werden die Vorgänge angezeigt, die mit einem Zertifikat verbunden sind, das nicht (mehr) in der Datenbank vorhanden ist. Dies kann vor allem nach der Übernahme der Datenbank aus der alten Version DPMAdirekt 3.x möglich sein. Sie können die Vorgänge löschen oder sie einem anderen Zertifikat zuordnen.

***Alle Vorgänge anzeigen und ausgewählte Vorgänge löschen:*** Anzeige aller Nutzervorgänge die durch den Benutzer löschbar sind. Vorgänge, die mit einem Zertifikat, das für den Pro-Dienst registriert ist, verknüpft sind, werden als nicht löschbar eingestuft und werden daher nicht angezeigt. Das Löschen hier sollte nur eine Ausnahme sein, wenn es in der Oberfläche des Hauptprogramms nicht mehr gehen sollte. Daher gibt es auch keine Möglichkeit einer Mehrfachmarkierung von Vorgängen.

***Zertifikatszuordnung ausgewählter Vorgänge ändern:*** Anzeige aller Vorgänge deren Zertifikatszuordnung durch den Nutzer änderbar ist.

**Vorsicht:** Wenn Sie bei Systemvorgängen, die mit einem Zertifikat verknüpft sind, das für den Pro-Dienst registriert ist, die Zuordnung hier ändern wird die Registrierung für dieses Zertifikat nicht mehr aktiv sein!!

***Anzeige noch abzuholender elektronischer Dokumente (Dokumentenversand) und Ändern des Status:*** Hier können Sie sich die elektronischen Dokumente anzeigen lassen, die in der Datenbank noch als vom Server abzuholen markiert sind. Durch einen Rechtsklick können Sie den Abholstatus auf abgeholt (true) setzen. Es wird dann nicht mehr versucht, dieses Dokument vom DPMA-Server abzuholen.

### 4.2.3 Das Menü „Zertifikatsverwaltung“

Die verwendeten Zertifikate werden in DPMAdirektPro nicht mehr im Dateisystem, sondern in der Datenbank gespeichert.

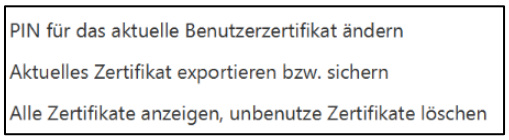



**Abbildung 19: Das Menü: „Zertifikatsverwaltung“**

***PIN für das aktuelle Benutzerzertifikat ändern:*** Da das Ändern der PIN für das aktuelle Benutzerzertifikat Auswirkung auf alle Nutzer hat, wurde die Möglichkeit zum Ändern in den AdminTool-Bereich verlagert. Die Kenntnis der alten PIN für das Zertifikat ist erforderlich.

***Aktuelle Zertifikat exportieren bzw. sichern:*** Für Sicherungszwecke kann an dieser Stelle das aktuelle Benutzerzertifikat exportiert werden.

**Hinweis:**

Dieser Punkt wurde in den AdminTool-Bereich verlagert, weil das Zertifikat den Schlüssel zum elektronischen Postfach beim DPMA darstellt und jeder, der das Zertifikat hat, über DPMAdirektPro die Dokumente aus diesem Postfach abrufen kann. Daher bewahren Sie das gesicherte Zertifikat zugriffsgeschützt auf! Leider lässt sich aktuell der Status „registriert“ für ein Zertifikat nicht wieder herstellen!

***Alle Zertifikate anzeigen, unbenutzte Zertifikate löschen:*** Zertifikate, die keinem Vorgang mehr zugeordnet sind, können hier gelöscht werden.

### 4.2.4 Das Menü „DB-Diagnostik“

In diesem Menü können einige Maßnahmen zur Datenbankdiagnose vorgenommen werden.

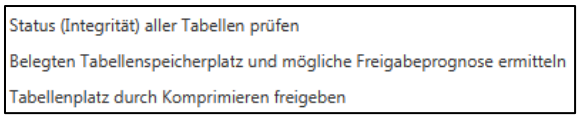



**Abbildung 20: Das Menü "DB-Diagnostik"**

***Status (Integrität) aller Tabellen prüfen:*** Prüft die Integrität der Tabellen in der Datenbank und erstellt einen Prüfbericht.

***Belegten Tabellenspeicherplatz und mögliche Freigabeprognose ermitteln:*** Wenn Daten aus der Tabelle im Hauptprogramm gelöscht werden, so wird zwar der Patz in der Datenbank freigegeben, der durch die Datenbank belegte Speicherplatz auf der Festplatte wird aber nicht reduziert. Hier kann der belegte Speicherplatz und eine Freigabeprognose angezeigt werden.

***Tabellenplatz durch Komprimieren freigeben:*** Es wird der Speicherplatz in der Datenbank komprimiert und auf der Festplatte freigegeben. Das Ergebnis wird angezeigt.

# 5 Rechte- und Benutzerverwaltung im AdminTool

Ab der Version DPMAdirektPro 3 wurde in das Programm ein Rechte- und Benutzerverwaltungssystem integriert, welche im AdminTool aktiviert und konfiguriert werden kann.

## 5.1 Grundlagen der Rechte- und Benutzerverwaltung

Im folgenden Abschnitt werden die Grundlagen der Rechte- und Benutzerverwaltung beschrieben.

### 5.1.1 Aktivierung/Deaktivierung des Rechte- und Benutzerverwaltungssystems

Im AdminTool kann unter ***Lokale Einstellungen*** im Tab ***Rechte- und Benutzerverwaltung*** die Rechtesteuerung für die Benutzer aktiviert werden.
Nach der Aktivierung können sich in DPMAdirektPro nur noch Benutzer anmelden, denen in der Rechteverwaltung ein Zugriff gestattet wurde. Nutzer, die in der Rechteverwaltung nicht aufgeführt sind, haben dann keinen Zugriff mehr auf das Programm.

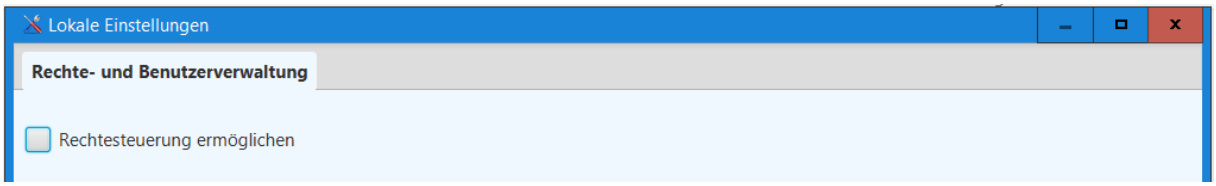



**Abbildung 21: Rechteverwaltungssystem aktivieren**

Als erstes wird nach dem Aktivieren der Administrator aufgefordert ein initiales Passwort für alle Benutzer, die später angelegt werden, zu vergeben.
Der neu angelegte Benutzer wird dann beim ersten Login aufgefordert, das initiale Passwort durch sein individuelles Passwort zu ersetzen.

Die Anforderungen an die Passwortvergabe sind wie folgt definiert:

- Das Passwort muss mindestens 6 Zeichen lang sein
- Das Passwort muss mindestens einen großen und einen kleinen Buchstaben enthalten
- Das Passwort muss mindestens eine Zahl enthalten

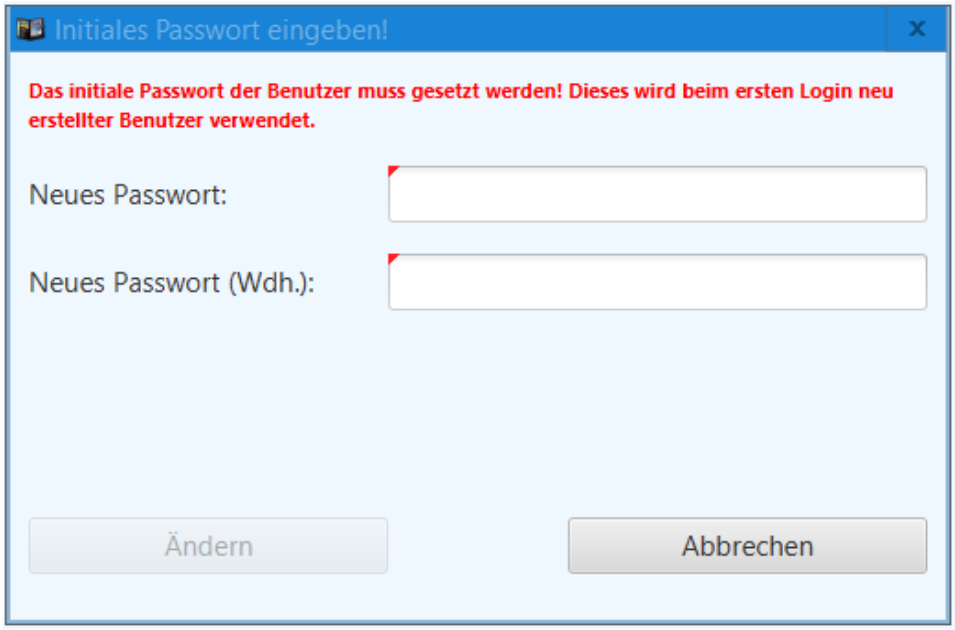



**Abbildung 22: Initiales Passwort für alle Benutzer vergeben**

Der Benutzer „admin“ existiert standardmäßig im Rechteverwaltungssystem. Die Person, die die Einrichtung der Rechte- und Benutzerverwaltung vornimmt, wird automatisch mit dem Admin-Account angemeldet. Dafür muss zuerst das im vorherigen Schritt vergebene initiale Passwort durch das individuelle Passwort für den Benutzer „admin“ ersetzt werden:

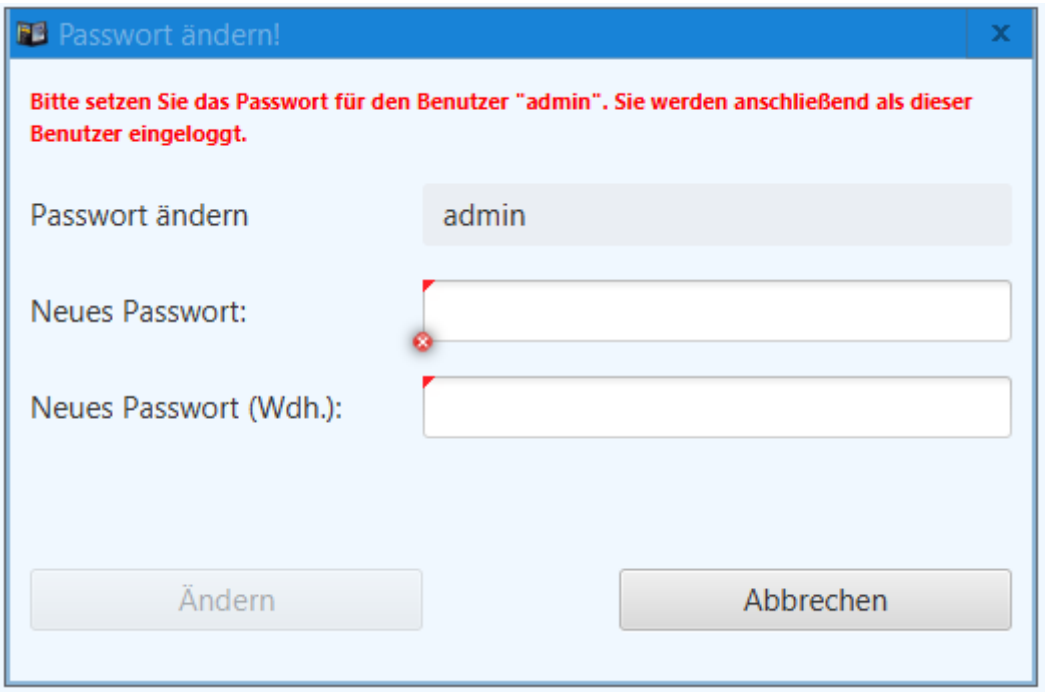



**Abbildung 23: individuelles Passwort für den Benutzer Admin setzen**

Nach der Freischaltung der Rechteverwaltung und Anmeldung des Benutzers „Admin“, erscheint eine Tab-Ansicht mit zwei Tabs ***Benutzerverwaltung*** und ***Rechtevergabe***.

Wird die Rechte- und Benutzerverwaltung wieder deaktiviert (siehe Abbildung 21), so gibt es wie vor der Aktivierung keine Einschränkungen mehr, alle Benutzer haben wieder identische Rechte und dürfen alles machen und es kann sich jede Person, die die PIN des Zertifikats kennt am Programm anmelden.

### 5.1.2 Benutzerverwaltung

Im Tab ***Benutzerverwaltung*** können Benutzer angelegt, verwaltet und dargestellt werden. Beim Hinzufügen oder Editieren eines neuen Benutzers müssen

- Benutzername (Bei neu hinzugefügtem Benutzer)
- Name
- Vorname
- Rollen (können direkt dem Benutzer zugewiesen werden)

angegeben werden.

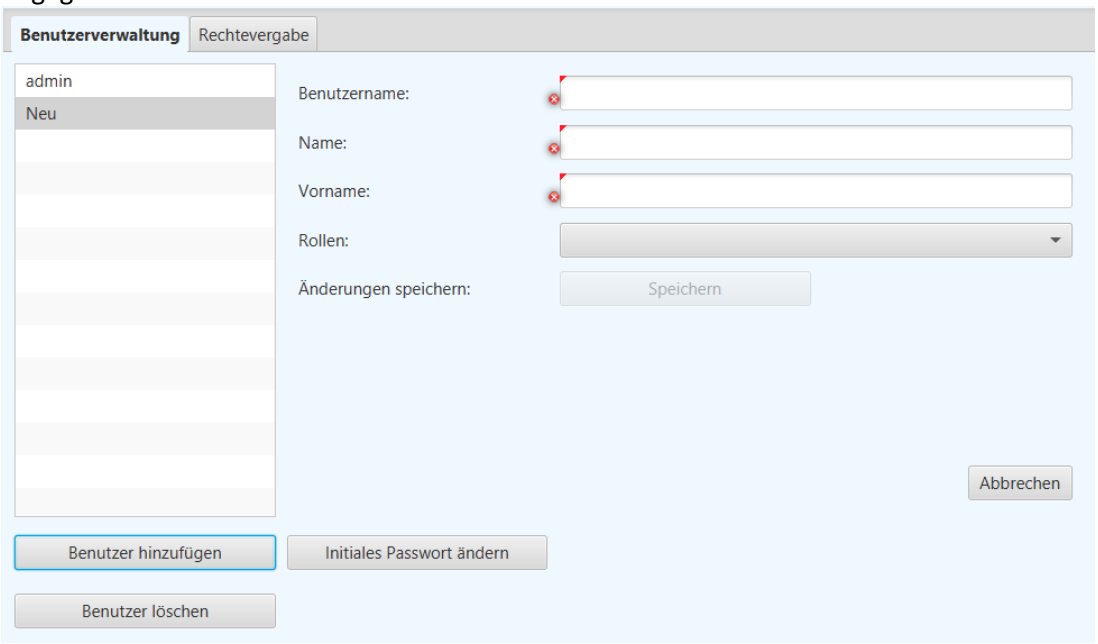



**Abbildung 24: Neuen Benutzer anlegen**

Einem Benutzer können mehrere Rollen mit entsprechenden Rechten zugewiesen werden. Nach dem Speichern steht die Funktionalität ***Passwort zurücksetzen*** zusätzlich zur Verfügung. Das Passwort kann nur auf das initiale Passwort, wie vom Administrator vergeben, zurückgesetzt werden.

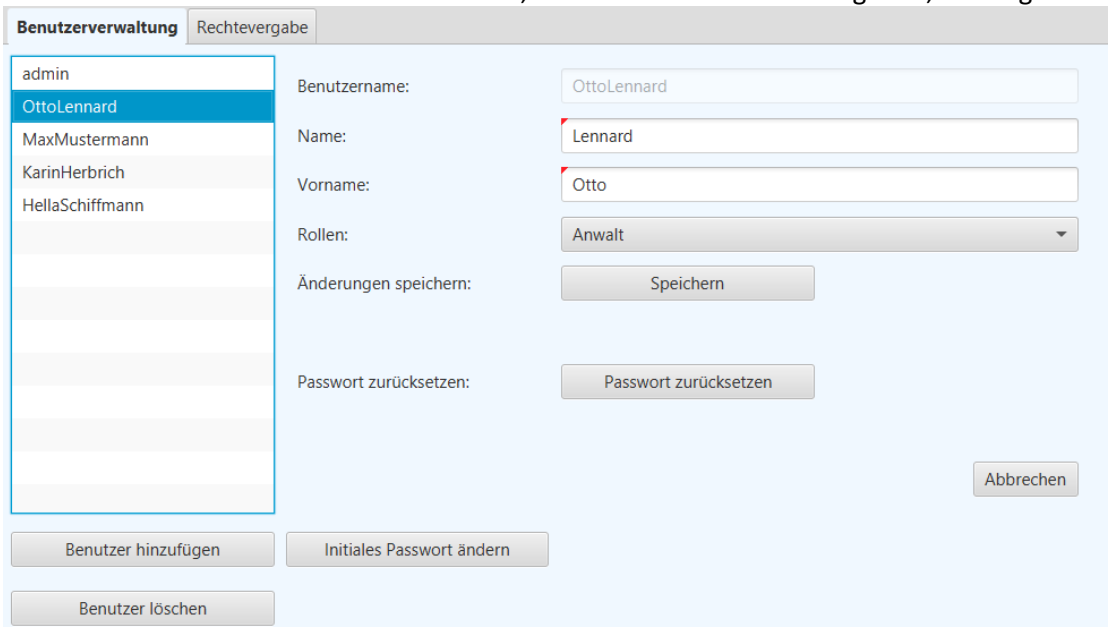



**Abbildung 25: Benutzer anlegen und Rolle(n) vergeben**

***Benutzer löschen:*** Hier können einzelne Benutzer entfernt werden. Ausnahme besteht nur für den Benutzer „admin“: Dieser ist geschützt, kann nicht gelöscht und seine Rolle nicht verändert werden.

***Initiales Passwort ändern:*** Mit dieser Funktion kann das initiale Passwort geändert werden:

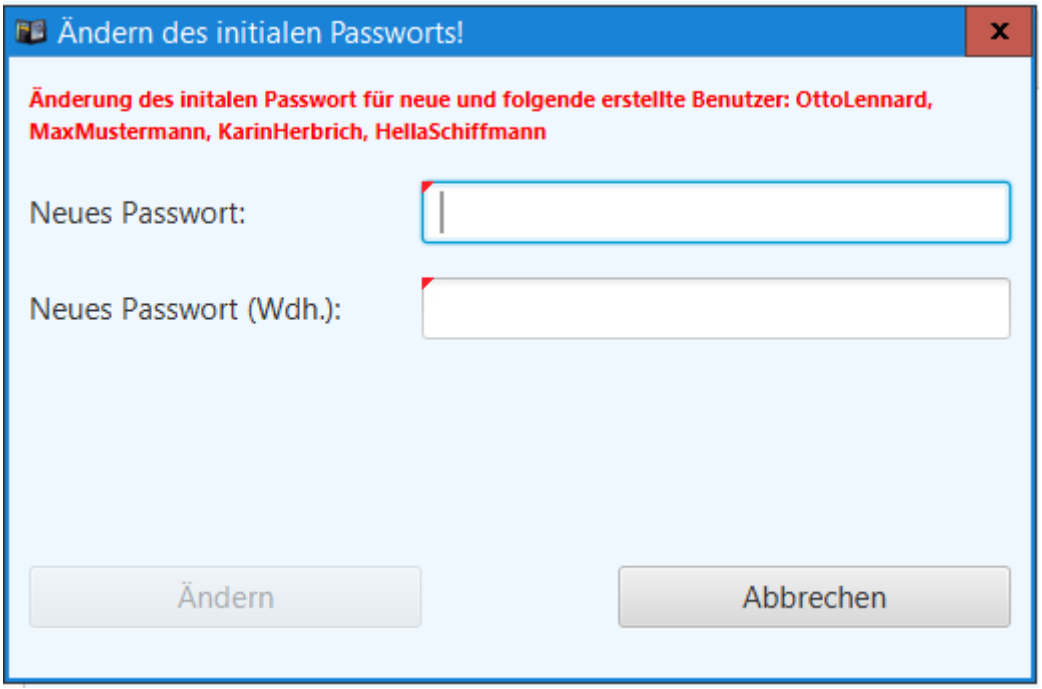



**Abbildung 26: Initiales Passwort für alle Benutzer ändern**

### 5.1.3 Rechtvergabe

Einzelne Rollen mit den entsprechenden Rechten sind im Rechteverwaltungssystem in DPMAdirekt-Pro vordefiniert. Es besteht aber die Möglichkeit, die Rechte für einzelne Rollen anzupassen.

Zunächst wird in der ComboBox (1) die zu ändernde Benutzerrolle ausgewählt. Im darunterliegendem Fenster werden die einzelne Rechte als Checkboxes angezeigt und können aus- bzw. abgewählt werden (2).

In der Liste rechts werden die Benutzer angezeigt, die aktuell mit der ausgewählten Rolle verknüpft sind.
Über die ComboBox (3) in Verbindung mit einem Button „+“ können weitere Benutzer der ausgewählten Rolle hinzugefügt werden.
***Rolle speichern*** (4) speichert die gemachten Änderungen.

***Zurücksetzen*** (5) setzt alle manuell gemachten Änderungen aller Rollen auf die Standardeinstellungen zurück.

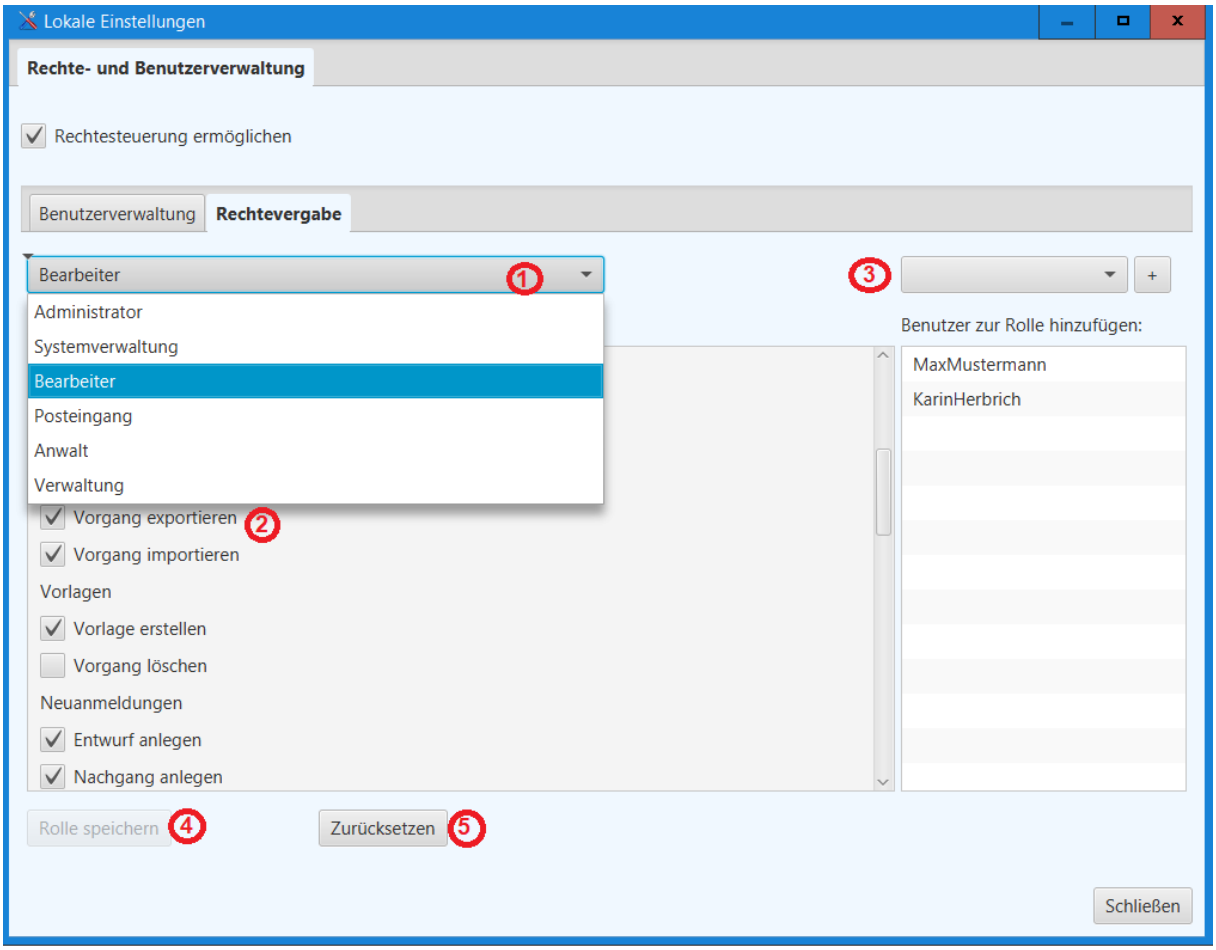



**Abbildung 27: Rechtvergabe**

***Schließen*** beendet die Rechteverwaltung. Vor dem Schließen wird überprüft, ob mindestens ein Benutzer erstellt worden ist und ob mindestens ein Benutzer Zugriff auf die Rechteverwaltung im Admin-Tool hat.
Sollte dies nicht der Fall sein, wird die Rechteverwaltung deaktiviert.

Der Benutzername und das initiale Passwort muss allen eingetragenen Benutzern von DPMAdirekt-Pro für das Login in das Programm mitgeteilt werden.

### 5.1.4 Programm-Login bei aktivierter Rechteverwaltung

Das Fenster zum Login kann zu zwei Zeitpunkten erscheinen.
Zum einem, wenn vor dem Start des Programms die Rechtverwaltung schon aktiviert ist, zum anderem, wenn während der Arbeit im Programm eine Aktivierung stattfindet.

Im folgenden Fenster gibt der Anwender seine Anmeldedaten ein. Diese werden bei Betätigen des „Anmelden“-Buttons überprüft.

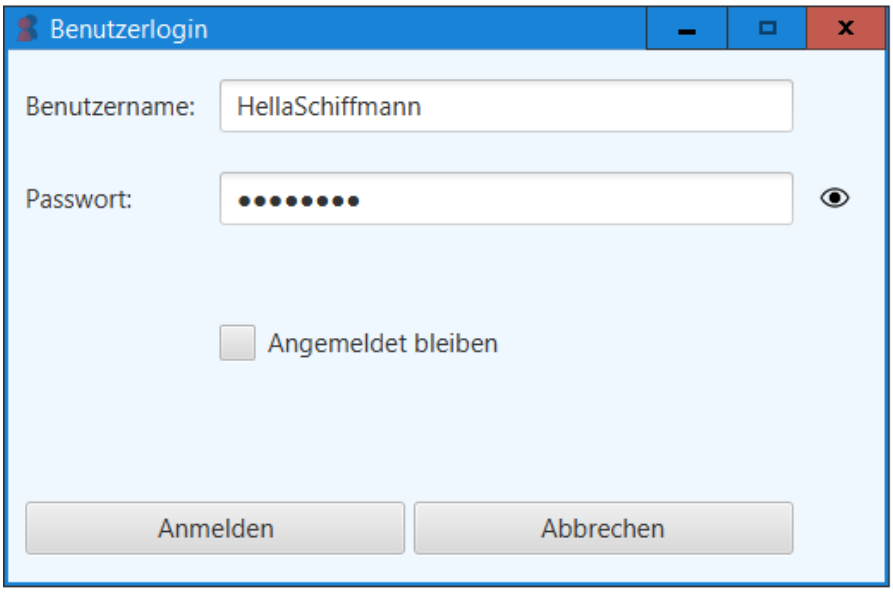



**Abbildung 28: Login in DPMAdirektPro**

Wurde für den Benutzer nur ein initiales Passwort vergeben, erscheint die Ansicht zur Passwortänderung. Nach der Änderung muss das Passwort im Login-Fenster noch mal eingegeben werden.

***Angemeldet bleiben***: Bei aktivierter CheckBox wird das Passwort verschlüsselt in den Benutzereinstellungen auf dem Rechner gespeichert und muss somit beim Programmstart nicht erneut eingegeben werden.

## 5.2 Die Passwort Verwaltung

### 5.2.1 Passwort ändern

Der Dialog zum Passwort ändern erscheint
- beim Login in das Programm, nachdem nur das initiale Passwort vergeben wurde
- wenn der Benutzer sein Passwort ändern will
- bei erstmaliger Aktivierung der Rechtverwaltung im Admin-Tool.

Es muss das Passwort angegeben werden. Um Rechtschreibfehler zu vermeiden muss das neue Passwort doppelt eingegeben werden.

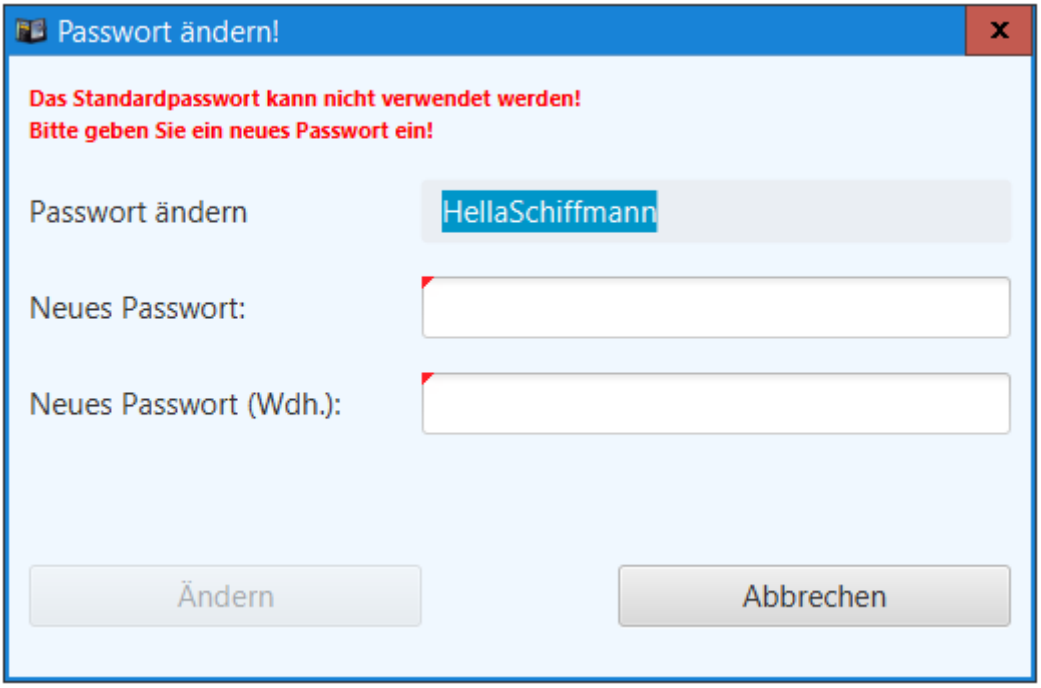



**Abbildung 29: Individuelles Passwort setzen**

### 5.2.2 Passwortsicherheit

Alle Passwörter werden verschlüsselt in der Datenbank bzw. in der Benutzerkonfiguration des Programms gespeichert.

Anforderungen an die Passwortvergabe sind wie folgt definiert:
- Das Passwort muss mindestens 6 Zeichen lang sein
- Das Passwort muss mindestens einen großen und einen kleinen Buchstaben enthalten
- Das Passwort muss mindestens eine Zahl enthalten

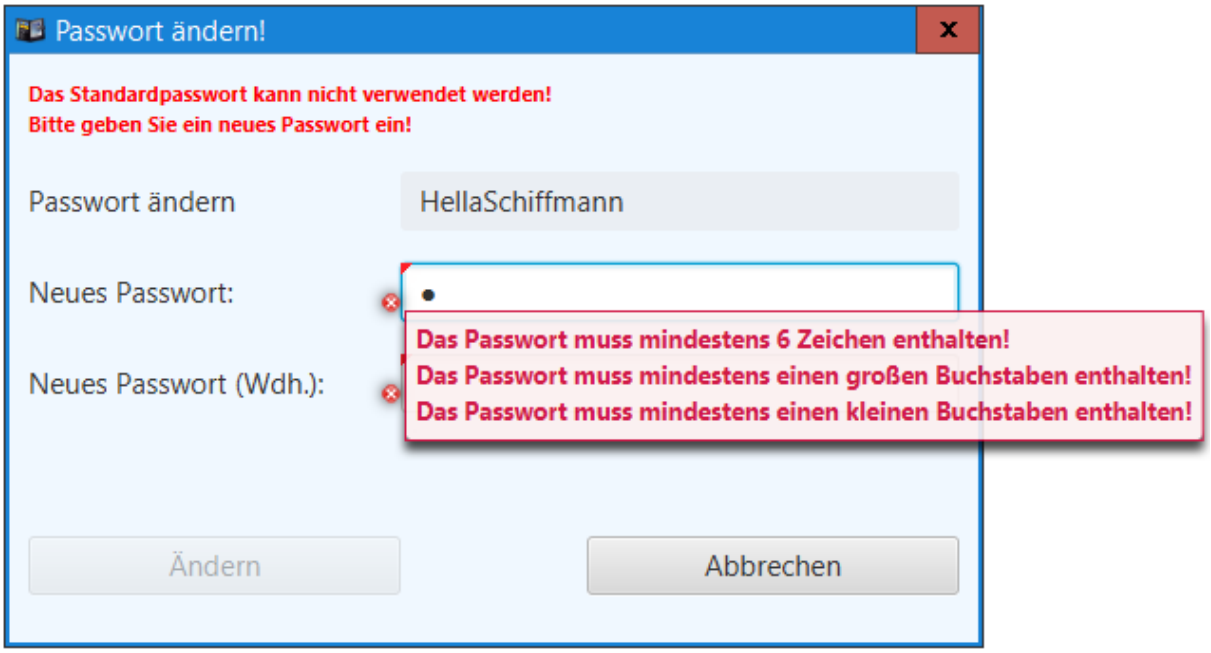



**Abbildung 30: Anforderungen an die Passwortvergabe**

### 5.2.3 Das initiales Passwort

Das initiale Passwort dient als allgemeines Passwort, dass vom Administrator vergeben wird und zum erstmaligen Login eines neuen Benutzers oder beim Zurücksetzen genutzt wird.

### 5.2.4 Das Master Passwort

Falls der Benutzer „Admin“ sein Passwort vergessen haben sollte, besteht über das Master-Passwort die Möglichkeit, sein Passwort zurückzusetzen und ein neues zu vergeben. Dieses Passwort ist nicht frei verfügbar und kann nur über die DPMAdirekt-Support per E-Mail an dpmadirekt@dpma.de erfragt werden.

### 5.2.5 Benutzer wechseln oder Passwort ändern

Unter welchen Namen der Benutzer aktuell im Programm angemeldet ist, wird in der Programmoberfläche rechts oben angezeigt.




**Abbildung 31: Menüleiste mit dem angemeldeten Benutzer**

Beim Klick auf die Menüleiste mit dem Benutzernamen wird das Fenster zum Benutzerwechsel und/oder zum Ändern des Passworts aufgerufen.

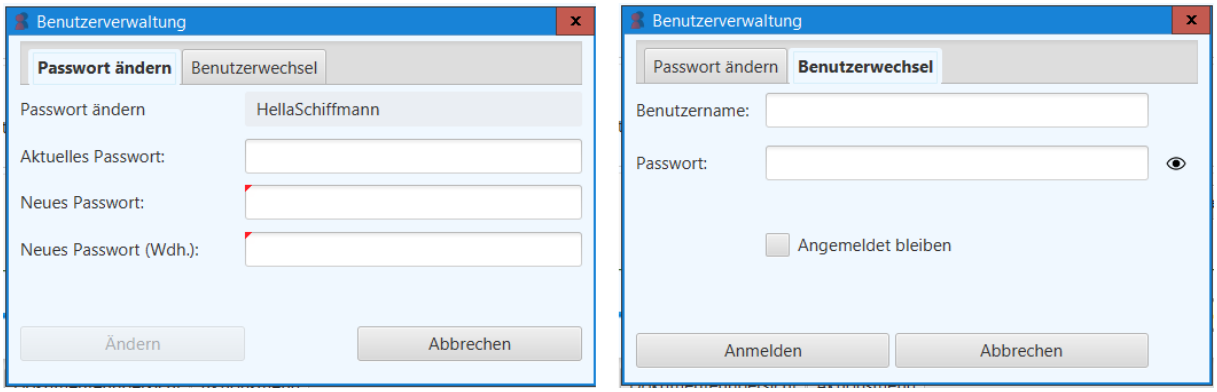



**Abbildung 12: Benutzerwechsel/ Passwort ändern**

## 5.3 Vorgänge und Aktionen

Entsprechend der vergebenen Rechten für die jeweilige Rolle des angemeldeten Benutzers, werden einzelne Aktionen und/oder Einstellungen für ihn ausgeblendet und stehen somit nicht zur Verfügung.

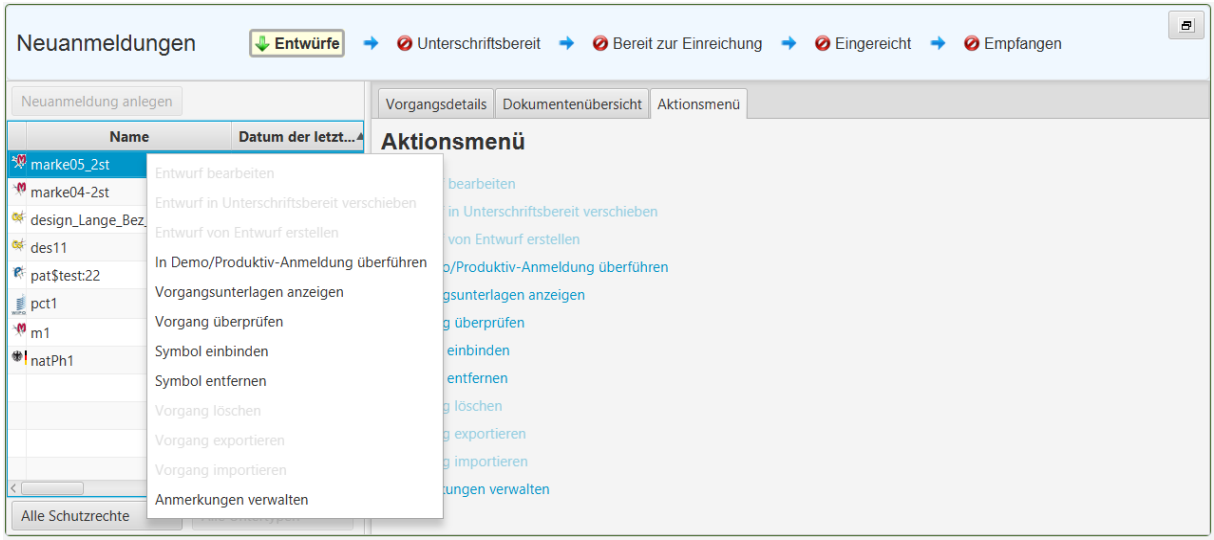



**Abbildung 32: Ausgesperrte und aktivierte Aktionen eines Vorgangs für die Benutzerrolle „Posteingang“**

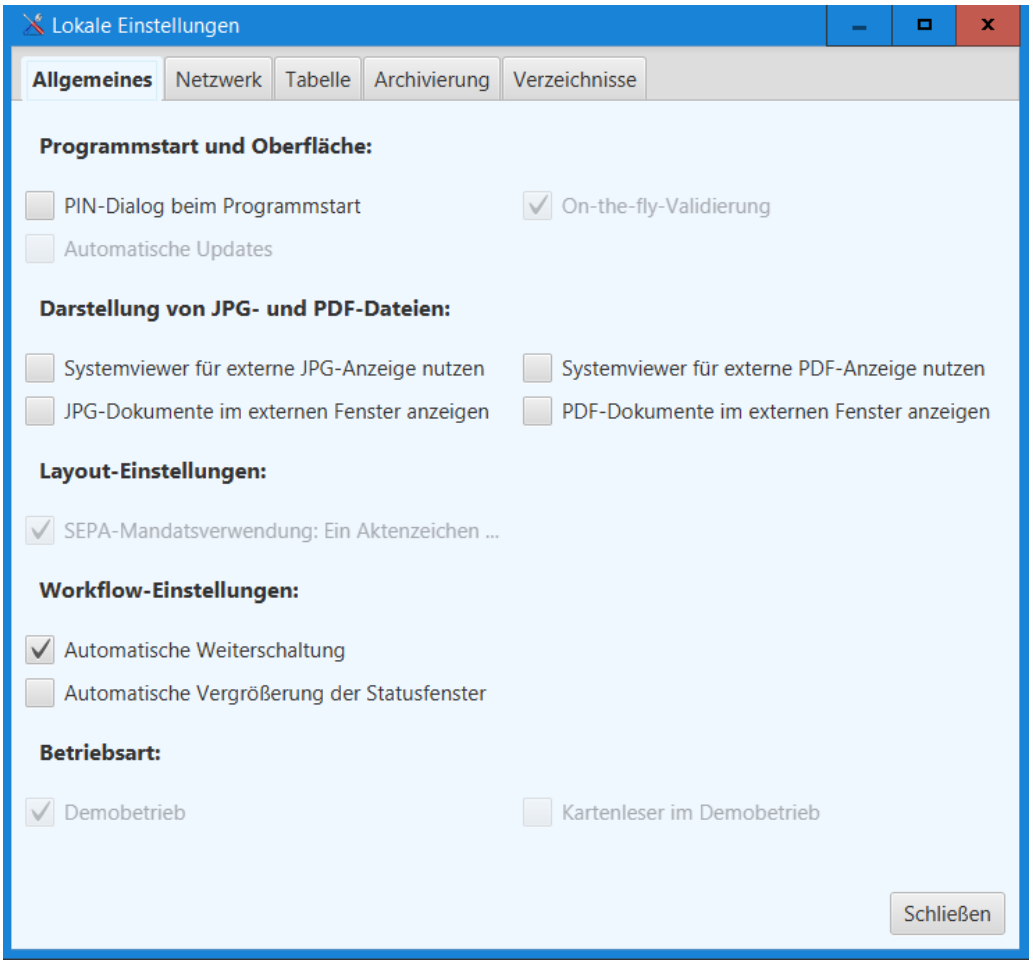



**Abbildung 33: Ausgeblendete Einstellungen für die Benutzerrolle „Posteingang“**

## 5.4 Voreingestellte Rechte der Standard-Benutzerrollen

| | Administra-tor | System-verwal-tung | Anwalt | Verwaltung | Bearbeitung | Posteingang |
|---|---|---|---|---|---|---|
| **Admin-Tool** | | | | | | |
| Rechteverwaltung | | | | | | |
| Zertifikat | | | | | | |
| Datenbank | | | | | | |
| **Einstellungen/ Menüleiste** | | | | | | |
| Automatische Updates ja/nein | | | | | | |
| Demo | | | | | | |
| Proxy | | | | | | |
| Archivierung | | | | | | |
| Filesystem | | | | | | |
| Zertifikat | | | | | | |
| Pro | | | | | | |
| On-the-fly-Validierung | | | | | | |
| SEPA-Mandatsverwendung | | | | | | |

| | | | | | | |
|---|---|---|---|---|---|---|
| **Import/Export** | | | | | | |
| Export | | | | | | |
| Import | | | | | | |
| **Volagen** | | | | | | |
| Vorlage erstellen | | | | | | |
| Vorgang löschen | | | | | | |
| **Neuanmeldung/ Nachgang** | | | | | | |
| Entwurf anlegen | | | | | | |
| Nachgang anlegen | | | | | | |
| Entwurf bearbeiten | | | | | | |
| Vorgang löschen | | | | | | |
| Verschieben in Unterschriftsbereit | | | | | | |
| **Unterschriftsbereit** | | | | | | |
| Verschieben zu Entwurf | | | | | | |
| Vorgang löschen | | | | | | |
| Autorisierung | | | | | | |
| **Postausgang** | | | | | | |
| Vorgang versenden | | | | | | |
| Alle versenden | | | | | | |
| Verschieben in Entwürfe | | | | | | |
| Manuelles verschieben in Erledigt | | | | | | |
| Empfangen | | | | | | |
| DRN anzeigen | | | | | | |
| Vorgang löschen | | | | | | |
| **Posteingang** | | | | | | |
| Erledigt verschieben | | | | | | |
| DRN anzeigen | | | | | | |
| Aktenzeichen anzeigen | | | | | | |
| **Erledigt** | | | | | | |
| Vorgang archivieren | | | | | | |
| Vorgang löschen | | | | | | |
| Aktenansicht | | | | | | |
| **Fehlerhaft** | | | | | | |
| Vorgang archivieren | | | | | | |
| Fehler anzeigen | | | | | | |
| DRN anzeigen | | | | | | |
| Vorgang löschen | | | | | | |
| **Druckbereit** | | | | | | |
| DRN anzeigen | | | | | | |
| Vorgang löschen | | | | | | |

**Abbildung 34: Vordefinierte Benutzerrollen und deren Rechte**

(grün: erlaubt, rot: verboten)

# 6 Nutzung der Zertifikate

Zur Nutzung von DPMAdirektPro sind zwei verschieden Zertifikate notwendig, ein Verschlüsselungszertifikat (= Softwarezertifikat) und ein Signaturzertifikat (= Signaturkarte).

## 6.1 Meldung: Gültigkeit des Zertifikats ist abgelaufen

Möglicherweise erhalten Sie beim Programmstart eine Meldung, dass die Gültigkeit des verwendeten Zertifikats abgelaufen ist. Diese Meldung wird auch bei den Ereignissen eingetragen.
Mit einem abgelaufenen Zertifikat werden künftig keine Anmeldungen mehr möglich sein. Sie sollten es daher schnellstmöglich tauschen. Eine Anmeldung zum elektronischen Dokumentenversand ist mit einem abgelaufenen Zertifikat ebenfalls nicht möglich.
Wenn das Zertifikat **nicht** für den Pro-Dienst (elektronischer Dokumentenempfang des DPMA) registriert ist, erneuern Sie das Zertifikat hier im AdminTool. Verfahren Sie dabei bitte wie im Abschnitt 4.1.3 Taskmenüpunkt „aktuelle Zertifikatszuordnung ändern“ beschrieben.

## 6.2 Das Verschlüsselungszertifikat

Das selbsterstelle Verschlüsselungszertifikat erscheint bei jedem Programmstart und fordert Sie zur Eingabe Ihrer dafür vergebenen PIN auf.
Das Zertifikat hat fünf Funktionen:

- autorisierte Anmeldung am Programm DPMAdirektPro
- Einrichtung eines virtuellen elektronischen Postfachs beim DPMA
- Zugriffssteuerung auf die Vorgänge in DPMAdirektPro (Multi-User-Version)
- Verschlüsselung des Nachrichtenweges vom DPMA zum Anwender
- Nutzung als Signaturzertifikat im Demomodus

Das Verschlüsselungszertifikat erstellen Sie beim Erststart von DPMAdirektPro oder später durch Auswahl des entsprechenden Menüpunktes im Programm. Die dort einzutragenden Angaben - einschließlich der PIN - legen Sie selbst fest.

### 6.2.1 Zugriffssteuerung auf die Vorgänge anhand eines Beispiels

Über das Verschlüsselungszertifikat können Sie festlegen, welche Benutzer auf welche Vorgänge zugreifen können. Alle, die das gleiche Zertifikat verwenden, können auf die gleichen Vorgänge in DPMAdirektPro zugreifen.

**Ein Beispiel:**

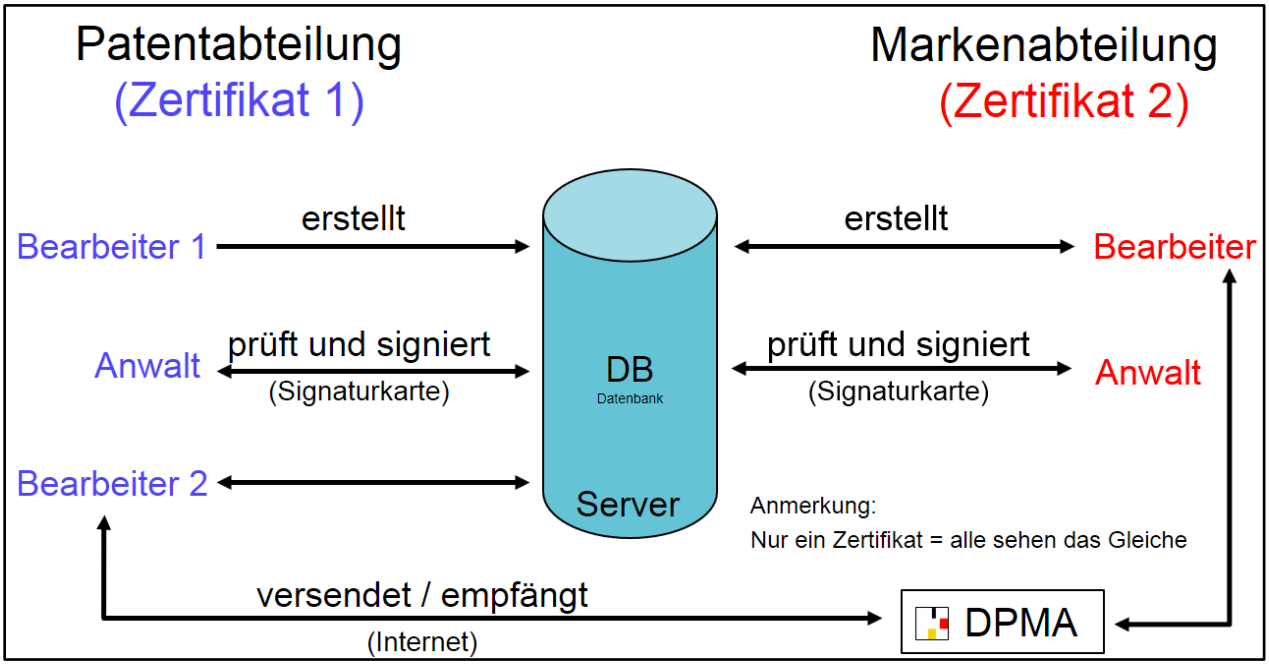



**Abbildung 35: Anwendungsszenario mit 2 getrennten Abteilungen**

In einer Kanzlei gibt es einen Patent- und einen Markenbereich (siehe Abbildung). In jedem Bereich sollen der jeweilige Anwalt (bzw. die unterschriftsberechtigte Person) und die Sachbearbeiter auf die eigenen Vorgänge zugreifen können. Ein bereichsübergreifender Zugriff wird nicht gewünscht. Es wurde die Multi-User-Version von DPMAdirektPro installiert.
Dazu wird ein Zertifikat für den Patentbereich und eins für den Markenbereich erzeugt. Das Patentzertifikat wird auf die Rechner des jeweiligen Anwalts (bzw. der unterschriftsberechtigten Person) und der beiden Sachbearbeiter des Bereichs kopiert und als zu nutzendes Zertifikat in DPMAdirektPro ausgewählt. Nun ist es möglich, dass der Patentbereich einen Vorgang arbeitsteilig bearbeitet. Der Markenbereich sieht diese Vorgänge nicht.

### 6.2.2 Sicherung (Backup) des Verschlüsselungszertifikats

Da Ihr Verschlüsselungszertifikat vielfältige Aufgaben hat, empfiehlt es sich, eine Kopie des Zertifikats gleich nach der Erstellung anzufertigen und diese sicher zu verwahren.

## 6.3 Das Signaturzertifikat (die Signaturkarte)

Das Signaturzertifikat ist auf Ihrer Signaturkarte enthalten und wird zum Signieren (Unterschreiben) der Nachricht an das DPMA benutzt.

Vor dem Versenden muss der Anwalt (bzw. die unterschriftsberechtigte Person) die einzureichenden Unterlagen autorisieren. Dazu werden in einem Fenster alle Unterlagen angezeigt. Anschließend werden diese Unterlagen signiert. Dazu muss die Signaturkarte in das Lesegerät eingeführt und die Signatur-PIN eingegeben werden.
Bei einigen Signaturkarten werden in der Zertifikatsauswahl zwei Zertifikate angezeigt. Zum Signieren wird das ***Signaturzertifikat*** benötigt.
Merke: Signaturkarte = persönliche Unterschrift

# 7 Fehlersuche und –behebung

Standardmäßig schreibt DPMAdirektPro ein Aktivitätenlog. Dieses finden Sie im Installationsverzeichnis von DPMAdirektPro (Standard: c:\Programme [(x86)]\DPMAdirektPro\client oder desktop) und dort im Verzeichnis ***log***.
Das aktuelle Programmlog heißt DPMAdirekt.log. Archivierte Logs haben als Endung das jeweilige Tagesdatum.
Die Logs DPMAdirekt_Communication.log enthalten die Logausgaben für die Kommunikation mit dem DPMA (Versenden/ Empfangen).

## 7.1 Bekannte Probleme

Bekannte Probleme und deren Behebung zeigt die folgende Tabelle:

| | |
|---|---|
| Signaturkarte wird nicht erkannt | Wenn weitere Kartensoftware installiert ist (z.B. epoline vom EPA oder Herstellersoftware) behindert diese möglicherweise den Zugriff von DPMAdirektPro auf die Karte. Deaktivieren Sie diese Software oder stecken Sie die Karte ein paar Mal in den Leser raus und rein. |
| PDFs werden mangelhaft dargestellt | Manchmal werden (vor allem eingescannte) PDFs nur in DPMAdirektPro schlecht dargestellt. Die verwendete Javakomponente zur PDF-Anzeige hat manchmal Probleme bei der korrekten Darstellung. In diesem Fall wählen Sie ***Im Systemviewer für externe PDF-Anzeige nutzen*** bei den Programmeinstellungen (siehe Anwenderbeschreibung des Hauptprogramms) Ihre Dokumente werden in DPMAdirektPro nicht verändert! |

| | |
|---|---|
| JPGs werden mangelhaft dargestellt | Manchmal werden Grafiken im JPG-Format nur in DPMAdirektPro schlecht dargestellt. Die verwendete Javakomponente hat manchmal Probleme bei der korrekten Darstellung. In diesem Fall wählen Sie ***Im Systemviewer für externe JPG-Anzeige nutzen*** bei den Programmeinstellungen (siehe Anwenderbeschreibung des Hauptprogramms). Ihre Dokumente werden in DPMAdirektPro nicht verändert! |
| Der Serverdienst startet nach der Installation nicht. | Beenden Sie gegebenenfalls im Taskmanager den Dienst jsl.exe. Kopieren Sie aus dem Verzeichnis serverinstallationspfad\server\ jre\jre1.6\bin\ die Datei ***msvcr71.dll*** in das Verzeichnis serverinstallationspfad\server\ und starten Sie den Dienst DPMAdirektService in der Dienstesteuerung.<br>Bei einer neuen Installation mit dem Verzeichnis ..\jre1.8\ muss die Datei ***msvcr100.dll*** kopiert werden. |

## 7.2 Fehlersuche im Debugmodus

Sollte das Programm nicht wie erwartet reagieren, so können Sie (eventuell in Zusammenarbeit mit dem DPMAdirekt-Support) über das oben beschriebene automatische Log hinausgehende Informationen in einer DOS-Konsole erhalten.
Dazu gehen Sie in das Installationsverzeichnis von DPMAdirektPro und Doppelklicken Sie die Datei ***DPMAdirektProDebug.exe***.
Das sich öffnende DOS-Fenster soll im Hintergrund geöffnet bleiben!

Anschließend arbeiten Sie wie gewohnt in der graphischen Oberfläche von DPMAdirektPro bis das Problem auftritt.
Möglicherweise ist das Problem in der Ausgabe des DOS-Fensters zu erkennen.
Mit Klick in die linke Ecke des DOS-Fensters und ***Bearbeiten\Alles Auswählen*** und ***Bearbeiten\Kopieren*** kann der Inhalt des DOS-Fensters in die Zwischenablage und von dort aus in eine E-Mail kopiert werden.
Wenn Sie Unterstützung benötigen, setzen Sie sich bitte mit dem technischen DPMAdirekt-Support (DPMAdirekt@dpma.de) in Verbindung.

# 8 Abbildungsverzeichnis:

Abbildung 2: Auswahl der Einzelplatzversion ..... 9
Abbildung 3: Auswahl der Serverinstallation ..... 11
Abbildung 4: DPMAdirektService.log ..... 12
Abbildung 5: Den Datenbankport prüfen ..... 12
Abbildung 6: Serveradresse auswählen ..... 12
Abbildung 7: Infodialog zur unbeaufsichtigten Installation ..... 14
Abbildung 8: Auswahl der zu deinstallierenden Komponenten ..... 15
Abbildung 9: Erstkonfiguration – Zertifikatsauswahl ..... 16
Abbildung 10: Erstkonfiguration – Proxy-Konfiguration ..... 17
Abbildung 11: Ein neues Benutzerzertifikat erzeugen ..... 18
Abbildung 12: Dialog zur Verwendung des neuen Zertifikats ..... 19
Abbildung 13: Passworteingabe für das AdminTool ..... 22
Abbildung 14: Die Oberfläche des AdminTools ..... 23
Abbildung 15: Zertifikatsauswahl für das Ändern der Zuordnung ..... 24
Abbildung 16: Gegenüberstellungsdialog zum Zertifikatsersetzen ..... 24
Abbildung 17: Die Schnellstartleiste ..... 25
Abbildung 18: Das Menü "Aktionen" ..... 26
Abbildung 19: Das Menü "Vorgangsverwaltung" ..... 28
Abbildung 20: Das Menü: „Zertifikatsverwaltung“ ..... 29
Abbildung 21: Das Menü "DB-Diagnostik" ..... 30
Abbildung 22: Rechteverwaltungssystem aktivieren ..... 31
Abbildung 23: Initiales Passwort für alle Benutzer vergeben ..... 32
Abbildung 24: individuelles Passwort für den Benutzer Admin setzen ..... 32
Abbildung 25: Neuen Benutzer anlegen ..... 33
Abbildung 26: Benutzer anlegen und Rolle(n) vergeben ..... 33
Abbildung 27: Initiales Passwort für alle Benutzer ändern ..... 34
Abbildung 28: Rechtvergabe ..... 35
Abbildung 29: Login in DPMAdirektPro ..... 36
Abbildung 30: Individuelles Passwort setzen ..... 37
Abbildung 31: Anforderungen an die Passwortvergabe ..... 38
Abbildung 32: Menüleiste mit dem angemeldeten Benutzer ..... 38
Abbildung 33: Ausgesperrte und aktivierte Aktionen eines Vorgangs für die Benutzerrolle „Posteingang“ ..... 39

Abbildung 34: Ausgeblendete Einstellungen für die Benutzerrolle „Posteingang“ ..... 40
Abbildung 35: Vordefinierte Benutzerrollen und deren Rechte ..... 41
Abbildung 36: Anwendungsszenario mit 2 getrennten Abteilungen ..... 43