



- **Vorteile der Netzwerkversion**
- **Bedeutung und Nutzung der Zertifikate**

Vorteile der Netzwerkversion

Wenn mehrere Personen aufgabenverteilt an einem Vorgang arbeiten sollen, wird der Einsatz der Netzwerkversion empfohlen. Diese Version ist eine typische Client-/Server-Anwendung, d.h. auf einen zentralen Server greifen mehrere Anwender mit ihren Clients zu (siehe Grafik). 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.

Sollte eine Firewall vor dem Server installiert sein, muss der Zugriff der Clients auf den Port 1527 freigeschaltet werden. Auf den einzelnen Clients werden keine Daten mehr gespeichert. Der Datenaustausch mit den Clients erfolgt über den Server. Ein mögliches Anwendungsszenario finden Sie im nächsten Punkt.

Es ist auch möglich, die Client- und Serverkomponenten zusammen auf einem Rechner zu installieren.

Bedeutung und Nutzung der Zertifikate

Zur Nutzung von DPMAdirekt sind zwei verschiedenen Zertifikate notwendig, ein Signaturzertifikat und ein Verschlüsselungszertifikat

Das Signaturzertifikat

Das Signaturzertifikat ist auf Ihrer qualifizierten Signaturkarte enthalten und wird zum Signieren der Nachricht an das Deutsche Patent- und Markenamt (DPMA) benutzt. Als Signaturkarte wird jede von der Bundesnetzagentur (www.bundesnetzagentur.de) zugelassene qualifizierte Signaturkarte akzeptiert. Mit der qualifizierten Signatur wird die persönliche Unterschrift ersetzt. Rechtsgrundlage ist u. a. das Bürgerliche Gesetzbuch (BGB):

„§ 126 (3): Die schriftliche Form kann durch die elektronische Form ersetzt werden, wenn sich nicht aus dem Gesetz ein anderes ergibt.

§ 126a (1): Soll die gesetzlich vorgeschriebene schriftliche Form durch die elektronische Form ersetzt werden, so muss der Aussteller der Erklärung dieser seinen Namen hinzufügen und



Newsletter 19

das elektronische Dokument mit einer qualifizierten Signatur nach dem Signaturgesetz versehen.“

Merke: Signaturkarte = persönliche Unterschrift

Das Verschlüsselungszertifikat

Das Verschlüsselungszertifikat erscheint bei jedem Programmstart und fordert Sie zur Eingabe Ihrer Signatur-/Verschlüsselungs-/Authentisierungs-PIN auf.

Es hat fünf Funktionen:

- Geschützte Anmeldung am Programm DPMAdirekt
- Einrichtung eines elektronischen Postfachs beim DPMA
- Nutzer- und Ablaufsteuerung in DPMAdirekt
- Verschlüsselung des Nachrichtenweges vom DPMA zum Anwender
- Nutzung als Signaturzertifikat im Demomodus

Es gibt zwei Möglichkeiten das Verschlüsselungszertifikat zu erhalten.

a) Bei der Installation oder später durch Auswahl des entsprechenden Menüpunktes wird ein Softwarezertifikat durch den Anwender erstellt. Die dort einzutragenden Angaben einschließlich der PIN legen Sie selbst fest.

b) Nutzung des Verschlüsselungszertifikats Ihrer Signaturkarte.

Wir empfehlen die Nutzung des selbst erstellten Softwarezertifikats. Sollten Sie das Verschlüsselungszertifikat der Signaturkarte nutzen, beachten Sie bitte, dass mit Ablauf der Gültigkeit Ihrer Karte auch dieses Zertifikat seine Gültigkeit verliert.

Die Anmeldung am Programm DPMAdirekt

Beim Start von DPMAdirekt wird Ihr eingerichtetes Softwarezertifikat nach der durch Sie vergebenen PIN fragen. So ist sichergestellt, dass nur der berechtigte Personenkreis auf Ihre Vorgänge zugreifen kann.

Einrichtung eines elektronischen Postfaches beim DPMA

Mit dem Verschlüsselungszertifikat wird beim DPMA ein so genanntes elektronisches Postfach eingerichtet. Das heißt, alle Benutzer, die sich mit dem gleichen Zertifikat an DPMAdirekt an-

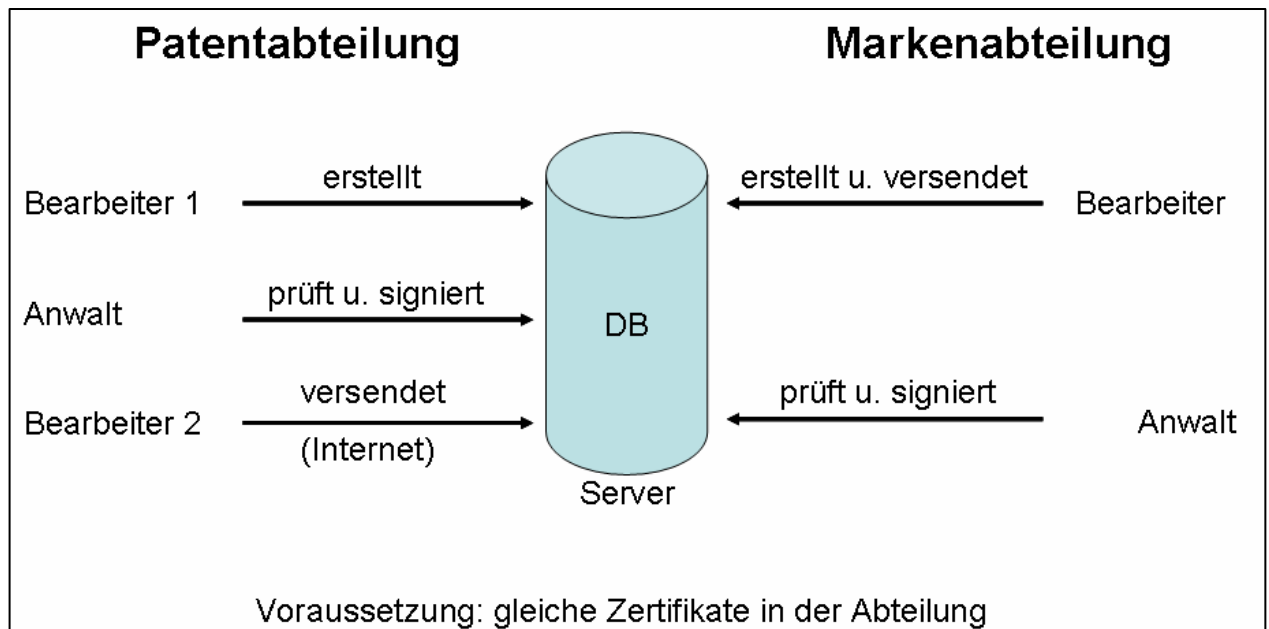


melden, können auf das gleiche Postfach zugreifen. Von diesem Postfach wird mit DPMAdirekt die Anmeldebenachrichtigung mit dem Amtlichen Aktenzeichen abgeholt.

Nutzer- und Ablaufsteuerung in DPMAdirekt 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 DPMAdirekt zugreifen.

Ein Beispiel:



Grafik: Beispiel eines möglichen Anwendungsszenarios

In einer Kanzlei gibt es einen Patent- und einen Markenbereich. In jedem Bereich sollen der jeweilige Anwalt und die Sachbearbeiter auf die eigenen Vorgänge zugreifen können. Ein bereichsübergreifender Zugriff wird nicht gewünscht. Es wurde die Netzversion von DPMAdirekt installiert.

Dazu wird ein Zertifikat für den Patentbereich und eins für den Markenbereich erzeugt. Das Patentzertifikat wird auf die Rechner des jeweiligen Anwalts und der Sachbearbeiter kopiert und als zu nutzendes Zertifikat in DPMAdirekt eingetragen. Nun ist es möglich, dass die Bereiche einen Vorgang arbeitsteilig bearbeiten können.



Newsletter 19

Für den Patentbereich wären folgende Abläufe möglich:

Der Sachbearbeiter 1 erstellt die Anmeldeunterlagen. Nachdem der Vorgang in den Status „Unterschriftsbereit“ verschoben wurde, ruft der Anwalt das Autorisieren auf. Nach Durchsicht der Unterlagen autorisiert er den Vorgang, d.h. er signiert mit seiner Signaturkarte. Der Vorgang wird automatisch in den Status „Bereit zur Einreichung“ verschoben. Sollte der Anwalt Fehler feststellen, kann er den Vorgang in den Status „Entwurf“ zurück verschieben. Eine Korrekturanmerkung kann hinzugefügt werden. Der Sachbearbeiter kann den Vorgang erneut bearbeiten und verschiebt ihn anschließend wieder nach „Unterschriftsbereit“.

Wenn der Vorgang in „Bereit zur Einreichung“ liegt, kann der Sachbearbeiter 2 den Vorgang an das DPMA versenden und anschließend die Anmeldebescheinigung abholen. Bei diesem Szenario wäre es möglich, dass nur dieser Sachbearbeiter in der Patentabteilung Zugang zum Internet benötigt.

Dem Bereich Marken ist es nicht möglich, Zugriff auf die Patentvorgänge zu erlangen.

Im Beispiel soll in der Markenabteilung der Sachbearbeiter das Erstellen und Versenden der Anmeldung übernehmen.

Bei weiteren Fragen oder Anregungen wenden Sie sich bitte an:

- Peter Klemm, Telefon (0 89) 21 95 – 37 79 oder
- Uwe Gebauer, Telefon (0 89) 21 95 – 26 25 oder
- per Mail an: DPMAdirekt@dpma.de