Das DMS-Portal der Nordrheinischen Ärzteversorgung

Dr. Peter Koch

Das DMS-Portal der Nordrheinischen Ärzteversorgung

von Dr. Peter Koch

Veröffentlicht 07. Oktober 2014, 12:18 Uhr

Zusammenfassung

Dieses Handbuch beschreibt die Benutzung und Installation des DMS-Portals der Nordrheinischen Ärzteversorgung.

Dieses Handbuch ist sowohl in elektronischer Form als auch in gedruckter Form verfügbar. Die elektronische Version erreichen Sie unter der Adresse http://portal.naev.de/help. Eine PDF-Datei zum Ausdruck des gesamten Handbuches ist unter http://portal.naev.de/help/doku.pdf [doku.pdf] verfügbar.

Inhaltsverzeichnis

Abbildungsverzeichnis

Kapitel 1. Benutzung des Portals

1.1. Grundlegender Ablauf

Dieser Abschnitt liefert einige Hintergrundinformationen zur Benutzung des DMS-Portals der Nordrheinischen Ärzteversorgung und kann überschlagen werden falls das Hauptinteresse darin besteht das Portal so schnell wie möglich benutzen zu können.

Über das DMS-Portal der Nordrheinischen Ärzteversorgung können dazu berechtigte Personen auf Dokumente aus dem Dokumenten Management System der Nordrheinischen Ärzteversorgung zugreifen. Aus Sicherheitsgründen ist allerdings ein direkter Zugriff nicht möglich und auch nicht ein Zugriff auf die Original-Dokumente.

Stattdessen wurde ein sogenannter Portal-Server eingerichtet, der als Vermittler zwischen der Aussenwelt und dem internen Netz der Nordrheinischen Ärzteversorgung fungiert. Dieser Server hat einerseits eine direkte Verbindung ins Internet und auf ihn kann deshalb von allen anderen Rechnern mit Internet-Verbindung zugegriffen werden. Andererseits befindet sich dieser Rechner physikalisch im Rechenzentrum der Nordrheinischen Ärzteversorgung und er hat deshalb über eine speziell abgesicherte und nur für ihn zugängliche Verbindung Zugriff auf das Dokumenten Management System der Nordrheinischen Ärzteversorgung.

Der Zugriff auf den Portalserver ist nur mittels eines sogenannten 2-Faktor Authentifizierungsverfahren möglich. Dabei muss der Anwender den Besitz eines Sicherheitstokens nachweisen (erster Authentifzierungsfaktor) und zusätzlich die Kenntnis eines Passwortes (zweiter Authentifizierungsfaktor). Als mögliche Sicherheitstoken verwendet die Nordrheinische Ärzteversorgung:

- CryptoSticks des Herstellers Feitian, die in ihrere Form kleinen blauen USB-Sticks ähneln
- Heilberufsausweise der Ärztekammer Nordrhein (sowohl gesetzeskonforme Version als auch Light-Variante)
- Mitarbeiterausweise der Nordrheinsichen Ärzteversorgung

Nach erfolgreicher Authentifizierung leitet der Portal-Server Dokumenten-Anfragen des Anwenders durch eine speziell gesicherte Verbindung an einen internen Server im Netz der Nordrheinischen Ärzteversorgung weiter. Die Aufgabe des internen Servers besteht darin, zu prüfen, auf welche Dokumente dem Anwender Zugriff gewährt werden darf, und diese ggf. aus dem Dokumenten Management System der Nordrheinischen Ärzteversorgung auszulesen. Nach dem Auslesen eines Original-Dokumentes wird dieses mit einem individuellen Wasserzeichen versehen und verschlüsselt an den Portal-Server übermittelt.

Auf keinen Fall verlassen Dokumente aus dem Dokumenten Management System der Nordrheinischen Ärzteversorgung das Netz der Nordrheinischen Ärzteversorgung in der unverschlüsselten Original-Fassung.

Zusammengefasst ergibt das folgenden Ablauf:

1. Authentifizierung am externen Portalserver
2. Weiterleiten von Dokumenten-Anfragenvom externen Portal-Server an den internen Portalserver.
3. Prüfung des Zugriffsberechtigungen auf dem internen Portal-Server.
4. Auslesen des Original-Dokumentes aus dem DMS.
5. Hinzufügen des individuellen Wasserzeichens und Verschlüsselung des Dokumentes.
6. Übermittlung des verschlüsselten Dokuemntes an den Portal-Server.
7. Weiterleitung des verschlüsselten Dokumentes vom Portal-Server an den Browser des Anwenders.

1.2. Benutzung mittels Dell XPS12 Tablet-PC

Im Nachfolgenden wird die Nutzung des Portals mit einem Dell Tablet-PC Modell XPS12 unter Einsatz des aktuellsten Firefox Browsers beschrieben. Die in diesem Abschnitt vorhandenen Screenshots wurden genau mit diesem Gerät erstellt. In nachfolgenden Abschnitten wird dann auf Unterschiede eingegangen, die sich bei der Benutzung mit anderen Geräten und/oder Browsern ergeben.

1.2.1. Anmeldung am Windows 8 Betriebssystem

Der Einschalt-Knopf des Dell XPS12 Tablet-PC befindet sich an der linken Geräteseite und wird nicht durch Drücken sondern durch Verschieben betätigt. Unter dem Einschaltknopf befindet sich ein Schalter zur Einstellung der Lautstärke, mit dem sie in Sitzungen störenden Geräusche vermeiden können. Im Auslieferungszustand des Gerätes ist der Lautsprecher auf Stumm geschaltet.

Die Anmeldung erfolgt auf allen Geräten mit dem Benutzer "naev". Da von Windows 8 bei der Anmeldung als zu verwendender Benutzername der zuletzt verwendete Name vorgeschlagen wird, ist es in der Regel nicht erforderlich den Benutzernamen einzugeben, sondern "naev" wird bereits angezeigt.

Das Passwort für die Anmeldung als Benutzer "naev" befindet sich auf der Nutzungsvereinbarung, die ihnen zusammen mit dem Gerät ausgehändigt wurde und die sie aus diesem Grund nicht gemeinsam mit dem Gerät aufbewahren sollten.

1.2.2. Verbinden des CryptoSticks

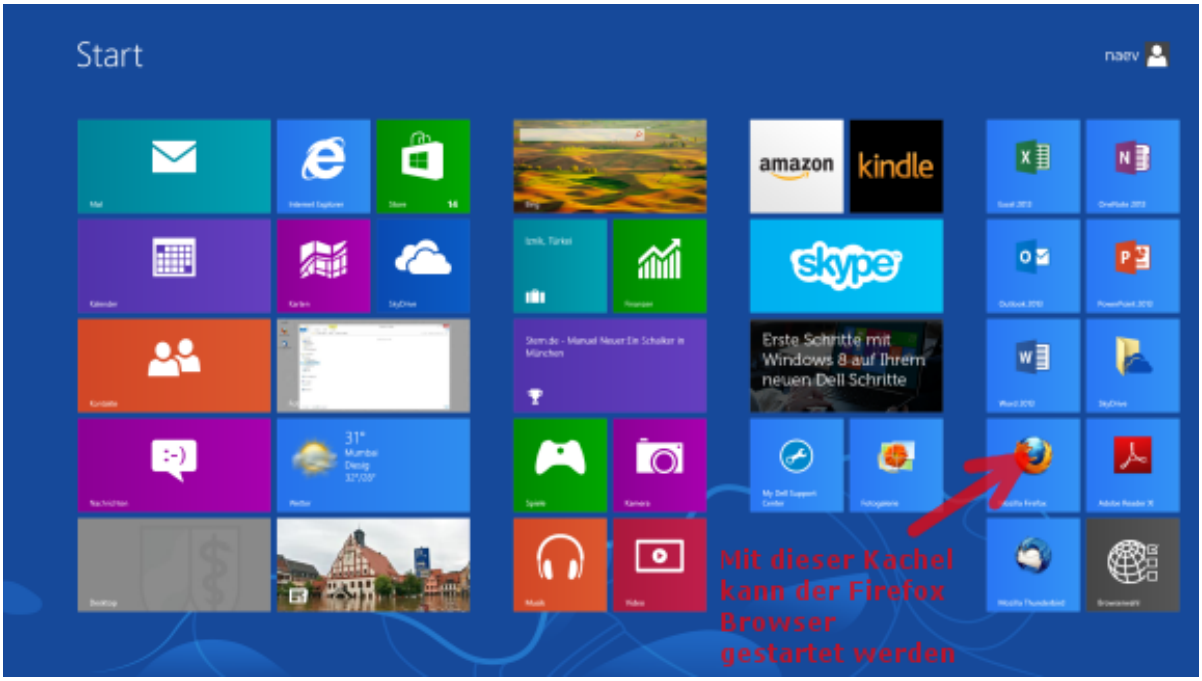
Vor dem Starten des Firefox-Browsers sollten sie unbedingt den CryptoStick mit ihrem Rechner verbinden, da bei einer nachträglichen Verbindung die Gefahr besteht, dass der Browser den CryptoStick nicht mehr erkennt.

Entsprechendes gilt bei Einsatz eines Heilberufsausweises. Dann sollte vor Starten des FireFox-Browsers der Kartenleser angeschlossen und der Heilberufsausweis eingesteckt sein.

1.2.3. Starten des Browsers

Für den Zugriff auf das DMS-Portal muss die Firefox Browser Anwendung gestartet werden. Sofern der Tablet-PC die Kachel-Oberfläche von Windows 8 anzeigt, kann dies durch Bestätigen der entsprechenden Kachel erfolgen (siehe nachfolgender Screenshot).

Abbildung 1.1. Die Kachel-Oberfläche von Windows 8

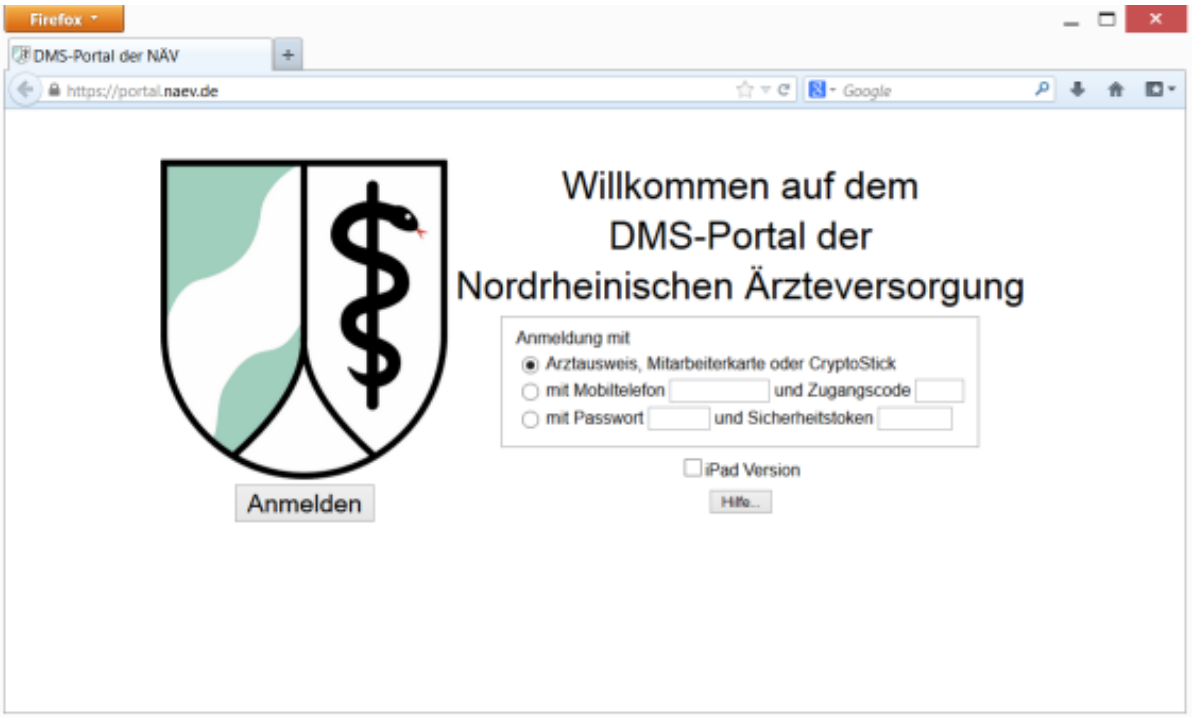


Alternativ kann mit der Windows-Taste auf die Desktop-Ansicht gewechselt werden und dort durch Doppelklick auf das Start-Icon des Firefox-Browsers die Anwendung gestartet werden. Die Windows-Taste befindet sich beim Dell XPS12 Tablet-PC am unteren linken Rand der Tastatur zwischen der Fn- und Alt-Taste (dritte Taste von links).

Abbildung 1.2. Die Desktop-Ansicht von Windows 8

In beiden Fällen wird der Firefox-Browser gestartet. Da er so vorkonfiguriert wurde, dass als Startseite portal.naev.de [http://portal.naev.de] angezeigt wird, sollte unmittelbar nach dem Start folgende Ansicht erscheinen. Sollte dies nicht der Fall sein, z.B. weil sie einen anderen Browser verwenden oder die Startseite geändert wurde, ist ggf. im Browser die URL portal.naev.de [http://portal.naev.de] manuell einzugeben. Beachten sie, dass die URL des DMS-Portals nicht wie so viele andere URLs mit www beginnt.

Abbildung 1.3. Die Startseite des DMS-Portals



1.2.4. Der Ameldevorgang am Portal

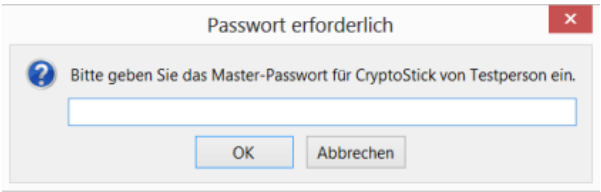
Die Anmeldung erfolgt durch Betätigung der entsprechenden Schaltfläche. Der Portal-Server überprüft dann das Vorhandensein eines gültigen und registrierten Zertifikates auf ihrem CryptoStick (oder Heilberufsausweis).

Wenn sie den "Anmelden"-Knopf betätigen, ohne dass ihr CryptoStick mit dem Rechner verbunden ist, erhalten sie die Fehlermeldung: **E1: keine Anmeldeinformation erhalten**. In diesem Fall müssen sie die Browser-Anwendung beenden und mit gestecktem CryptoStick erneut starten.

Sollten sie obige Fehlermeldung auch bei gestecktem CryptoStick (bzw. bei gestecktem Hailberufsausweis) erhalten, so liegt die Vermutung nahe, dass der FireFox-Treiber für ihren CryptoStick (bzw. Heilberufsausweis) nicht korrekt installiert wurde. Wenden sie sich in diesem Fall bitte an ie EDV-Abteilung der Nordrheinischen Ärzteversorgung.

Falls der Firefox-Browser das Vorhandensein des CryptoSticks feststellt und dieser noch nicht freigeschaltet wurde, so wird er nach Bestätigen des **Anmelden**-Knopfes die 8-stellige PIN des CryptoSticks anfordern. Hierzu erscheint folgendes Fenster:

Abbildung 1.4. Der PIN Abfragedialog während der Anmeldung



In obigem Beispiel wurde zu Demonstartionszwecken ein CryptoStick eingesetzt, auf dem sich ein Zertifikat befindet, das auf den Namen "Testperson" ausgestellt wurde. Bei einem echten Zugriff erscheint in obigem Dialog der Name des tatsächlichen Besitzers. Beachten sie, dass alle ausgegebenen CryptoSticks ein identisches Aussehen haben. Ob der von ihnen benutzte CryptoStick tatsächlich der ihrige ist oder sie irrtümlich den CryptoStick eines Kollegen benutzen, lässt sich optisch nicht unterscheiden sondern nur durch die Angabe des Namens in obigem PIN-Eingabedialog.

Den Anfangswert der PIN ihres CryptoSticks finden sie auf der Nutzungsvereinbarung, die ihnen zusammen mit dem Gerät ausgehändigt wurde und die sie aus diesem Grund nicht gemeinsam mit dem Gerät aufbewahren sollten.

Beachten sie auch, dass nach 5facher Falscheingabe der PIN der CryptoStick dauerhaft unbrauchbar wird. Sollten sie also sicher sein, dass sie die korrekte PIN benutzen und die Anwendung behauptet das Gegenteil, so besteht die Gefahr, dass mehrfache Wiederholungen der gleichen PIN-Eingabe den CryptoStick dauerhaft unbrauchbar machen. Wenden sie sich in einem solchen Fall bitte an die Hotline der EDV-Abteilung der Nordrheinischen Ärzteversorgung.

Nachdem sie die PIN ihres CryptoSticks einegeben haben werden sie mit dem DMS-Portal der Nordrheinischen Ärzteversorgung verbunden. Die Anmeldung ist nur für eine befristete Zeit gültig und endet automatisch, wenn sie für eine bestimmte Zeit keine Aktivitäten durchführen. In jedem Fall wird die Anmeldung beendet, wenn sie den Firefox-Browser schließen.

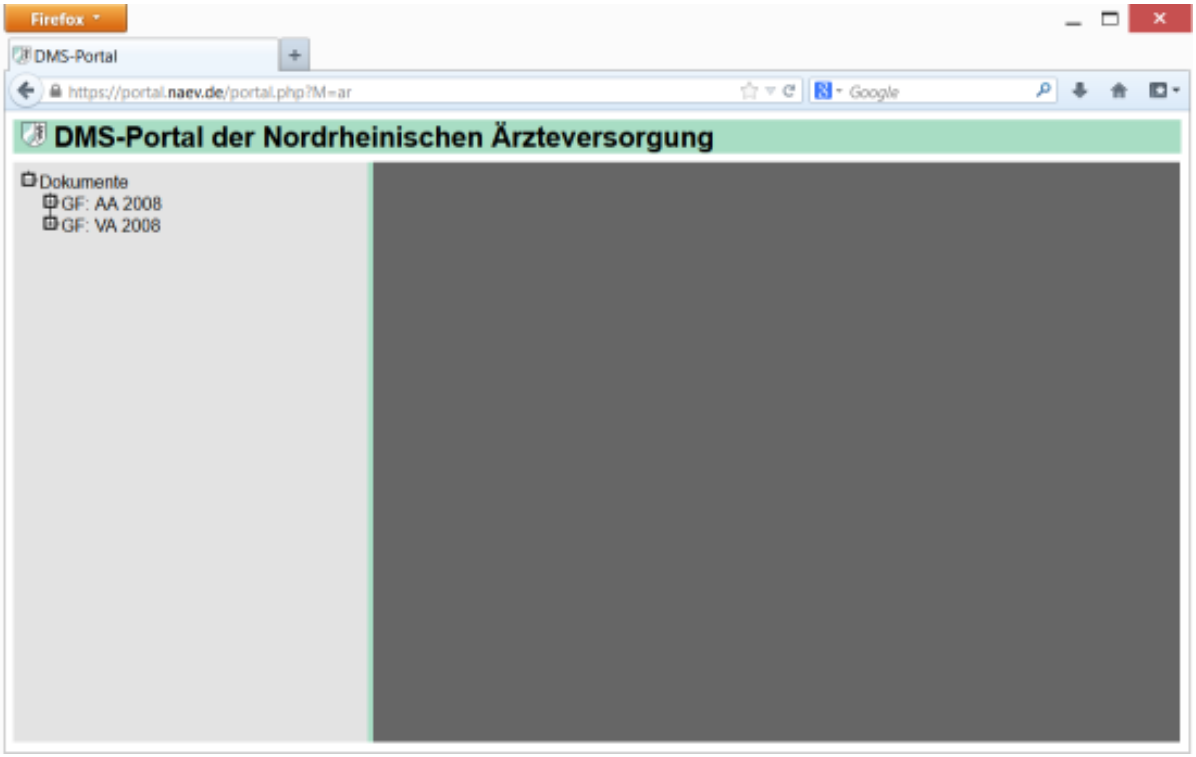
Wenn sie einen Heilberufsausweis verwenden wird in analoger Weise die PIN des Ausweises abgefragt, es sei denn sie haben diese bereits vorher anlkäßlich einer anderen Authentifizierung eingegeben.

1.2.5. Nutzung des Portals

Unmittelbar nach erfolgter Anmeldung kommt es zu einer kurzen Verzögerung während der vom Browser das Inhaltsverzeichnis des DMS-Portals eingelesen wird. Diesen Einlesevorgang erkennen sie daran, dass im linken Fensterbereich ein sich drehendes Rad angezeigt wird. Damit die Verzögerung möglichst kurz ausfällt, wird direkt nach der Anmeldung nur das Inhaltsverzeichnis der Gremiensitzungen seit Anfang 2014 eingelesen. Das vollständige Inhaltsverzeichnis kann mit dem Knopf am oberen rechten Bildrand nachgeladen werden.

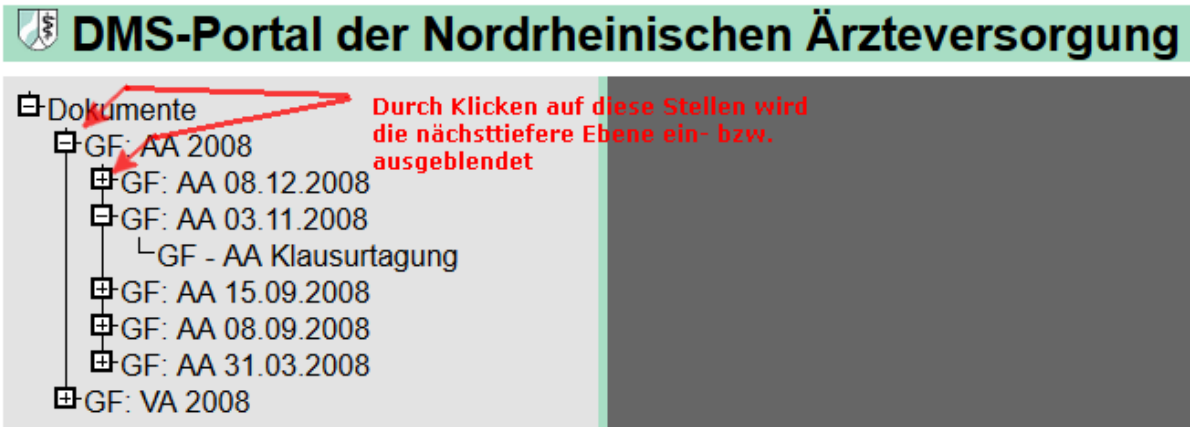
Ist das Inhaltsverzeichnis eingelesen, erhalten sie folgende Ansicht (im nachfolgenden Screenshot ist aus Datenschutzgründen nur ein stark verkürztes Inhaltsverzeichnis aus dem Jahr 2008 angezeigt, das tatsächlich verwendete Inhaltsverzeichnis ist natürlich deutlich umfänglicher und aktueller):

Abbildung 1.5. Das Inhaltsverzeichnis des DMS-Portals



Das Inhaltsverzeichnis zeigt auf oberster Ebene die Jahrgänge an, zu denen Dokumente bereitstehen, in obigem Screenshot also die AA-Protokolle aus 2008 und die VA-Protokolle aus 2008. Auf der mittleren Ebene können zu einem Jahr die in diesem Jahr stattgefundenen Gremiensitzungen ausgewählt werden. Auf der untersten Ebene findet man pro Gremiensitzung alle zur ausgewählten Sitzung gehörenden Dokumente.

Abbildung 1.6. Das Aufklappen der Inhalts-Ebenen



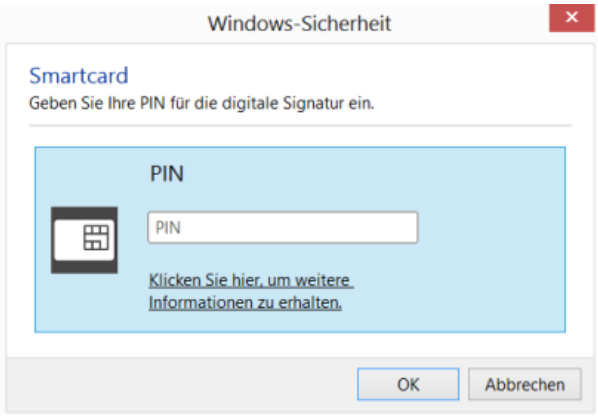
In obigem Beispiel wurden alle AA-Sitzungen des Jahres 2008 ausgewählt und für die AA-Sitzung vom 3.11.2008 die vorhandenen Dokumente angezeigt (in diesem Fall aus Demonstrationszwecken nur ein einziges Dokument mit Titel **Klausurtagung**).

Wählt man ein Dokument auf der dritten Ebene aus (durch Anklicken), wird genau dieses Dokument im rechten Bereich des Fensters als PDF-Dokument angezeigt.

Da die PDF-Dokumente vom Portal-Server im verschlüsselten Zustand an den Firefox-Browser ausgeliefert werden, muss das Dokument lokal auf dem Rechner des Anwenders mit dem dort vorhandenen CryptoStick entschlüsselt werden. Diese Entschlüsselung wird vom Acrobat Reader vorgenommen,

der dafür ebenfalls die PIN des CryptSticks benötigt. Aus diesem Grund wird der Acrobat Reader vor der Anzeige des ersten Dokumentes erneut die PIN des CryptoSticks abfragen. Die Acrobat-Anwendung verwendet hierfür im Gegensatz zum Firefox-Browser folgenden Dialog:

Abbildung 1.7. Der PIN Abfragedialog für die Dokumenten-Entschlüsselung



Beachten sie, dass in der PIN-Abfrage des Acrobat Readers nicht der Name des CryptoStick-Besitzers angegeben wird. Ausserdem bezeichnet der Acrobat Reader den CryptoStick als Smartcard und verlangt nach einer PIN für eine durchzuführende Signatur. Dies ist ein Ungenauigkeit des Acrobat Readers, der in Wirklichkeit die PIN ihres CryptoSticks für einen Entschlüsselungsvorgang benötigt.

Für die Anzeige weiterer Dokumente ist keine erneute PIN-Eingabe erforderlich, so dass zusammen mit der Anmeldung die PIN genau zwei Mal eingegeben werden muss.

Nach erfolgter Entschlüsselung des Dokumentes ergibt sich folgende Ansicht:

Abbildung 1.8. Die Ansicht eines Dokumentes im DMS-Portal

1.3. Grundlegender Ablauf, Teil 2

Dieser Abschnitt liefert weitere Informationen zur Nutzung des Portals. Die Informationen aus diesem Abschnitt sind vor allem im Fehlerfall von Bedeutung und müssen deshalb bei der ersten (hoffentlich erfolgreichen) Nutzung nicht beachtet werden.

Für die Anzeige eines Dokumentes müssen folgende Schritte erfolgreich durchgeführt werden:

1. Zuerst ist im Inhaltsverzeinis ein Klick auf das anzuzigende Dokument durchzuführen. An dieser Stelle ist es hilfreich zu erkennen, ob der Klickvorgang vom Browser erkannt wurde, oder ob man ggf. auf eine falsche Stelle geklickt hat. Letzteres kann insbesondere dann passieren wenn der Klickvorgang auf dem Bildschirm des Tablet-PC mit dem Finger ausgeführt wurde.

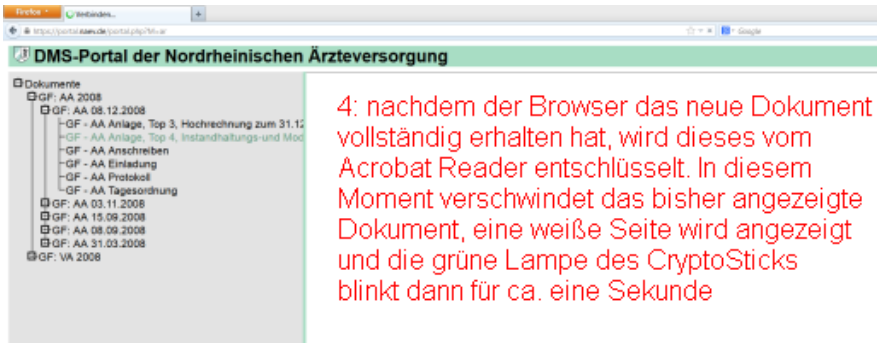
   Ob der Klickvorgang vom Browser erkannt wurde lässt sich durch Beobachten der Reiter-Überschrift erkennen. Lautet die Überschrift im Normalfall "DMS-Portal", so ändert sie sich als Reaktion auf eine Dokumentenanforderung in "Verbinden..."

2. Das DMS-Portal reagiert auf die Dokumentenanforderung indem es seinerseits das Dokument vom internen Portal-Server anfordert, es verschlüsselt und danach an den Browser weiterleitet. Während dieses Vorgangs wird in der Reiter-Überschrift des Browserfensters neben der "Verbinden..."-Überschrift ein sich drehender Kreis angezeigt.

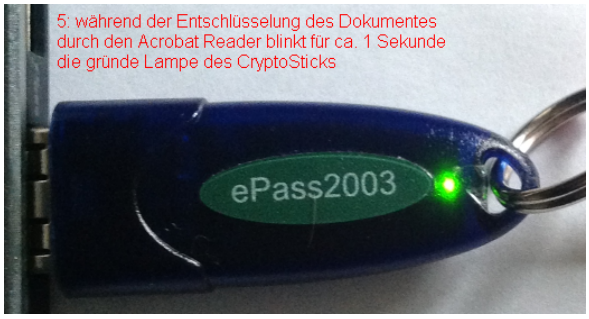
3. Während der Browser auf den Server wartet, also dann wenn das Dokument vom internen Portal-Server angefordert und verschlüsselt wird, wird der drehende Kreis in schwarzer Farbe angezeigt und der Kreis dreht sich im Gegenuhrzeigersinn. Sobald das Dokument an den Browser übermittelt wird ändert sich die Farbe in Grün und die Drehrichting in den Uhrzeigersinn.

   Hiermit hat man im Fehlerfall eine einfache Möglichkeit zu erkennen, wo ggf. die Ursache des Fehlers liegt. Bei drehendem schwarzem Kreis antwortet der Portal-Server nicht, was auf Server-Probleme hindeutet. Bei drehendem grünen Kreis dauert die Übermittlung des Dokumentes sehr lange, was auf eine langsame oder gestörte Internet-Verbindung hindeuten kann.

4. Sobald das angeforderte Dokument vollständig empfangen wurde, löscht der Browser das bisher angezeigte Dokument und zeigt stattdessen eine weiße Seite. In diesem Moment ist es die Aufgabe des Acrobat Readers das empfangene Dokument zu entschlüsseln. Dazu greift er auf den CryptoStick zu. Vor dem ersten Zugriff wird zusätzlich die PIN des CryptoSticks abgefragt.



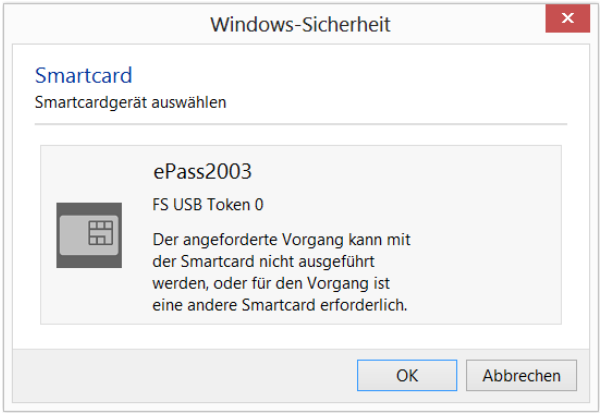
5. Beim Zugriff auf den CryptoStick blinkt dessen grüne Lampe. Wenn dies unmittelbar nach Anzeige der weißen Seite nicht passiert, ist das ein Indiz dafür, dass zwar das verschlüsselte Dokument korrekt vom Server empfangen werden konnte aber nicht angezeigt werden kann, weil die Verbidnung zwischen Browser und CryptoStick nicht (mehr) möglich ist.



Leider kann es passieren, dass der Browser die Verbindung zum CryptoStick verliert. Z.B. dann, wenn der Dell XPS12 Tablet-PC zugeklappt wird, sich dabei in den Energiesparmodus versetzt und später wieder angeschaltet wird. Im Gegensatz zur bloßen Abschaltung des Bildschirms (nach 15 Minuten Inaktivität) wird beim Energiesparmodus die Stromversorgung des CryptoSticks abgeschaltet - erkennbar am Verlöschen der grünen Lampe.

Nach dem Wiederanschalten des Tablet-PCs erscheint in diesem Fall dann folgende Fehlermeldung:

Abbildung 1.9. Fehlermeldung beim Verlust der Verbindung zum CryptoStick



Nach Erscheinen obiger Meldung bleibt keine andere Möglichkeit als den Firefox-Broser zu schliessen und den Anmeldevorgang beim Portal komplett zu wiederholen. Eventuell kann es sogar erforderlich sein, den CryptoStick zu entfernen und erneut mit dem Tablet-PC zu verbinden.

Kapitel 2. Installation

Sofern sie einen Dell XPS12 Tabelt-PC erhalten haben, können sie diesen ohne Installation einsetzen und das nachfolgende Kapitel ist für sie nur dann von Interesse, wenn sie auf das DMS-Portal zusätzlich auch von einem anderen Fest-PC oder Laptop aus zugreifen wollen.

Auf dem PC muss zur Nutzung des DMS-Portal der Nordrheinischen Ärzteversorgung eine möglichst aktuelle Version des Firefox-Browsers der Mozilla-Foundation eingesetzt werden.

Die aktuelleste deutsche Version des Firefox-Browsers findet man unter der Adresse http://www.mozilla.org/de/firefox auf den deutschsprachigen Seiten der Mozilla-Foundation.

Auf den Webseiten der Mozilla-Foundation findet man auch Hinweise zur Installation des Firefox-Browsers.

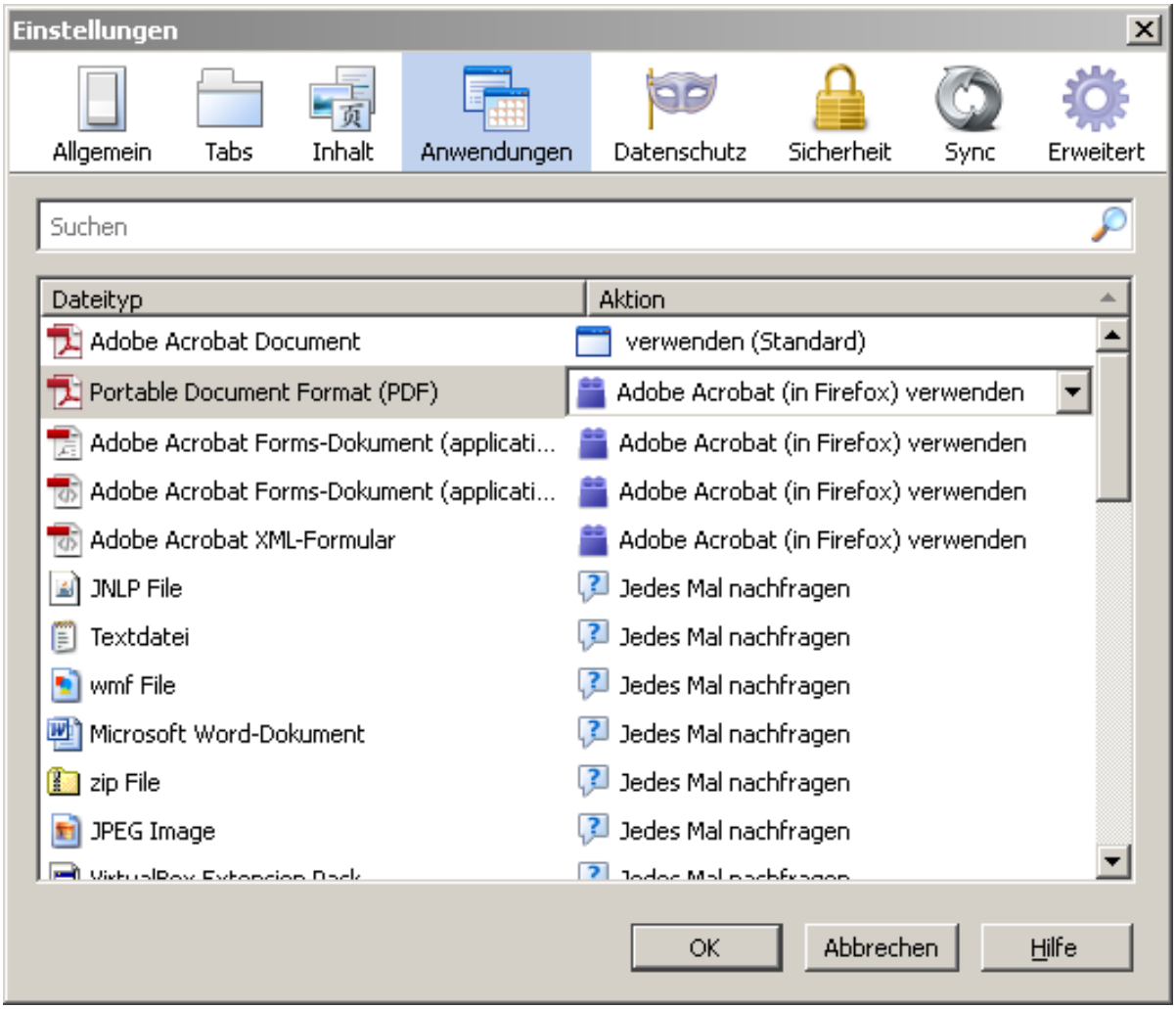
Darüberhinaus wird der kostenlose Acrobat-Reader Version XI benötigt und der Firefox-Browser muss so eingestellt sein, dass er für die Anzeige von PDF-Dateien den Acrobat-Reader benutzt. Wenn sie diese Anleitung im Firefox-Browser lesen, dann können sie auf diesen Link klicken [doku.pdf] und bei richtigen Einstellungen ihres Browsers, sollte dann im Browser-Fenster die PDF-Version dieser Anleitung mittels Acrobat-Reader angezeigt werden.

Alle uns bekannten Alternativen zum Acrobat-Reader (u.a. auch der Foxit-Reader) können leider nicht benutzt werden. Sie sind zwar schneller und benötigen weniger Speicher als der Acrobat-Reader, das aber nur weil selten benötigte Funktionen wie die Möglichkeit verschlüsselte Dateien anzuzeigen, fehlen. Geanud diese Möglichkeit zur Entschlüsselung wird aber beim Zugriff auf das Portal benötigt.

Es ist ebenfalls nicht möglich, den internen PDF-Viewer des Firefox-Browsers zu verwenden, da auch dieser nicht in der Lage ist verschlüsselte PDF-Dokumente zu entschlüsseln.

Ob sie die PDF_anzeige ihres FireFox-Browser korrekt eingestellt haben, erkennen sie in den Einstellungen auf dem Reiter "Anwendungen". Dort muss für den Dateityp "Portable Document Format (PDF)" die Aktion "Adobe Acrobat (in Firefox) verwenden" ausgewählt sein.

Abbildung 2.1. Die Einstellungen zur PDF-Ansicht im Firefox-Browser



Damit der Firefox-Browser und/oder der Acrobat-Reader auf einen CryptoStick oder einen elektronischen Ausweis zugreifen kann, sind mehrere Treiber erforderlich, nämlich:

- Betriebssystem-Treiber
- Firefox-Treiber
- Acrobat-Reader Treiber

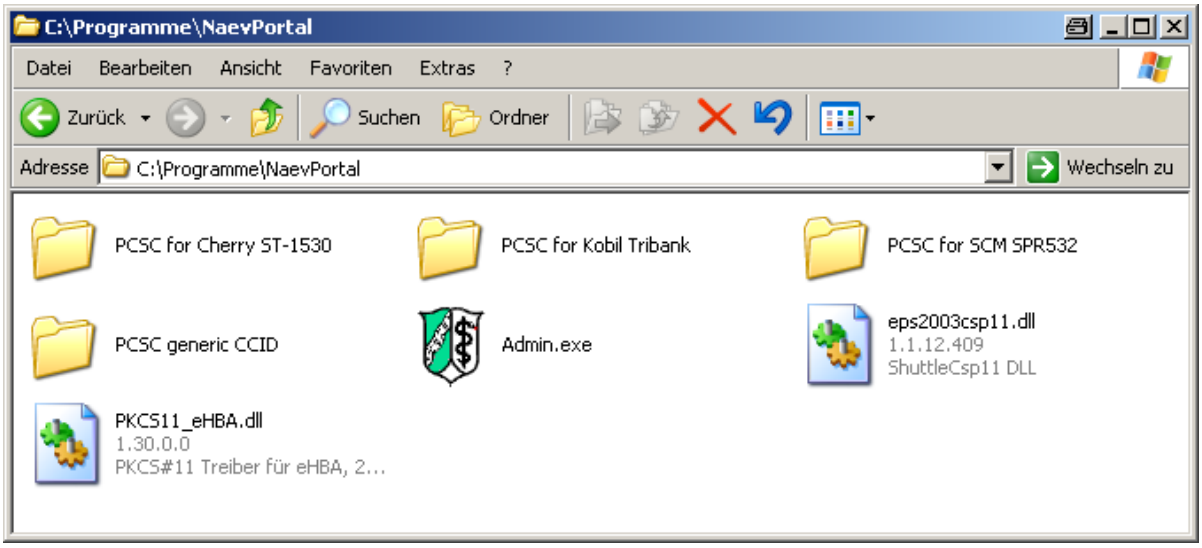
Zur Installation dieser Treiber sind Dateien erforderlich, die als ZIP-Datei vom Portalserver der Nordrheinischen Ärzteversorgung heruntergeladen werden können. Die Downloadadresse lautet: http://portal.naev.de/download/NaevPortal.zip

Die ZIP-Datei können sie durch einfachen Klick auf obigen Link auf ihren Rechner herunterladen. Das ZIP-Archiv enthält einen Ordner mit Namen `NaevPortal`, der wiederum folgende Dateien enthält:

- Verzeichniss mit Betriebssystem-Treibern für einige, häufig verwendete Kartenleser. Diese Namen dieser Verzeichnisse beginnen jeweils mit "PCSC ....". Diese Treiber benötigen sie nur, falls sie einen Heilberufsausweis verwenden wollen.
- Eine Treiberdatei mit Namen `PKCS11_eHBA.dll`. Diese ist bei Anwendern erforderlich, die einen elektronischen Arztausweis einsetzen.
- Eine Treiberdatei mit Namen `eps2003csp11.dll`. Diese ist bei Anwendern erforderlich, die einen CryptoStick Model ePass2003 benutzen.
- Ein Administrationsprogramm mit Namen `Admin.exe`.

Zur Installation kopieren sie bitte den Inhalt der ZIP-Datei (also das Verzeichnsis `NaevPortal`) in ihr `C:\Programme (x86)`-Verzeichnis. Im Anschluss an diesen Kopiervorgang sollte ein Verzeichnis mit Namen `C:\Programme (x86)\NaevPortal` mit folgendem Inhalt existieren:

Abbildung 2.2. Das Inhaltsverzeichnis des Installations-Ordners



2.1. Treiberinstallation für Kartenleser

Wenn Sie einen CryptoStick benutzen, benötigen sie keinen Kartenleser und dementsprechend auch keine Kartenleser-Treiber. In diesem Fall können sie den nachfolgenden Abschnitt überspringen, da die Betriebssystemtreiber für den CryptoStick automatisch beim ersten Einstecken des CryptoSticks installiert werden.

Für die Installation von Treibern für einen Kartenleser sind lokale Administratorrechte erforderlich. Falls sie nicht über diese Rechte verfügen, müssen sie sich ggf. an den Administrator ihres Rechners wenden. Vorher sollten sie jedoch überprüfen, ob die Treiber nicht bereits vorhanden sind.

Hierzu starten sie das Administrationsprogramm `Admin.exe` ohne dass sich eine Karte im Kartenleser befindet (bzw. ohne dass sich der elektronische Ausweis im USB-Stick Format in einem USB-Port befindet). Lassen sie sich dann mit der "Kartenanzahl"-Schaltfläche die Anzahl der vorhandenen elektronischen Ausweise anzeigen. Stecken sie dann ihren elektronischen Ausweis in den Kartenleser (bzw. einen USB-Port). Wenn sich dann bei erneuter Betätigung der "Kartenanzahl"-Schaltfläche die Anzahl der vorhandenen Karten erhöht, wird ihr Kartenleser bereits unterstützt und eine Installation zusätzlicher Treiber ist nicht erforderlich. Bleibt die Anzahl konstant, fehlt ein Treiber oder es liegt ein anderes Problem vor.

Zur Installation eines Treibers für einen Kartenleser mit USB-Anschluss verfahren sie wie folgt:

1. Entfernen sie den Kartenleser (bzw. den Ausweis in USB-Stick Format) vom Rechner.

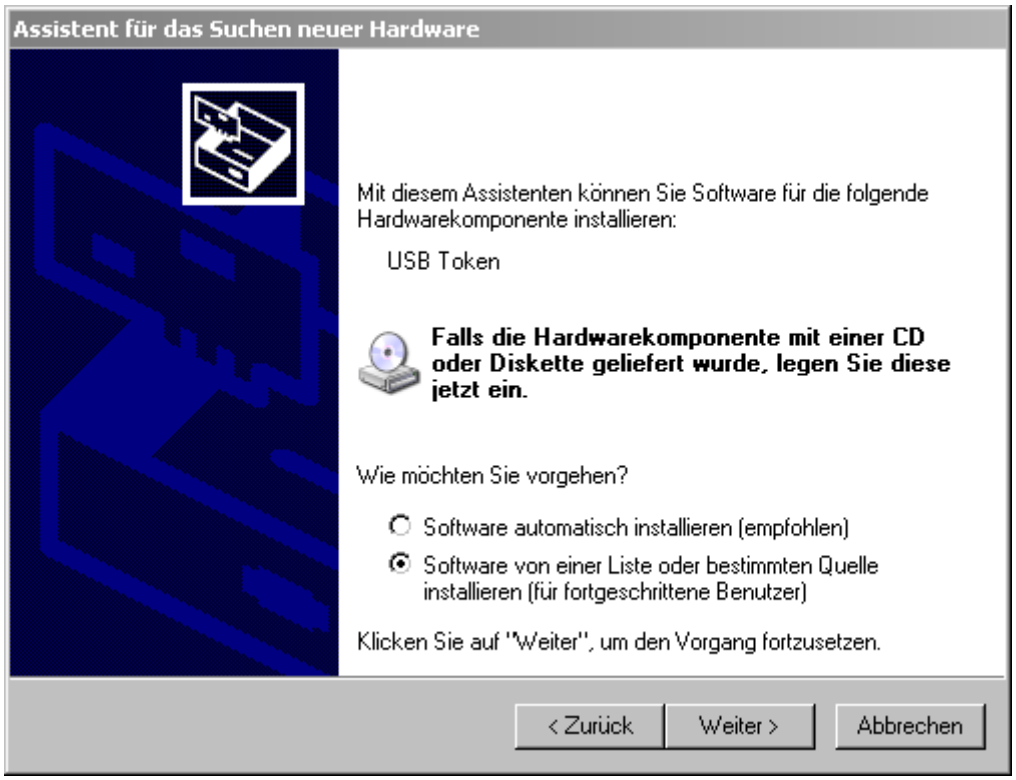
2. Schliessen sie den Kartenleser (bzw. den Ausweis in USB-Stick Format) erneut an ihren PC an.

3. Ihr Rechner sollte nun ein neues unbekanntes Gerät erkennen und versuchen einen passenden Treiber zu installieren. Falls dies nicht passiert, existiert bereits ein Treiber oder ihr PC konnte das Gerät nicht erkennen.

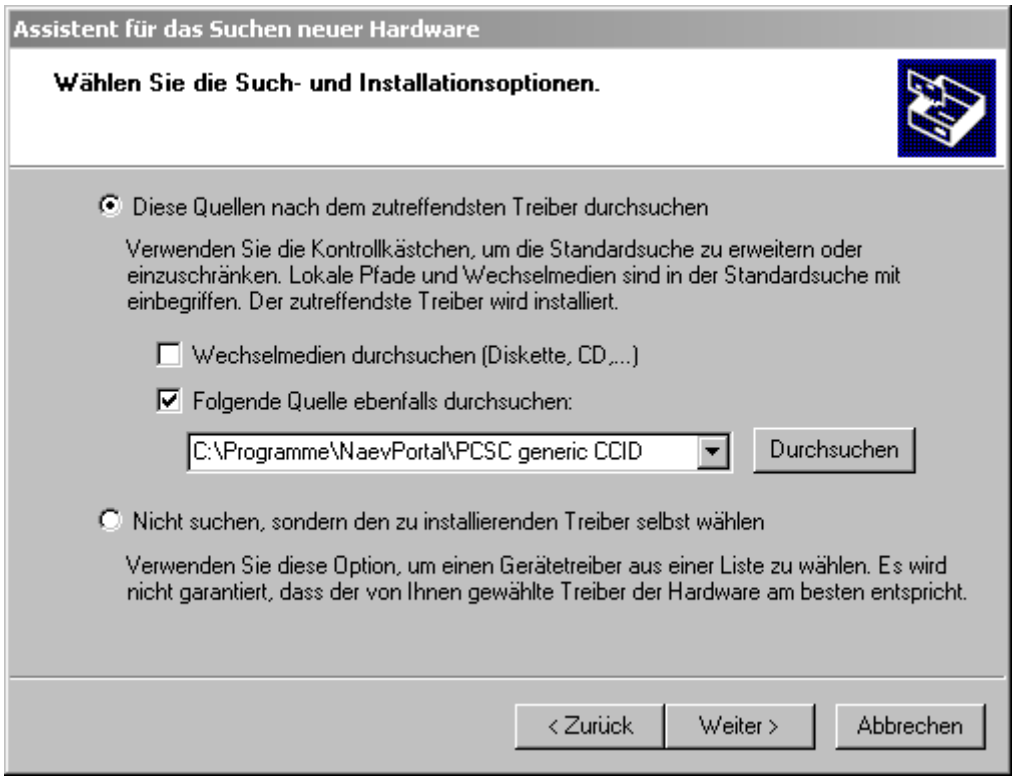
4. Falls sie nicht über Administrator-Rechte verfügen erscheint in diesem Moment das folgende Fenster, in dem sie aufgefordert werden den Namen und das Passwort eines Benutzers anzugeben, der im Gegensatz zu ihnen über Administrator-Rechte verfügt.

5. Danach erscheinen die beiden folgenden Fenster:

und



6. Wählen sie im ersten Fenster die Option, bei der kein Kontakt mit "Windows Update" hergestellt wird und im zweiten Fenster diejenige Option, bei der Software von einer bestimmten Quelle installiert wird. Bei Windows XP heissen diese Option z.B. "Nein, diesmal nicht" und "Software von einer Liste oder bestimmten Stelle installieren", bei anderen Windows Betriebssystemen geringfügig anders. Mit zwei Mal "Weiter" gelangen sie zu folgendem Fenster.

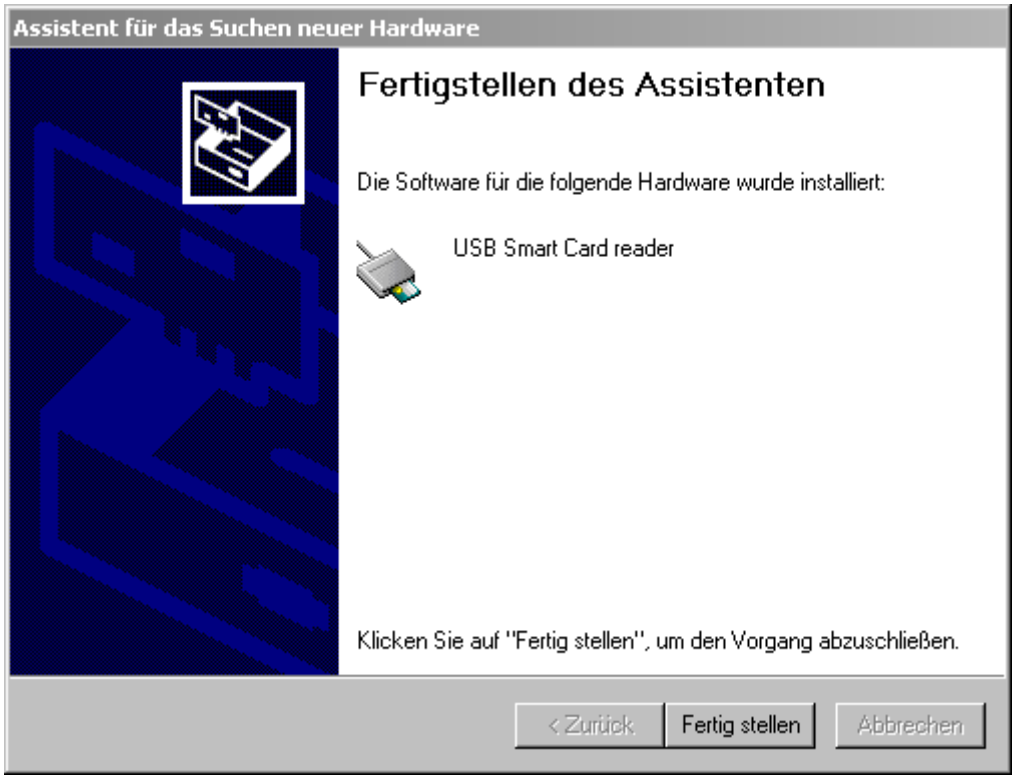


7. Wählen sie nun mit der "Durchsuchen"-Schaltfläche den Ordner aus, in dem sich der passende Treiber befindet. Der von ihnen angelegte Ordner `C:\Programme (x86)\NaevPortal` enthält eine Reihe solcher Treiber-Ordner für die gängigsten Kartenleser. Sollte sie über ein Kartenlesermodell verfügen, für das kein passender Ordner in `C:\Programme (x86)\NaevPortal` vorhanden ist, so wenden sie sich bitte an die EDV-Abteilung der Nordrheinischen Ärzteversorgung. Die Namen der Treiber-Ordner beginnen alle mit "PCSC..." (für Personal Computer Smart Card).

Wenn sie einen elektronischen Ausweis in USB-Stick Format verwenden, dann benutzen sie den Treiber-Ordner `PCSC generic CCID`, ansonsten den Ordner mit der passenden Modellbezeichnung.

Zum Teil enthalten Modelle eines Herstellers die Hardware eines anderen Herstellers und in diesen Fällen ist der Treiber-Ordner des eigentlichen Herstellers der Hardware zu verwenden. So enthält z.B. der Cherry-Kartenleser Modell ST-2000 intern einen Kartenleser des Herstellers SCM. Es schadet nicht, unterschiedliche Treiber-Ordner auszuprobieren.

8. Nach erfolgreicher Installation erhalten sie folgende Meldung:

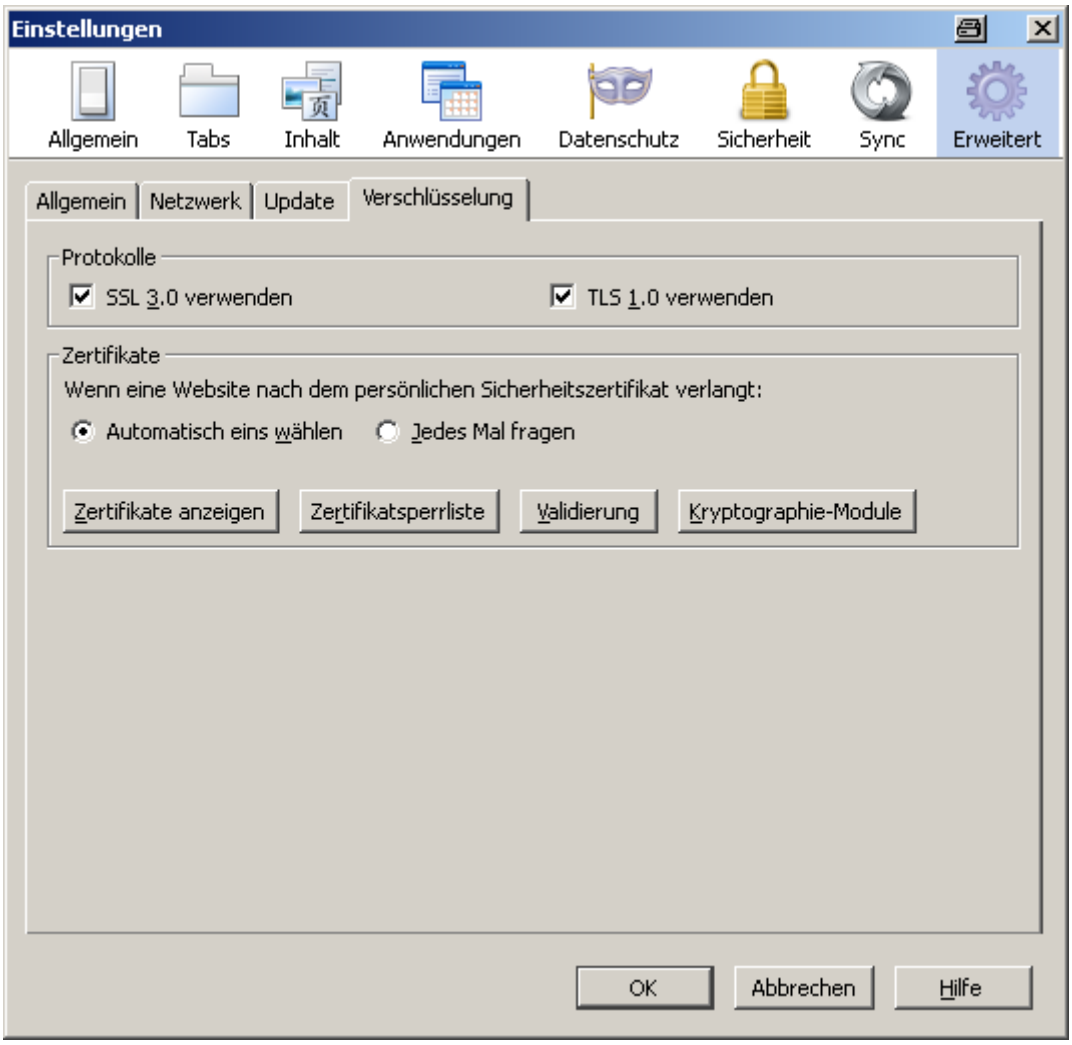


ansonsten die Meldung, dass kein passender Treiber gefunden wurde.

2.2. Treiberinstallation im Firefox-Browser

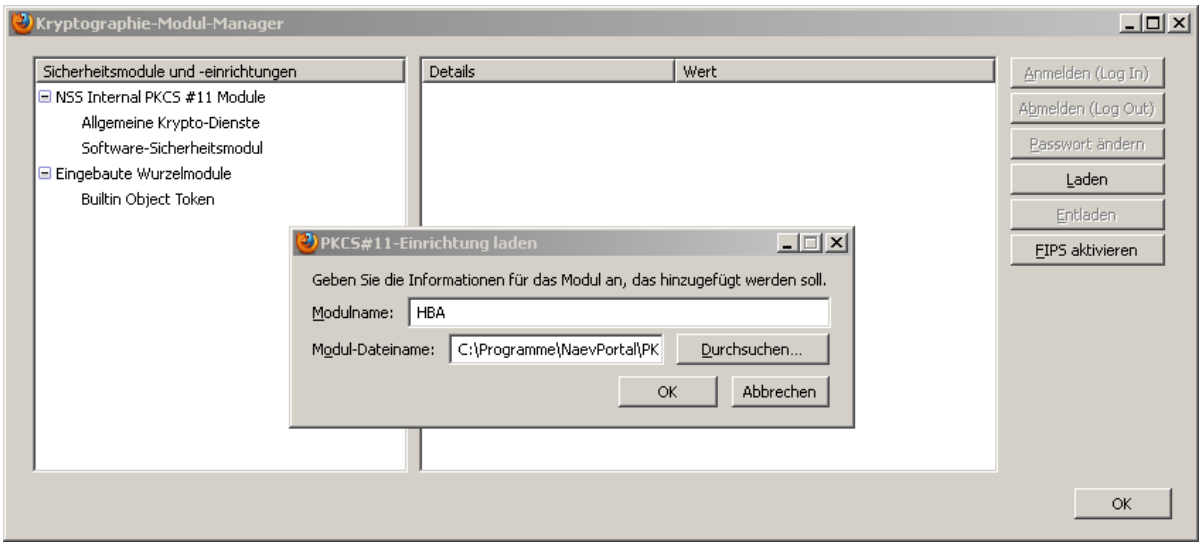
Für diese Installation sind keine speziellen Administrator-Rechte erforderlich. Ganz im Gegenteil: wird ein PC von mehreren Anwendern benutzt und benutzen diese Anwender jeweils ein eigenes Windows-Profil, so muss jeder Anwender die nachfolgenden Einstellungen separat vornehmen, da sie benutzerindividuell gespeichert werden.

Starten sie den Firefox-Browser und wählen sie aus dem "Extra"-Menü den Menüpunkt "Einstellungen". Es erscheint ein Fenster, an dessen oberen Rand einzelne Einstellungsbereiche ausgewählt werden können. Klicken sie hier auf den Bereich "Erweitert". Darauf erscheint im unteren Bereich des Fensters vier übereinanderliegende Karteikarten, deren Reiter mit "Allgemein", "Netzwerk", "Update" und "Verschlüsselung" bezeichnet sind. Durch Klicken auf den Reiter "Verschlüsselung" wird dieser in den Vordergrund gebracht.



Im Bereich Zertifikate wählen Sie bitte "Automatisch eins wählen", dies erspart ihnen bei der späteren Nutzung die permanente Nachfrage, welche Zertifikate benutzt werden sollen.

Treiber für elektronische Arztausweise werden in der Firefox-Notation "Kryptographie-Module" genannt. Durch Betätigen der entsprechenden Schaltfläche erhalten sie folgenden Dialog:



Auf der linken Seite sind die bereits vorhandenen Module zu erkennen. Jeder Firefox Browser erfügt über zwei interne Module mit den Namen "NSS Internal PKCS#11 Module" und "Eingebaute Wurzelmodule". Diese dürfen auf keinen Fall gelöscht werden. Wenn mehr als diese beiden Module existieren, wurden bereits zusätzliche Module installiert. In diesem Fall sollten sie prüfen, ob das gewünschte Modul für ihren CryptoStick oder ihren elektronischen Heilberufsausweis bereits vorhanden ist.

Durch Betätigen der "Laden"-Schaltfläche erscheint ein weiterer Dialog, in dem sie den Namen eines neuen Moduls und den zu verwendenden Dateinamen eingeben können. Benutzen sie hierbei folgende Werte:

- Falls sie einen Arztausweis benutzen wollen:
  - als Modulname: HBA
  - als Modul-Dateiname: `C:\Programme (x86)\NaevPortal\PKCS11_eHBA.dll`
- Falls sie einen CryptoStick Model ePass2003 benutzen wollen:
  - als Modulname: CryptoStick
  - als Modul-Dateiname: `C:\Programme (x86)\NaevPortal\eps2003csp11.dll`

Verwenden sie auf keinen Fall im Eingabefeld für den Modulnamen Umlaute, da Firefox solche Namen nicht anzeigen kann, was dazu führt, dass ein derart installiertes Modul nicht mehr entfernt werden kann.

Mit der "OK"-Schaltfläche wird das Modul installiert und sollte danach als weiteres Modul angezeigt werden.

Ab diesem Moment sollte eine Anmeldung am Portal mit elektronischem Ausweis möglich sein, allerdings kann der verwendete Acrobat-Reader noch keine Dokumente entschlüsseln, bevor nicht der gleiche Treiber, der von Firefox verwendet wird, auch im Acrobat Reader als zu verwendender Treiber eingestellt wird.

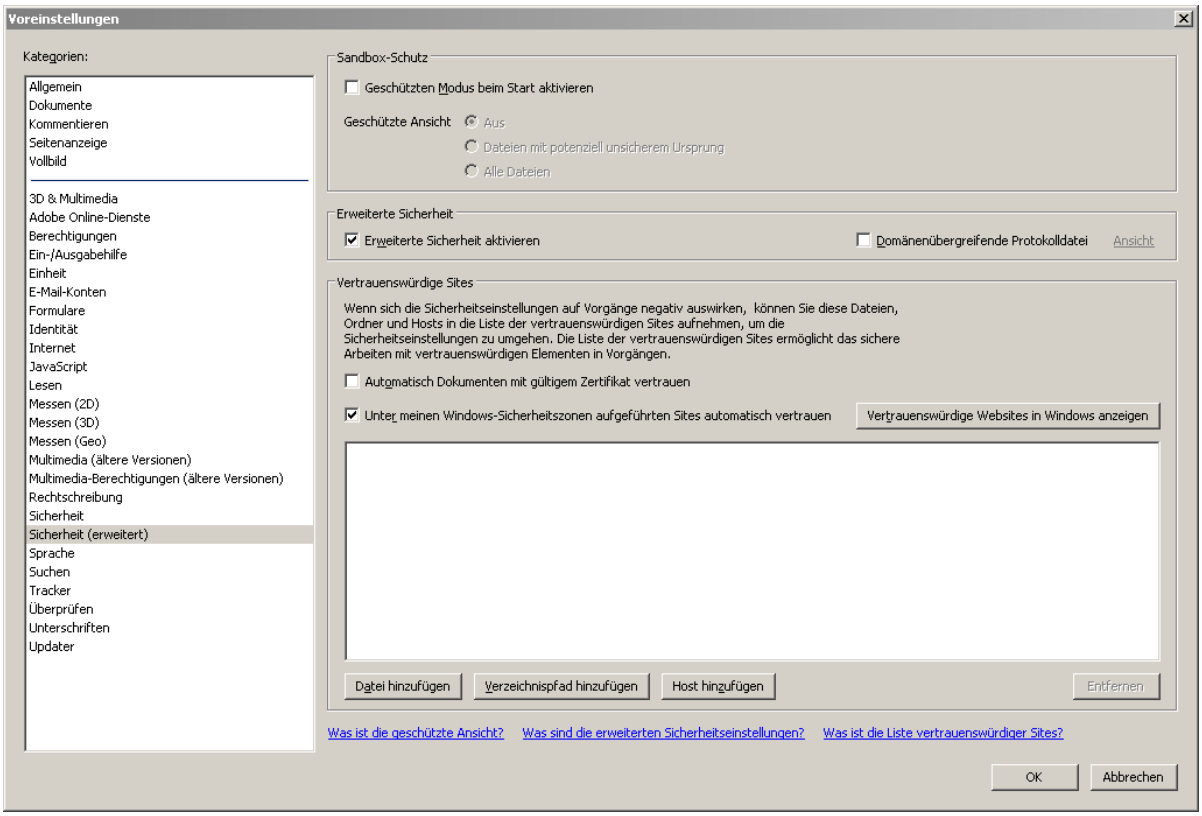
2.3. Treiberinstallation im Acrobat Reader

Der Acrobat Reader benutzt sowohl die Treiber des Betriebssystems als auch eigene Treiber um auf Zertifikate zuzugreifen. Fall sie einen CryptoStick benutzen, sollte der dafür erforderliche Treiber bereits vom Betriebssystem geliefert werden und die Installation zusätzlicher AcrobatReader-Treiber nicht erforderlich sein. In diesem Fall können sie die nachfolgende Anleitung benutzen um zu prüfen, ob ihr CryptoStick korrekt erkannt wird.

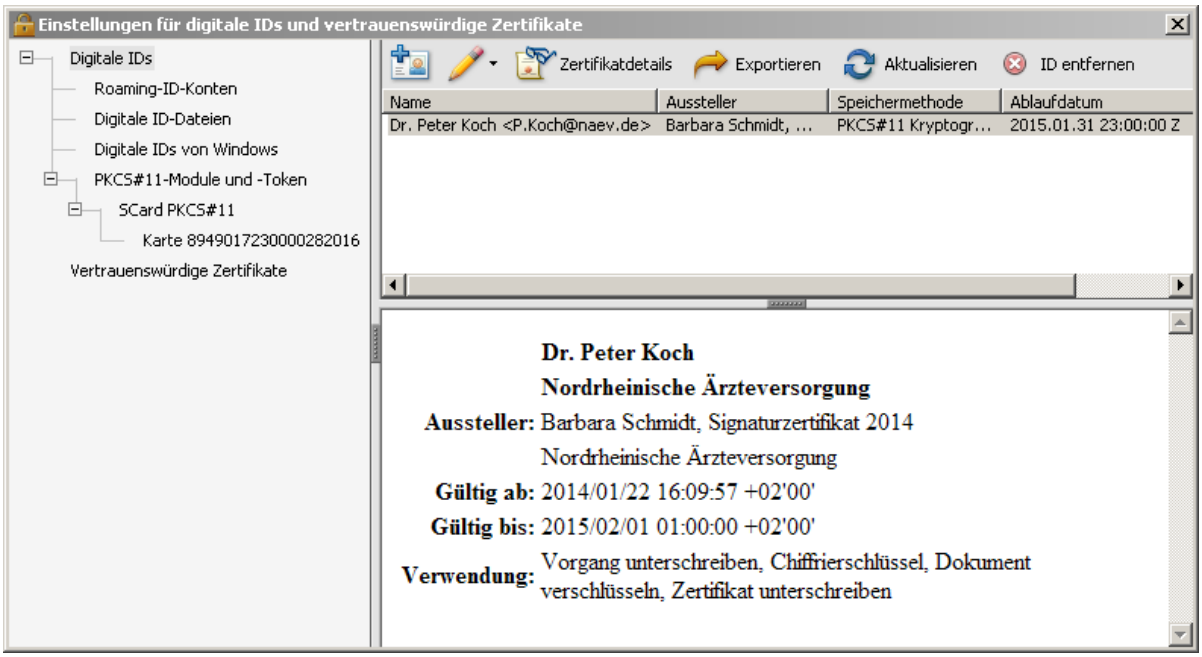
Treiber für einen Heilberufsausweis sind normalerweise nicht im Betriebssystem vorhanden und können deshalb vom AcrobatReader nicht mitbenutzt werden. Falls sie also einen Heilberufsausweis nutzen wollen, ist die Installation separater Treiber erforderlich.

Die nachfolgende Anleitung bezieht sich auf den Acrobat Reader Version XI. Bei Vorgängerversionen sehen die Menüeinstellungen zum Teil völlig anders aus.

Starten sie den Acrobat-Reader XI und wählen sie den Menü-Punkt "Bearbeiten" und innerhalb dieses Menüs den Punkt "Voreinstellungen". Danach erscheint ein zweigeteiltes Fenster, in dessen linker Hälfte sie eine Kategorie auswählen können, zu der dann Einstellungsmöglichkeiten in der rechte Hälfte möglich sind. Wählen sie hier bitte in der linke Hälfte die Kategorie "Sicherheit (erweitert)" und prüfen sie ob in der rechten Hälfte die Option "Geschützten Modus beim Start aktivieren" ausgeschaltet ist. Sollte sie angeschaltet sein, entfernen sie bitte den entsprechenden Haken, beenden dann den Acrobat Reader komplett und starten ihn neu. Ist die Option bereits ausgeschaltet, können sie direkt mit dem nächsten Schritt fortfahren.



Wählen sie nun die Kategorie "Unterschriften" und betätigen sie auf der rechten Seite die Schaltfläche "Weitere..." im Bereich "Identitäten und vertrauenswürdige Zertifikate". Es öffnet sich dann ein Fenster, in dem Zertifikate aufgeführt sind, die vom Acrobat Reader verwendet werden können. Wenn sie (wie in nachfolgendem Screenshot) im linken Bereich "Digitale IDs" auswählen, werden alle zur Verfügung stehende Zertifikate aufgelistet. Bei Auswahl von "Digitale IDs von Windows" nur diejenigen Zertifikate, die vom Betriebssystem erkannt wurden, und bei Auswahl eines PKCS#11-Moduls (so heissen eigene Treiber des Acrobat Readers in dessen Sprachgebrauch) sehen sie nur die Zertifikate, die sich auf den ausgewählten Geräten befinden.



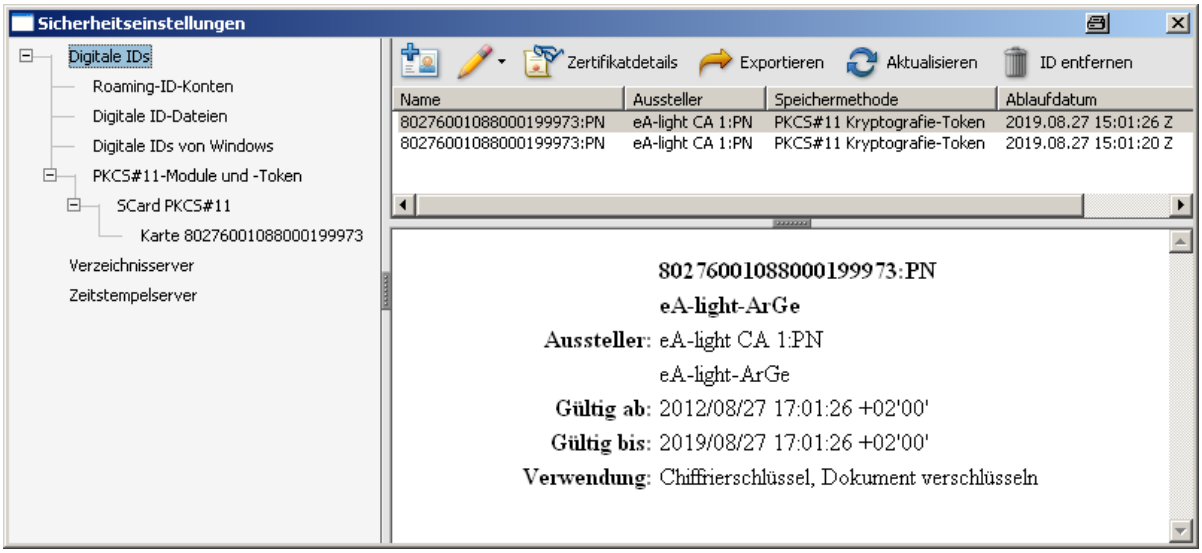
Wenn sie einen CryptoStick verwenden, sollte dieser bereits vom Betriebssystem erkannt werden und ihr Zertifikat deshalb im Bereich "Digitale IDs von Windows" auftauchen. Ist dies nicht der Fall, können sie wie nachfolgend beschreiben einen separaten Acrobat-Reader-Treiber für ihren CryptoStick installieren. Die bessere Alternative ist in diesem Fall allerdings die EDV-Abteilung der Nordrheinischen Ärzteversorgung zu kontaktieren, damit ihr Betriebssystem entsprechend ergänzt wird. In einem nach-

folgenden Kapitel ist beschrieben, wie sie prüfen können ob und welche CryptoStick-Treiberversion in ihrem Betriebssystem enthalten ist.

Falls sie einen Heilberufsausweis verwenden wollen und ihr Zertifikat nicht angezeigt wird, so wählen sie im links angezeigten Inhaltsverzeichnis den Eintrag "PKCS#11-Module und Token". Danach benutzen sie die Schaltfläche "Modul anhängen" am oberen Fensterrand. Daraufhin erscheint ein Auswahldialog ihres Betriebssystems, mit dem sie die gleiche Treiberdatei auswählen müssen, die sie auch bei der Installation des Firefox Kryptographie-Moduls verwendet haben, also:

- `C:\Programme (x86)\NaevPortal\PKCS11_eHBA.dll` (bei Heilberufsausweisen)
- `C:\Programme (x86)\NaevPortal\eps2003csp11.dll` (bei CryptoSticks Model ePass2003)

Acrobat nennt ihren elektronisches Ausweis "Digitale ID" und wenn sie nach erfolgreicher Installation im Inhaltsverzechnis den Eintrag "Digitale IDs" auswählen, dann sollten sie in etwas folgende Ansicht erhalten:



Beachten sie, dass ein Arztausweis Light kein "richtiges" Zertifikat enthält sondern lediglich zwei Zertifikate, die für eine anonyme Nummer ausgestellt wurden. Genau diese Nummer wird ihnen als Inhaber der Digitalen ID angezeigt. "Richtige" Arztausweise und auch alle elektronischen Ausweise, die von der EDV-Abteilung der Nordrheinischen Ärzteversorgung ausgestellt wurden, enthalten als Inhaberangabe jeweils den vollständigen Namen des Besitzers. Für die Funktion des DMS-Portals der Nordrheinischen Ärzteversorgung ist der fehlende Name in Arztausweisen Light allerdings ohne Bedeutung.

Kapitel 3. Administration

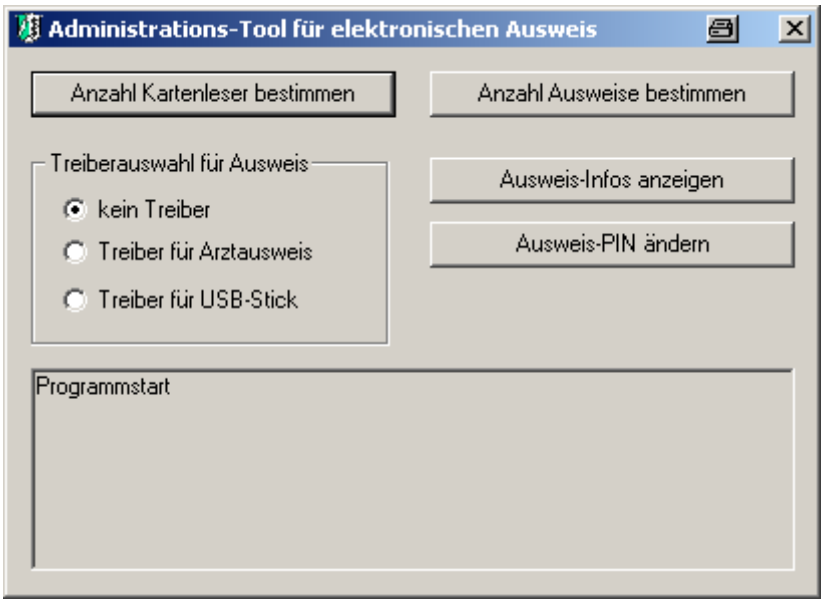
Wenn ihr elektronischer Ausweis nicht korrekt funktioniert, kann das mehrere Gründe haben:

- Ihr Betriebssystem kann nicht mit dem Ausweis kommunizieren, weil kein korrekter Treiber für ihren Kartenleser (bzw. den verwendeten USB-Stick) vorhanden ist.
- Firefox verfügt nicht über einen passenden Treiber für ihren Ausweis.
- Acrobat-Reader verfügt nicht über einen passenden Treiber für ihren Ausweis.

Auf einem PC kann die Funktionsweise sowohl des Treibers für den Kartenleser als auch des Treibers für den elektronischen Ausweis wie folgt überprüft werden:

3.1. Überprüfen des Karten-Lesers

Zur Überprüfung des Kartenlesers starten sie das Administrationsprogramm `Admin.exe`. Es befindet sich im Verzeichnis `C:\Programme (x86)\NaevPortal` und sollte sich mit folgender Ansicht melden:



Mit den oberen beiden Schaltflächen können sie überprüfen, ob ihr PC mit ihrem elektronischen Ausweis kommunizieren kann. Wenn dies nicht der Fall ist erübrigt sich jede weitere Fehlersuche, da die gesamte restliche Funktionalität (Anmeldung mit Firefox bzw. Entschlüsselung mit Acrobat Reader) dann nicht funktionieren kann.

Eine sehr sichere Mtheode um herauszufinden, ob ihr Ausweis vom PC aus ausgelesen werden kann, ist die Anzeige der vorhandenen Karten jeweils mit gesteckter und mit nicht gesteckter Karte. Mit gesteckter Karte sollte genau eine Karte mehr angezeigt werden als ohne.

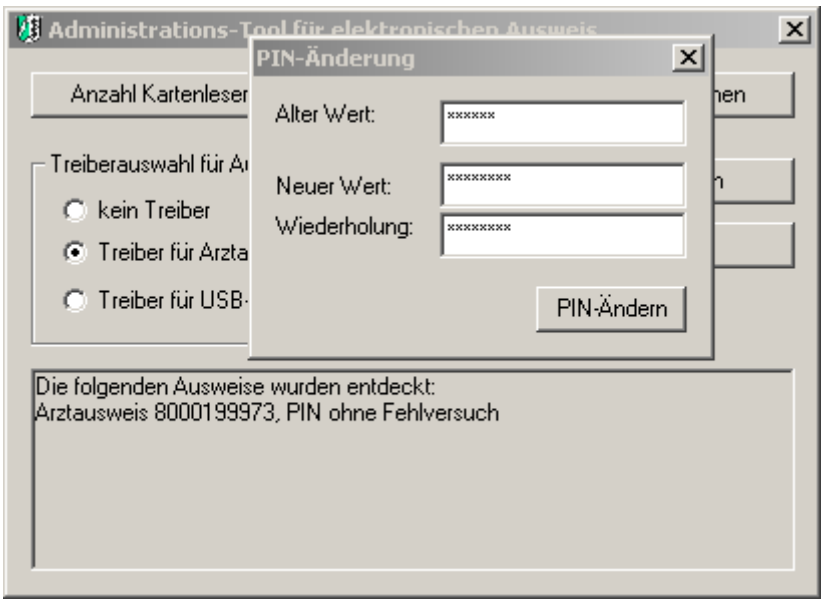
3.2. Ändern der PIN

Bevor sie die PIN ihres elektronischen Ausweises ändern sollten sie überprüfen, in welchem Zustand sich ihr Ausweis befindet. Hierzu benutzen sie die Schaltfläche "Ausweis-Infos anzeigen". Dadurch erhalten sie Informationen über die Seriennummer ihres Ausweises und zum Zustand ihrer PIN.

Je nach verwendetem elektronischen Ausweis haben sie 3 oder mehr Versuche eine gültige PIN einzugenen. Dnach wird ihr elektronischer Ausweis gesperrt und kann eventuell unter Verwendung einer PUK wieder entsperrt werden. Das Administrationsprogramm zeigt ihnen an, ob sie bereits einen Fehlversuch unternommen haben, ob nur noch genau ein Versuch möglich ist und ob der Ausweis bereits gesperrt ist. Wenn die letzte PIN-Eingabe erfolgreich war, lautet die Meldung "PIN ohne Fehlversuch".

Das Adminstrationsprogramm bietet keine Möglichkeit eine gesperrte PIN mittels PUK zu entsperren. Sollte dies erforderlich sein, wenden sie sich bitte an die EDV-Abteilung der Nordrheinischen Ärzteversorgung.

Falls sie sich mittels der Schaltfläche "Ausweis-Infos anzeigen" über den Zustand ihrer PIN informiert haben, können sie mittels "Ausweis PIN ändern", die PIN ändern.



Beachten sie, dass für einige elektronische Ausweise Mindest- und Höchstlängen für die PIN gelten:

- erlaubte Längen beim Arztausweis: 4 bis 12 Ziffern.
- erlaubte Längen beim Ausweis in USB-Stick Format: 8 bis 32 Ziffern.

Die Bedienung der Maske zur PIN-Änderung ist selbsterklärend. Nach erfolgreicher Änderung erhalten sie eine entsprechende Meldung. Falls die Änderung fehlschlägt, achten sie bitte auf die Fehlermeldung "INVALID" PIN bedeutet, dass die alte oder neue PIN ein ungültiges Format hatte, z.B. zu wenige oder zu viele Ziffern. "INCORRECT" PIN dagegen bedeuet, dass die alte PIN falsch eingegeben wurde.

Beachten sie dass nach mehrfach falschen Eingaben ihrer alten PIN ihr elektronischer Ausweis dauerhaft gespert wird und ggf. ersetzt werden muss. Wenn sie sich also sicher sind, eine korrekte alte PIN eingegeben zu haben und die Änderung trotzdem nicht funktioniert, wiederholen sie bitte nicht den Vorgang ohne die Ursache des Fehlers zu klären.