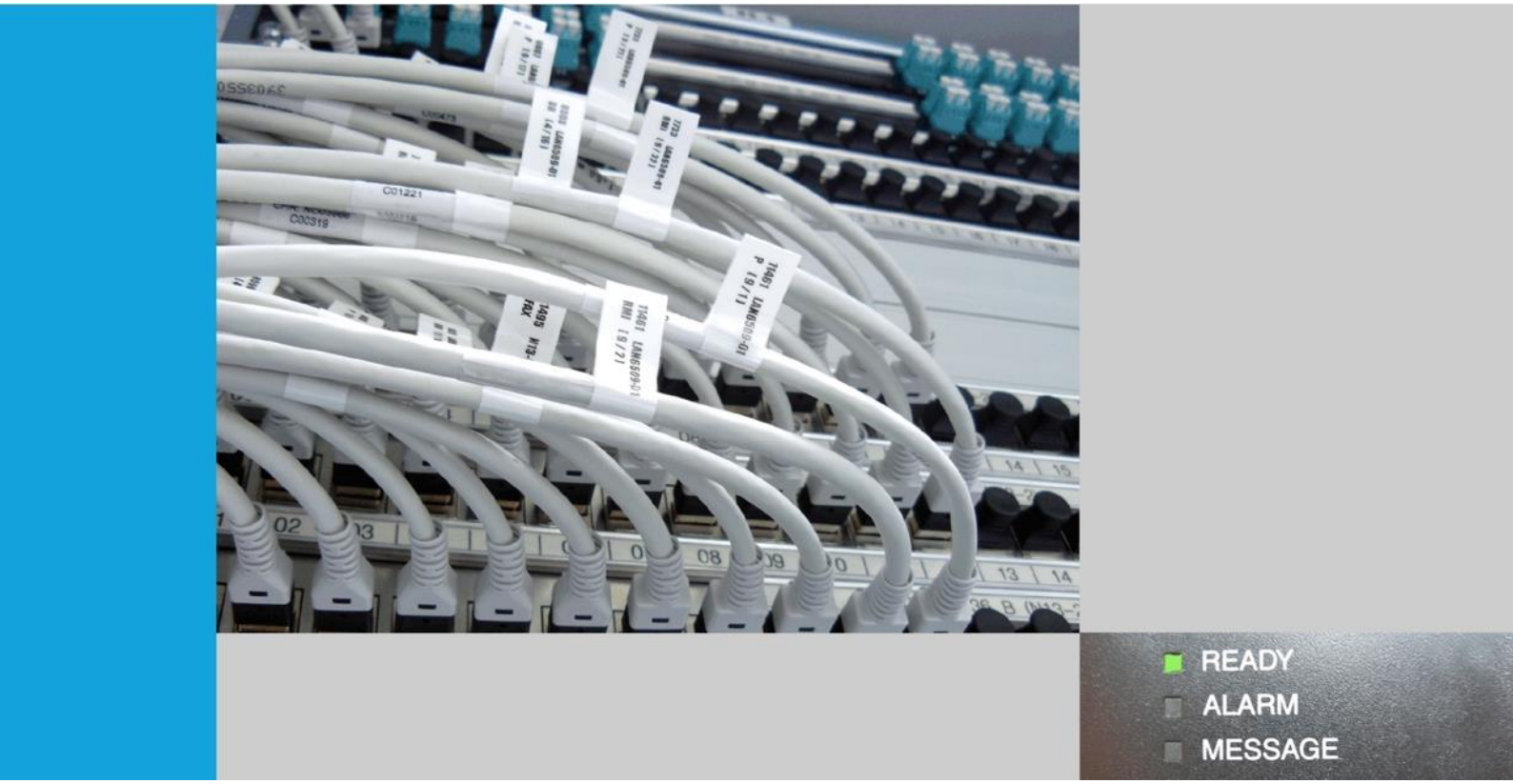
Landesamt für Digitalisierung,
Breitband und Vermessung

IT-Dienstleistungszentrum des Freistaats Bayern



Schulung für Registrierungsstellen der Bayern-PKI

- Arbeit mit dem Zertifikatsverwaltungssystem -

München, den 04.07.2019

1 Allgemein

1.1 Voraussetzung

Damit die Teilnehmer der Bayern-PKI das Zertifikatsverwaltungssystem nutzen können, müssen einige Bedingungen erfüllt sein:

Ausstattung	RA	RA mit Smartcard-produktion	Anwender	Anwender mit Autoenroll-ment	Anwender mit Smartcard
PC (Windows)		X		X	
PC (Windows oder Linux)	X		X		X
Java JRE/JDK 1.8	X	X	X	X	X
Drucker	X	X			
PDF Reader	X	X			
Nexus Card SDK*		X			
Kartenlesegerät**		X			X
Middleware***		X			X

* Die Software „Nexus Card SDK“ inklusive Installationsanleitung kann von unserer Webseite https://www.pki.bayern.de (Bayern-PKI → Registrierungsstellen → Downloads) heruntergeladen werden. Hier finden Sie auch aktuelle Informationen.

** Als Kartenlesegerät kommt z.B. ein Cherry ST-2000U in Frage.

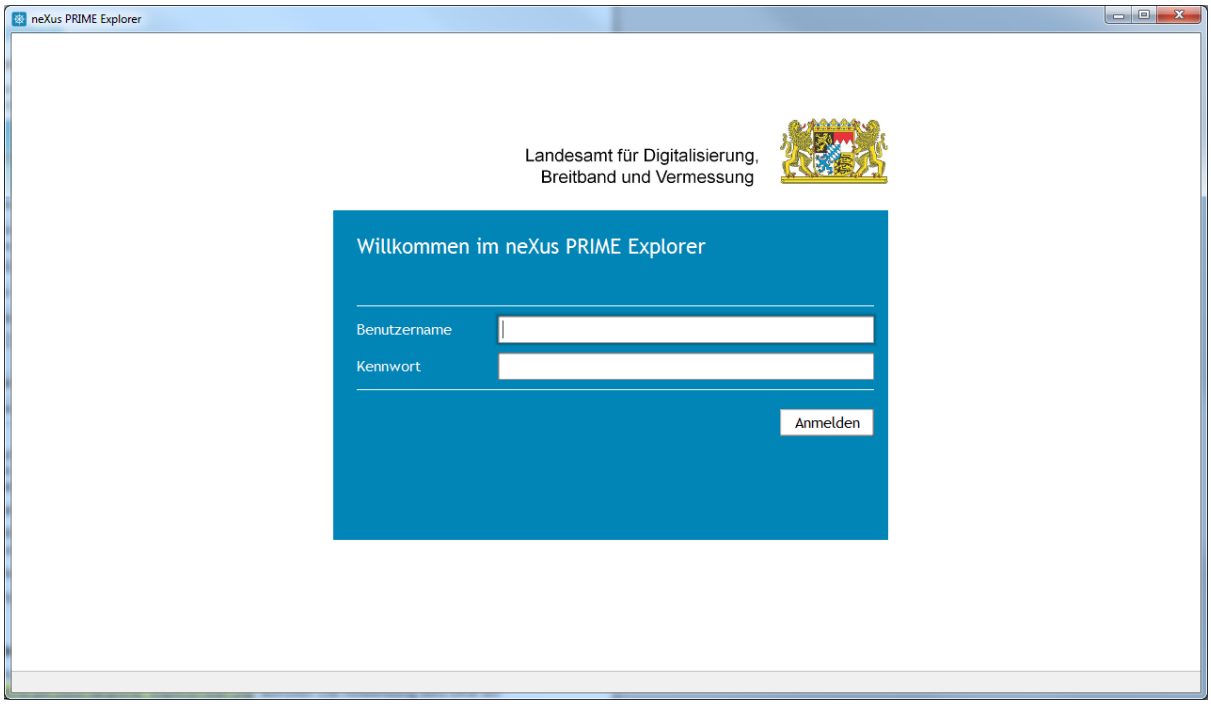
*** Die Middleware funktioniert als Softwarekommunikation zwischen dem Betriebssystem des PC und dem Kartenlesegerät. Zur Verfügung stehen:

- Charismatics smart security interface
- Cryptovision cv act sc/interface

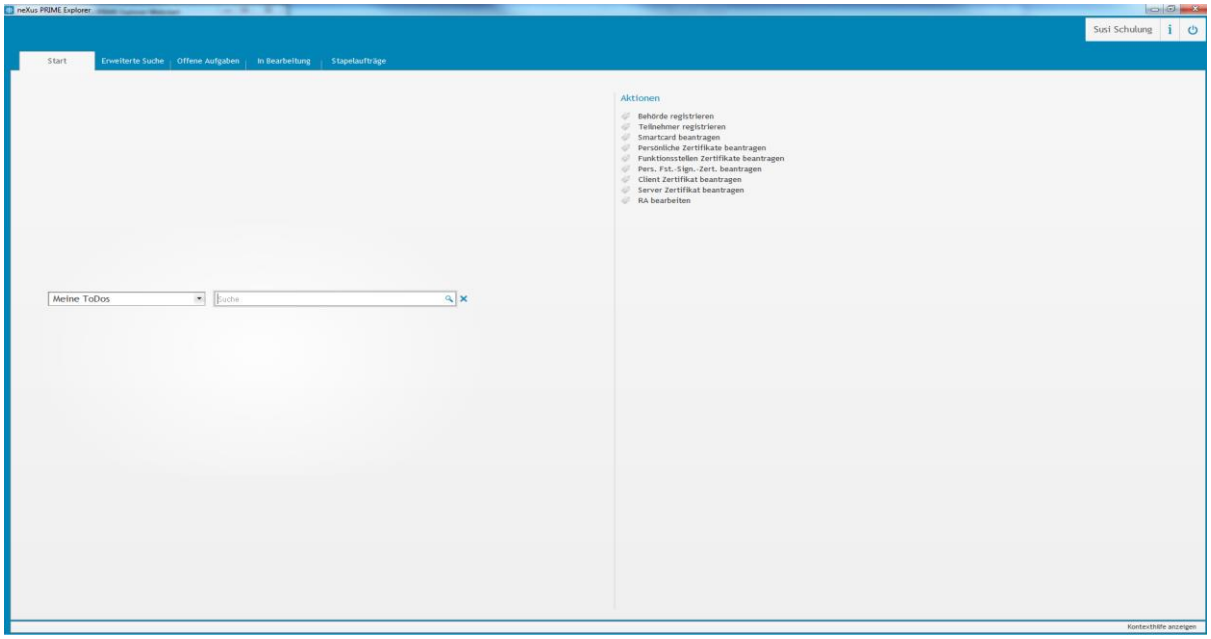
1.2 Übersicht

Nexus Prime ist eine Java Web Start Anwendung, die Sie über die URL https://prime.pki.bybn.de/prime_explorer/start.jnlp aufrufen. Die Anwendung wird lokal auf Ihrem PC ausgeführt, wobei einzelne Teile im Hintergrund serverseitig ablaufen.

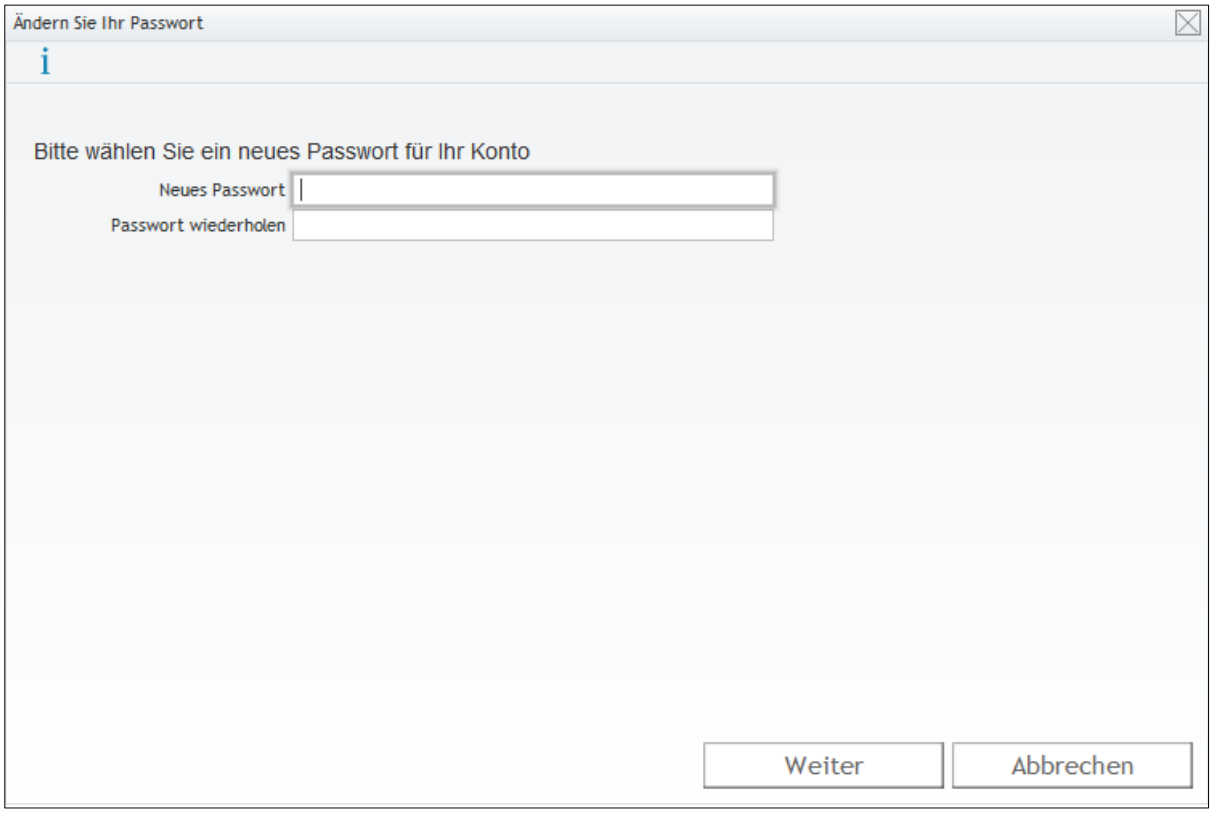
Nach dem Laden der Anwendung begrüßt Sie folgender Startbildschirm:

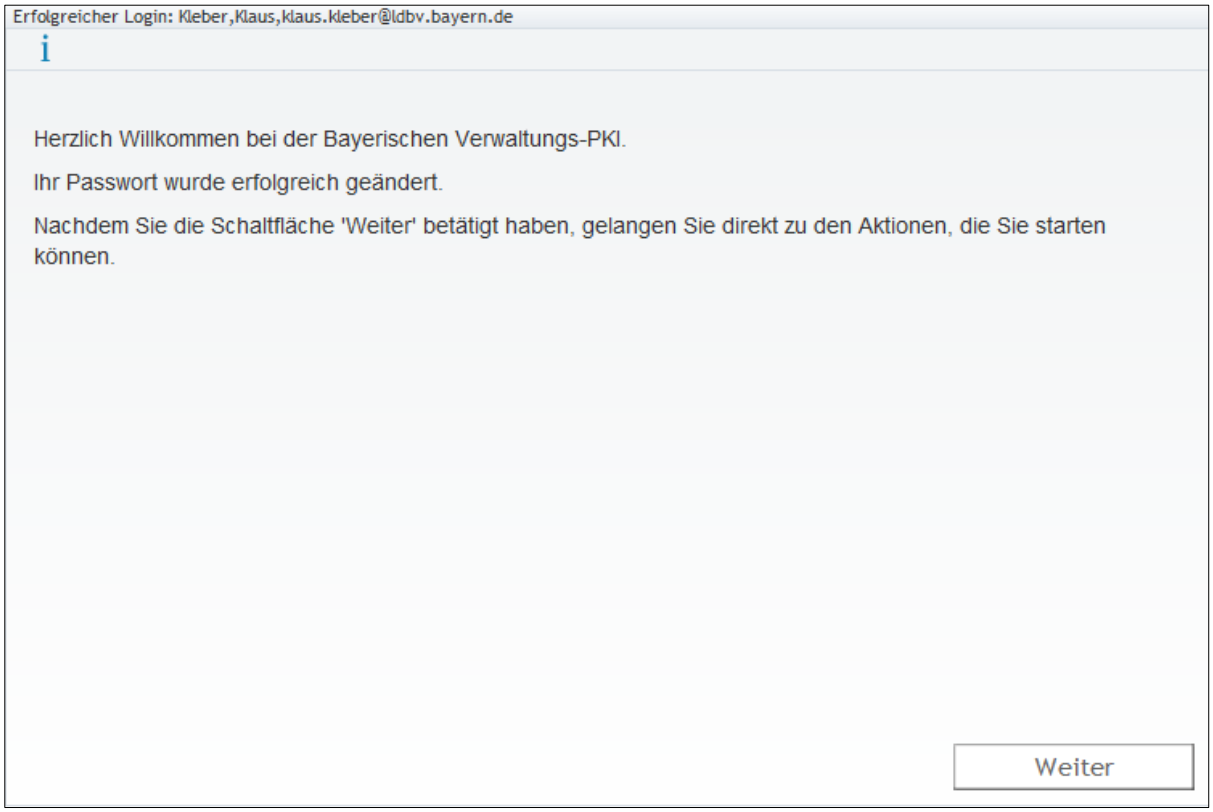


Melden Sie sich bitte mit Ihrem Benutzernamen (entspricht der E-Mail Adresse) sowie Ihrem Passwort an. Anschließend bekommen Sie die nachfolgende Seite angezeigt.



Falls Sie sich zum ersten Mal mit Ihrer Kennung an Prime anmelden, oder gerade Ihr Passwort zurückgesetzt haben, müssen Sie Ihr initiales Passwort ändern.


Ändern Sie Ihr Passwort
Bitte wählen Sie ein neues Passwort für Ihr Konto
Neues Passwort
Passwort wiederholen
Weiter
Abbrechen

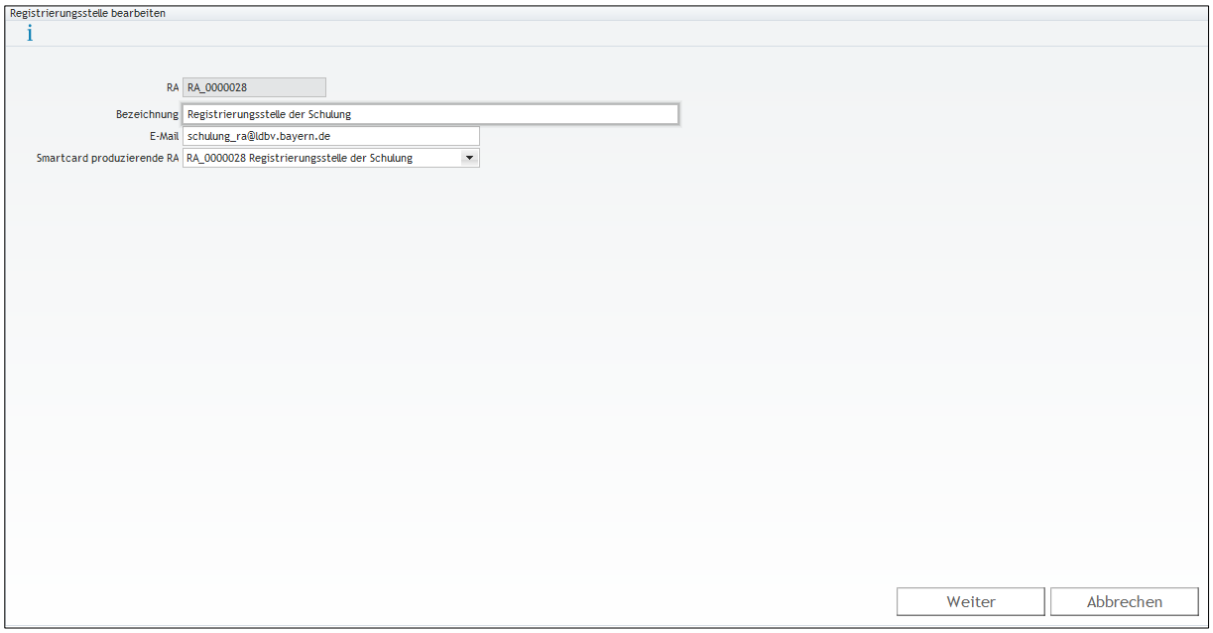

Erfolgreicher Login: Kleber,Klaus,klaus.kleber@ldbv.bayern.de
Herzlich Willkommen bei der Bayerischen Verwaltungs-PKI.
Ihr Passwort wurde erfolgreich geändert.
Nachdem Sie die Schaltfläche 'Weiter' betätigt haben, gelangen Sie direkt zu den Aktionen, die Sie starten können.
Weiter

2 Aufgaben und Tätigkeiten einer Registrierungsstelle

2.1 Ansehen und Ändern der Registrierungsstellendaten

Sie können jederzeit die eingetragenen Informationen zu Ihrer Registrierungsstelle ansehen und ggfs. anpassen. Insbesondere ist es wichtig, dass Sie die E-Mail Adresse aktuell halten, damit wir Ihnen jederzeit wichtige Informationen zukommen lassen können.

Rufen Sie dazu in der **Prime Startseite** die **Aktion „RA bearbeiten“** auf.



Das Feld „Smartcard produzierende RA“ wird im Regelfall auf Ihre eigene Registrierungsstelle eingestellt sein. Was dieses Feld zu bedeuten hat wird im Kapitel 5.2.1.2 erläutert.

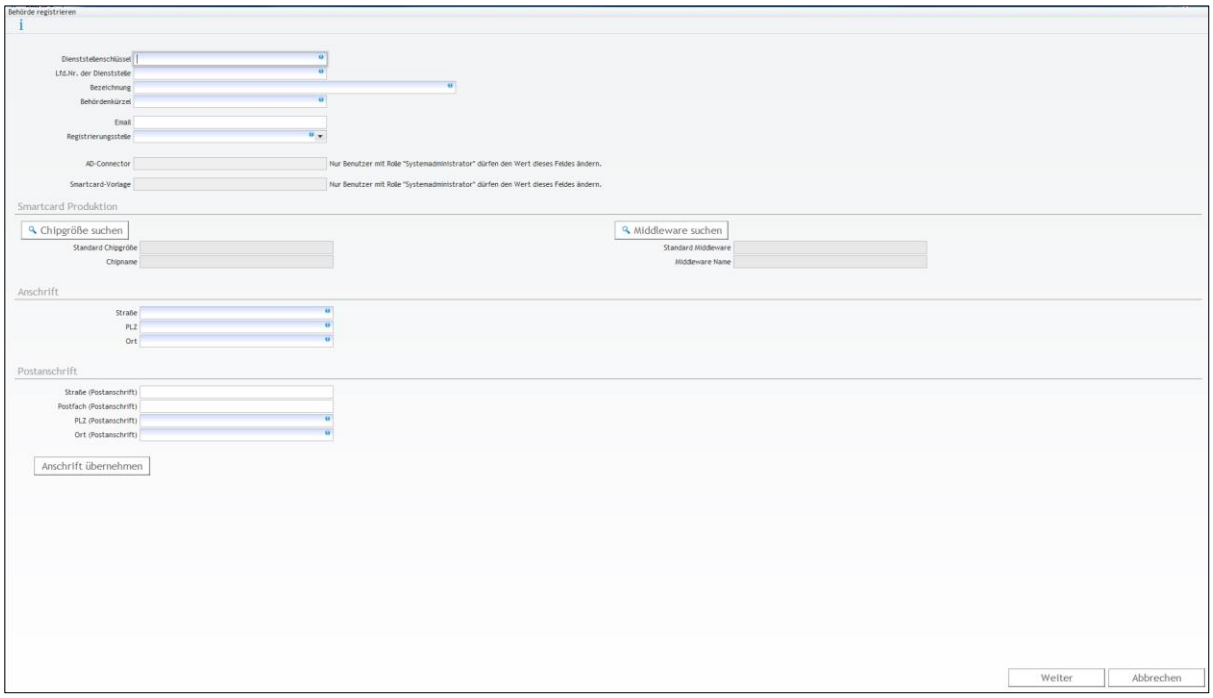
2.2 Einrichten und Pflegen betreuter Behörden

2.2.1 Einrichten einer weiteren Behörde

Eine Behörde kann nur neu angelegt werden, wenn sie einer bereits registrierten Registrierungsstelle zugewiesen wird. Die Behörde kann nur der eigenen Registrierungsstelle zugewiesen werden.

Behörden müssen eindeutig sein, überprüft wird die Kombination aus Dienststellenschlüssel. und Lfd-Nr. der Dienststelle.

Zum Anlegen einer weiteren Behörde rufen Sie in der **Prime Startseite** die **Aktion „Behörde registrieren“** auf.



Hinweis: blau hinterlegte Felder sind Pflichtfelder

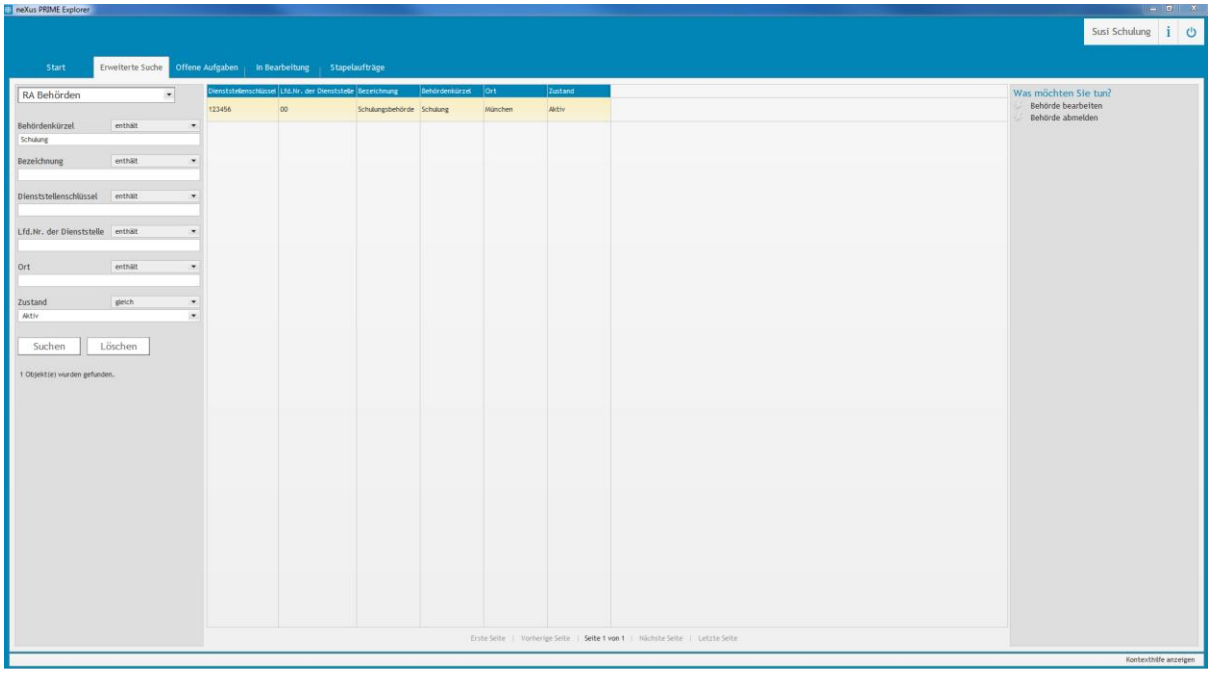
Falls Ihnen die Werte für Dienststellenschlüssel und Lfd.Nr. der Dienststelle nicht bekannt sind, können Sie im Behördennetz (www.bybn.de) das Behörden- und Dienststellenverzeichnis abfragen. Sollten sie eine Dienststelle anlegen wollen, für die es keinen Dienststellenschlüssel gibt, setzen Sie sich bitte mit der Wurzel Registrierungsstelle im IT-DLZ in Verbindung. Diese vergibt dann eine eindeutige Nummer.

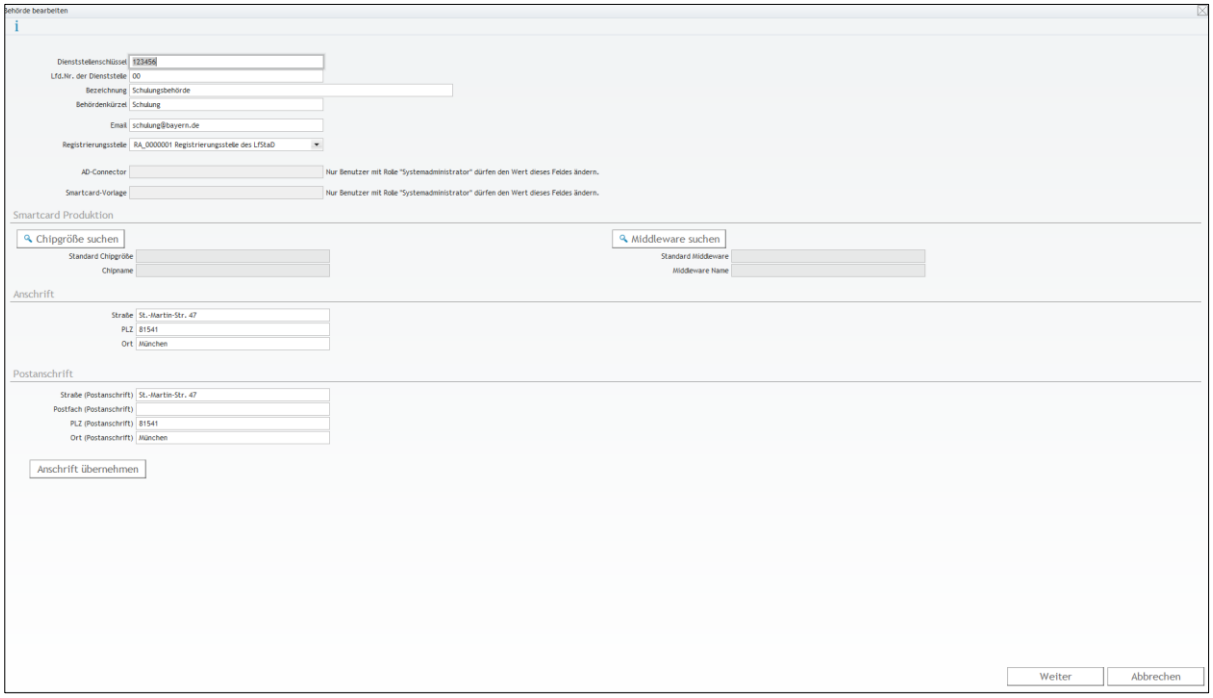
Die Felder „Standard Chip-Größe“ und „Standard Middleware“ sind nur in Verbindung mit Smartcards relevant und werden im Kapitel 5.2.1.3 erläutert.

2.2.2 Pflege der Daten betreuter Behörden

Für eine bereits registrierte Behörde können nachträglich die Daten bearbeitet werden. Suchen Sie dazu zuerst über den Menüpunkt **„Erweiterte Suche“** mit der **Abfrage „RA Behörden“** die zu bearbeitende Behörde.

Markieren Sie die zu bearbeitende Behörde in der Auswahlliste. Im Feld rechts unter „Was möchten Sie tun?“, können Sie auf „**Behörde bearbeiten**“ klicken.





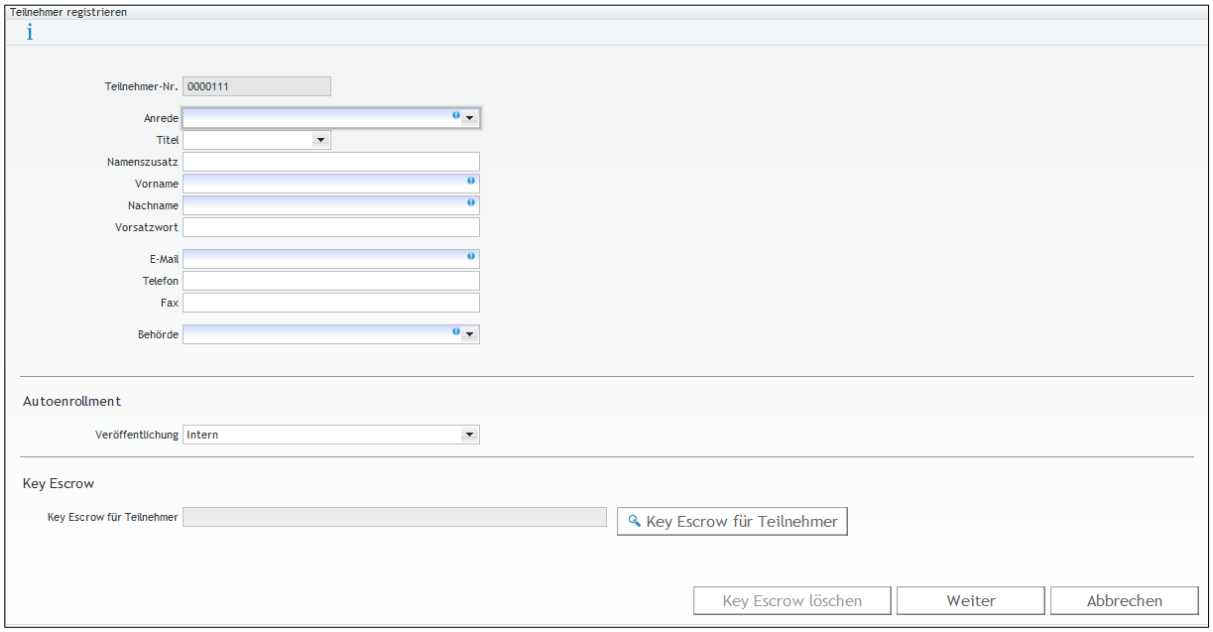
Hinweis: Wenn Sie das Behördenkürzel ändern, werden alle Zertifikate, die sich auf Teilnehmer, Funktionsstellen, Server oder Clients dieser Behörde beziehen, gesperrt und müssen anschließend neu beantragt werden!

2.3 Einrichten und Pflegen von neuen Teilnehmern

2.3.1 Einrichten eines neuen Teilnehmers

Jeder Mitarbeiter, der an der PKI teilnehmen möchte, muss zunächst über eine Registrierungsstelle, die bei seiner Behörde eingerichtet ist, registriert werden. Zur Teilnehmer-Registrierung wird ein neuer Benutzer im System angelegt. Abhängig von der gewählten RA-Funktion bekommt der Benutzer unterschiedliche Berechtigungen im System und somit andere Menüpunkte angezeigt.

Aktion: Teilnehmer registrieren



Hinweis: blau hinterlegte Felder sind Pflichtfelder

1. Persönliche Daten eingeben (Anrede, Name, Telefon, …)

   An die angegebene E-Mail-Adresse werden später die beantragten Zertifikate zugesandt. Gleichzeitig dient die E-Mail Adresse als Benutzername auch zur Anmeldung am System. Bitte beachten Sie die Groß- und Kleinschreibung der E-Mail Adresse und erfassen Sie sie so, wie sie in Ihrem E-Mail System eingetragen ist.

2. Behörde

   In dem Auswahlfenster sehen Sie alle Behörden aufgelistet, die Ihrer Registrierungsstelle zugeordnet sind. Sie finden dabei pro Behörde die drei Informationen Behördenbezeichnung, Dienststellenschlüssel und laufende Nummer der Dienststelle. Wählen Sie die Behörde aus, in der der zu registrierende Teilnehmer arbeitet.

3. Autoenrollment

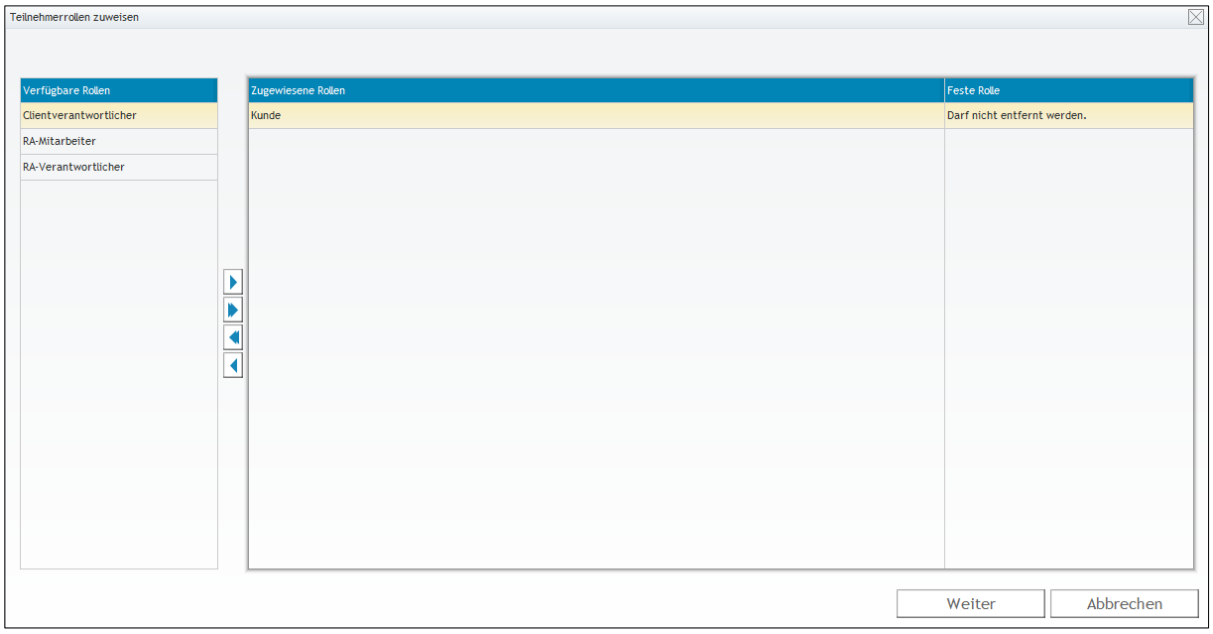
   Autoenrollment ist eine Microsoft Technologie, die es Windows Clients ermöglicht, unter bestimmten Voraussetzungen, automatisiert, d.h. ohne Zutun des Anwenders, Zertifikate zu beziehen. In diesem Fall kann der Teilnehmer für das Verschlüsselungszertifikat die gewünschte Zertifikatsveröffentlichung nicht während der Zertifikatsbeantragung auswählen. Stattdessen greift die hier gewählte Einstellung. **Intern** bedeutet dabei eine Zertifikatsveröffentlichung im Behördennetz. **Intern + Extern** bedeutet eine Veröffentlichung im Behördennetz und im Internet.

4. Key Escrow

Bei der Registrierung eines Teilnehmers wird dieser Abschnitt in der Regel nicht benötigt. Eine Beschreibung für Key Escrow finden Sie im Kapitel 4.1.

5. → Weiter

   Weisen Sie dem Teilnehmer die notwendigen Berechtigungen im System zu. In den meisten Fällen ist die Rolle „Kunde“ ausreichend.



6. → Weiter

   Ein Benutzer mit der entsprechenden Funktion wird im System angelegt. Ein Registrierungsbrief mit den neuen Login-Daten wird an Ihrem Standarddrucker ausgedruckt und muss von Ihnen an den Teilnehmer weitergeleitet werden. Dieser kann sich nun am System anmelden und die benötigten Zertifikate beantragen.

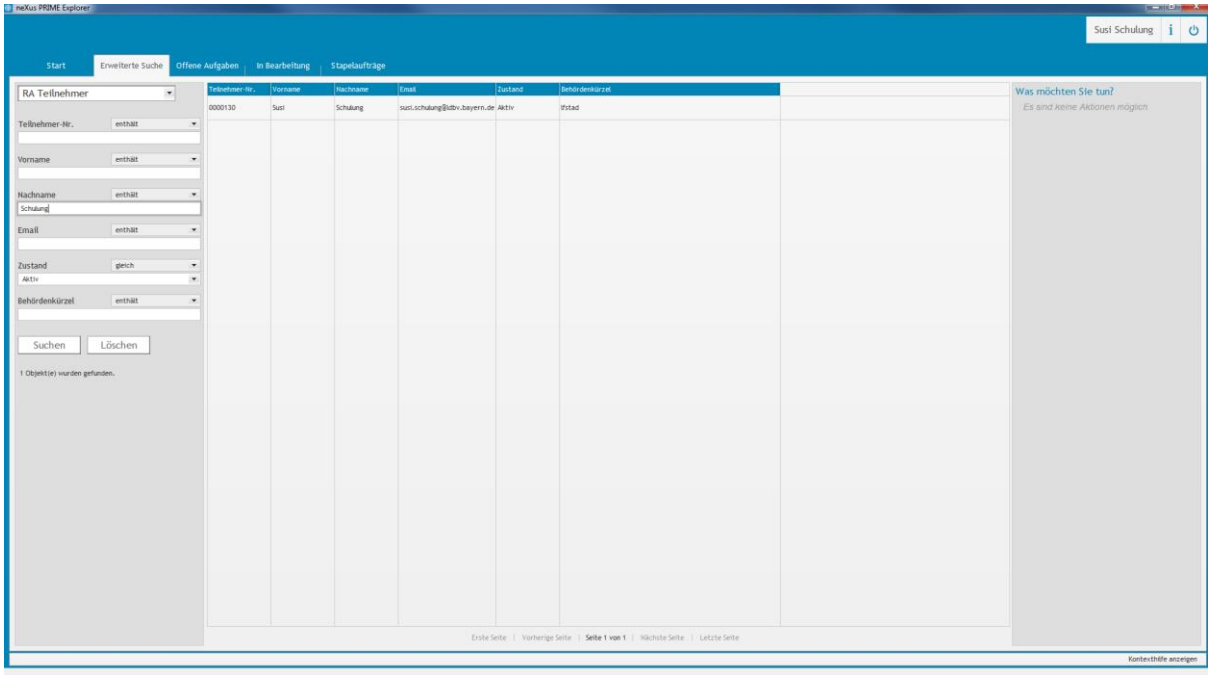
Bei der ersten Anmeldung muss der Benutzer ein neues, nur ihm bekanntes, Passwort eingeben. Damit wird das alte, bei der Registrierung automatisch erstellte und zugewiesene, Passwort überschrieben.

Hinweis: Wir bieten auch die Möglichkeit mehrere Teilnehmer auf einmal im Zuge eines „Massenimports“ zu registrieren. Beachten Sie dazu das Kapitel 6.1.

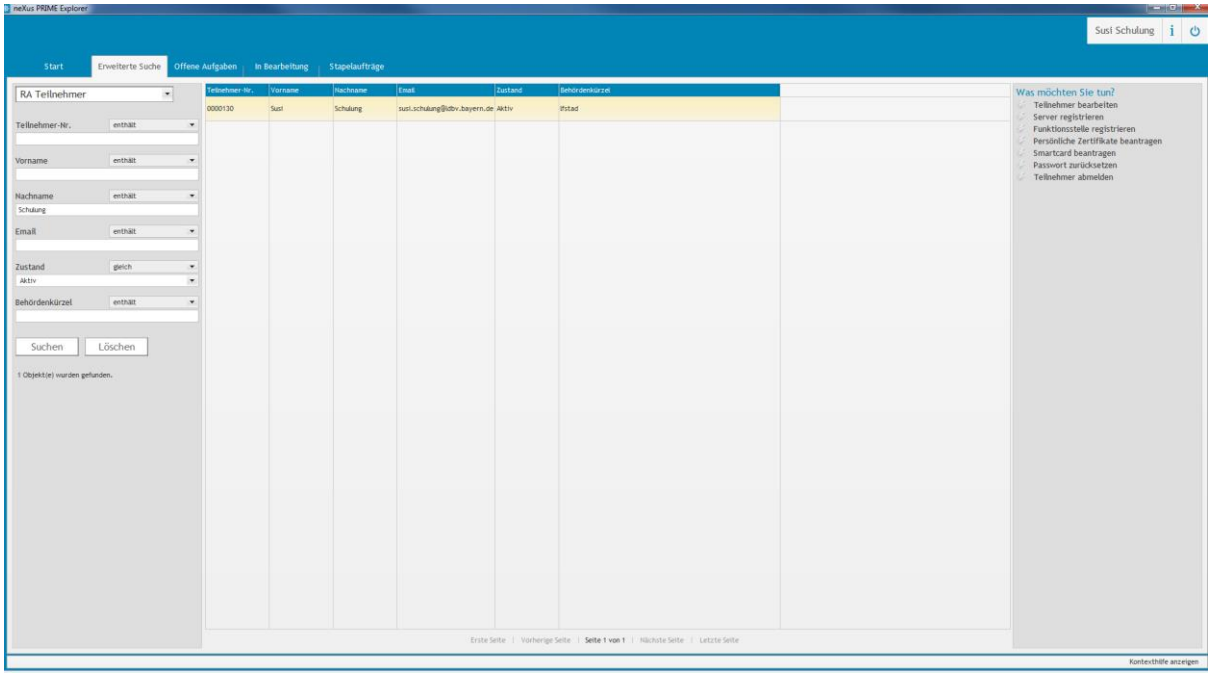
2.3.2 Pflege der Daten eines Teilnehmers

Bei Änderungen der Teilnehmerdaten (z.B. Namensänderung) muss sich der Teilnehmer an seine zuständige Registrierungsstelle wenden. Falls sich Daten ändern, die auch im Zertifikat enthalten sind, werden dabei die gültigen Zertifikate des Teilnehmers gesperrt.

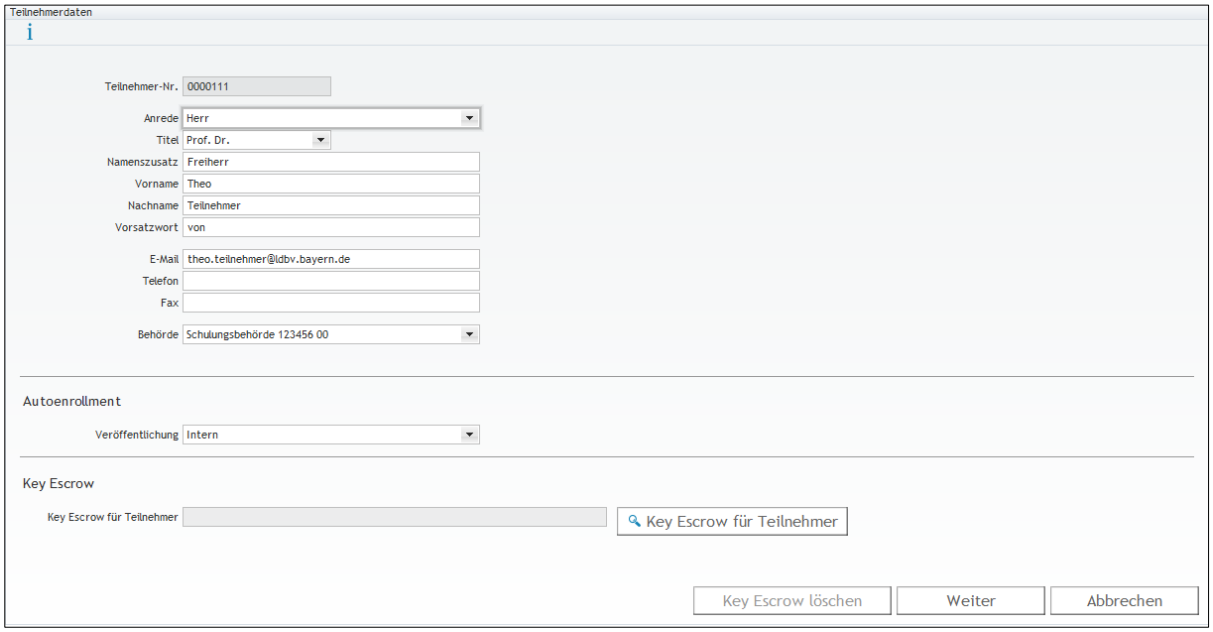
Suchen Sie zuerst über den **Menüpunkt „Erweiterte Suche“** mit der **Abfrage „RA Teilnehmer“** den zu bearbeitenden Teilnehmer.



Markieren Sie den zu bearbeitenden Teilnehmer in der Auswahlliste. Anschließend werden Ihnen die möglichen Aktionen für diesen Teilnehmer eingeblendet.

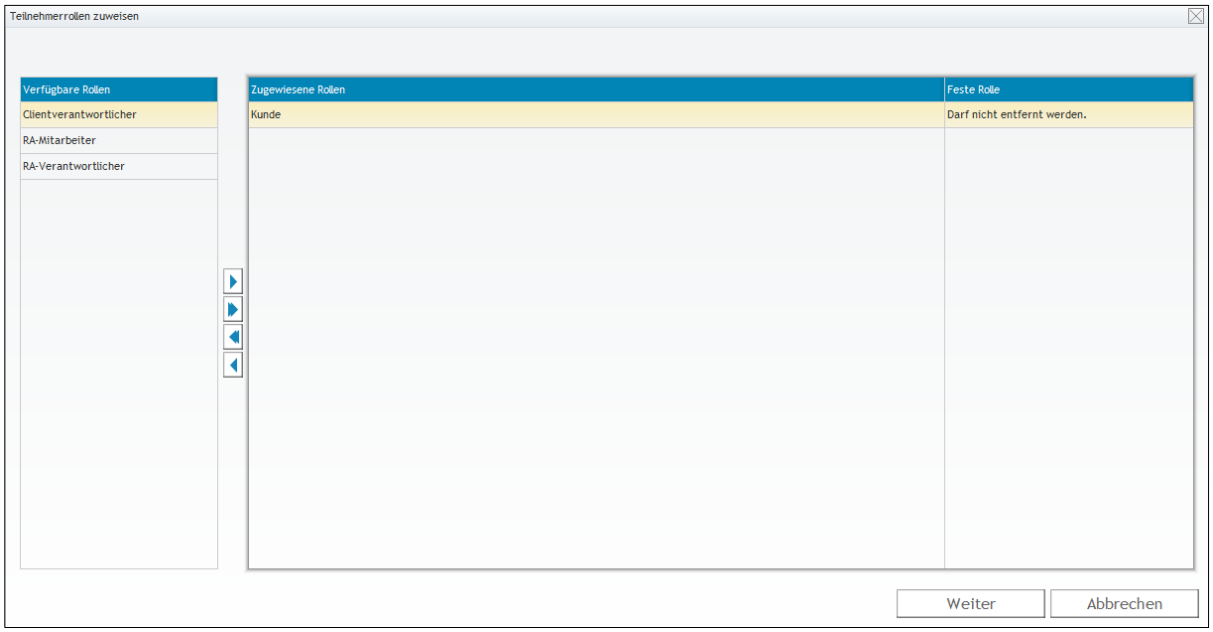


Klicken Sie auf **„Teilnehmer bearbeiten“** unter „Was möchten Sie tun?“.



Hinweis: Ändert sich die E-Mail Adresse, ändert sich damit auch die Anmeldekennung.

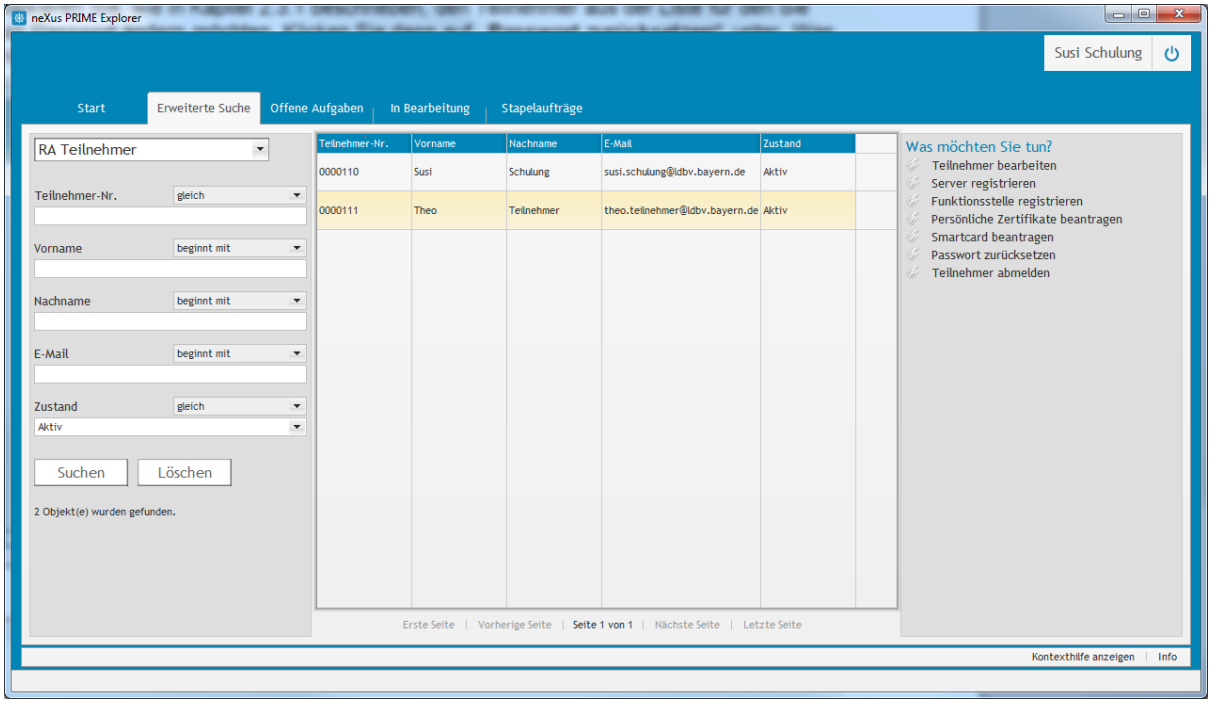
Nach dem Drücken auf die Schaltfläche **„Weiter“**, haben Sie noch die Möglichkeit die Berechtigung des Teilnehmers anzupassen.

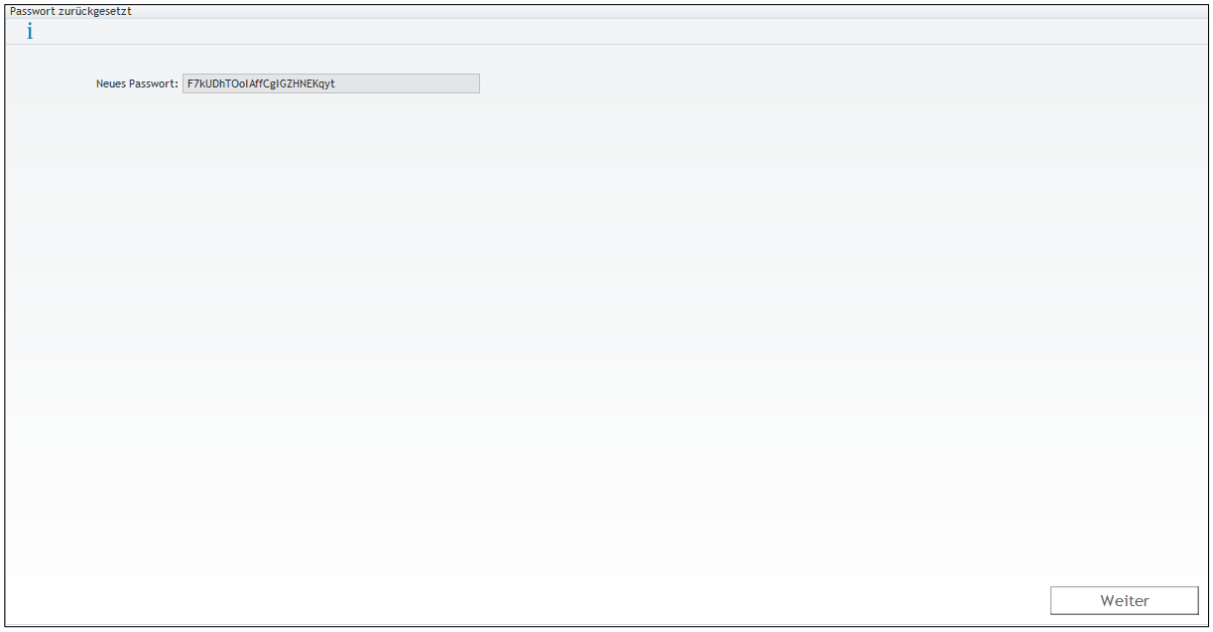


Hinweis: Die Berechtigungen in Prime werden während der Anmeldung ermittelt und zwischengespeichert und bleiben während der gesamten Sitzung erhalten. Änderungen an der Rollenzuordnung (Berechtigung) wirken sich somit erst nach der nächsten Anmeldung an Prime aus.

2.3.3 Zurücksetzen eines Kontopasswortes

Markieren Sie, wie in Kapitel 2.3.1 beschrieben, den Teilnehmer aus der Liste für den Sie das Passwort ändern möchten. Klicken Sie dann auf **„Passwort zurücksetzen“** unter „Was möchten Sie tun?“.



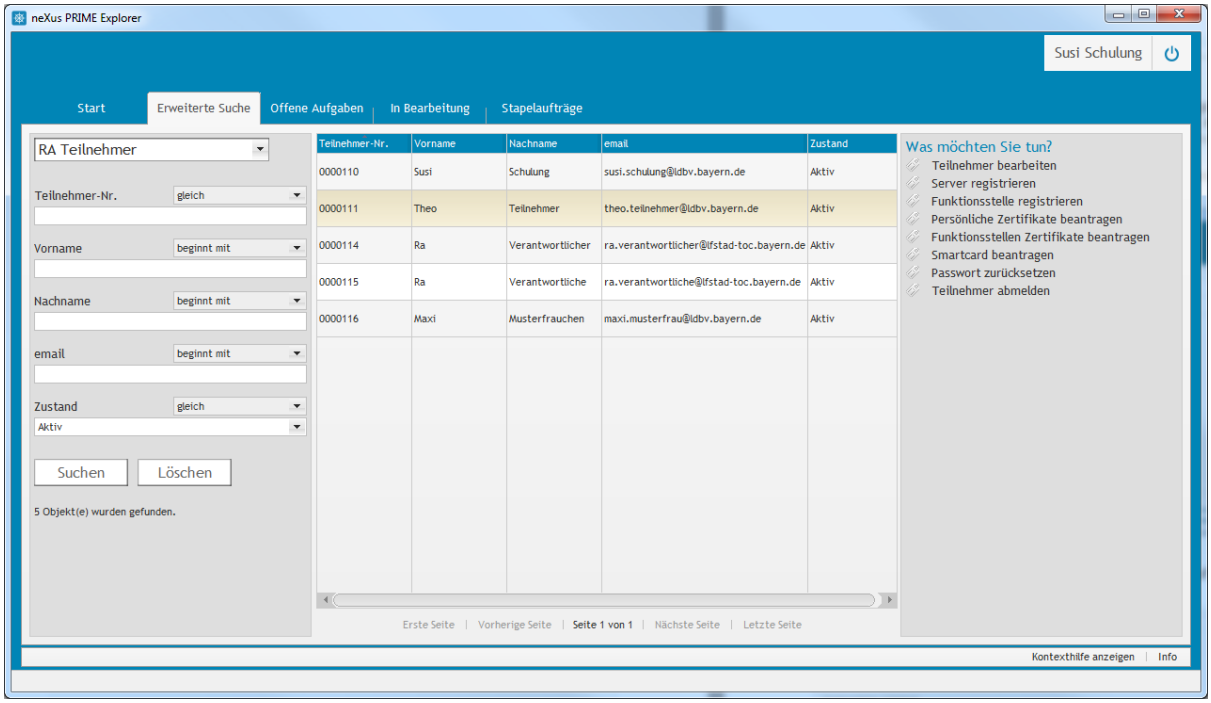


Abschließend wird ein Registrierungsbrief für den Teilnehmer ausgedruckt.

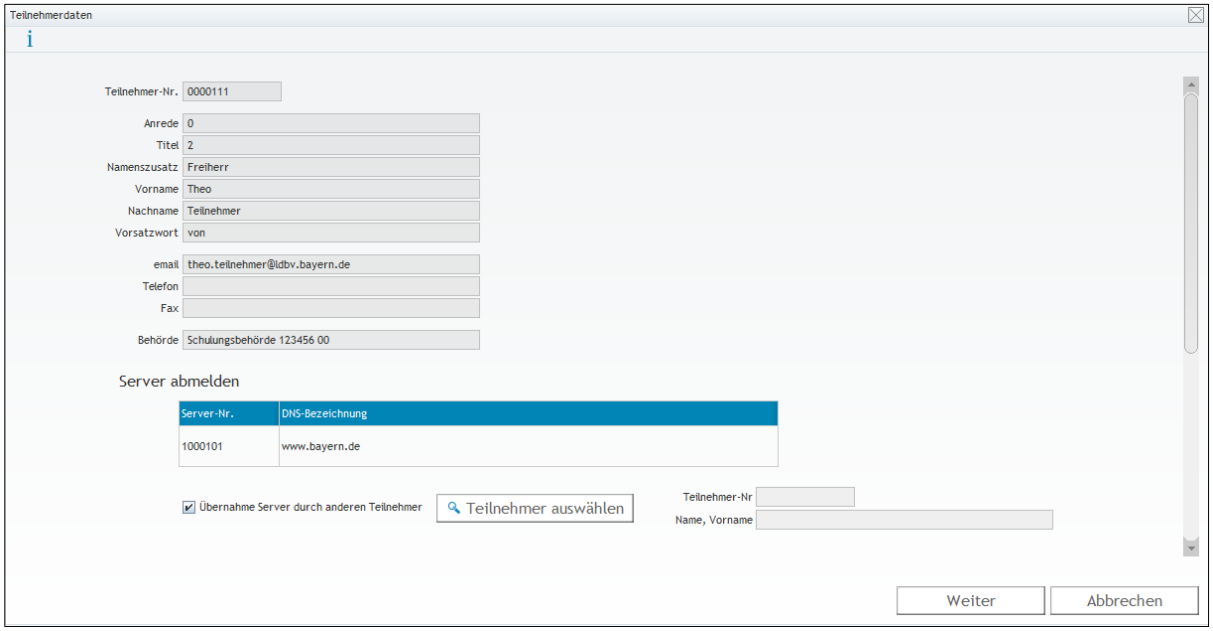
2.3.4 Teilnehmer abmelden

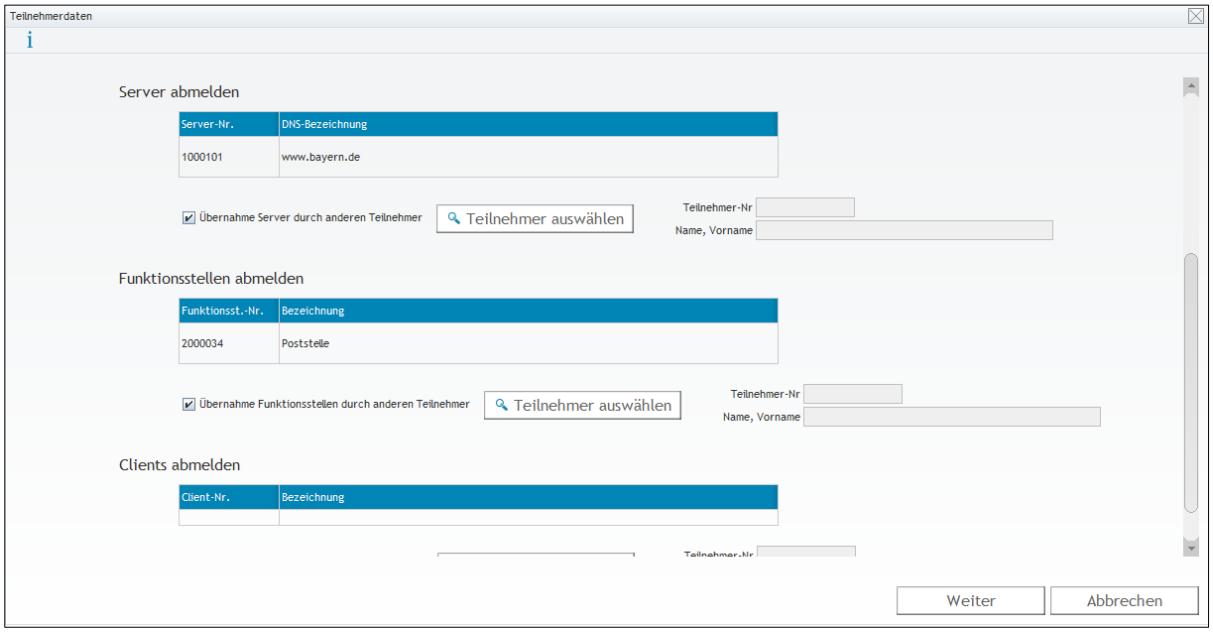
Wenn ein registrierter Teilnehmer den Einflussbereich Ihrer Registrierungsstelle verlässt oder aus anderen Gründen kein Zertifikat mehr bekommen soll, können Sie den Teilnehmer aus dem Zertifikatsverwaltungssystem entfernen. Dabei werden eventuell vorhandene gültige Zertifikate gesperrt.

Suchen Sie zuerst über den **Menüpunkt „Erweiterte Suche“** mit der **Abfrage „RA Teilnehmer“** den zu bearbeitenden Teilnehmer.



Markieren Sie den abzumeldenden Teilnehmer und klicken auf **„Teilnehmer abmelden“** unter „Was möchten Sie tun?“.





Falls dem Teilnehmer Funktionsstellen, Server oder Clients zugeordnet sind, werden diese hier angezeigt.

Sie haben nun die Möglichkeit die Verantwortlichkeit für die Funktionsstellen, Server oder Clients auf einen anderen Teilnehmer zu übertragen (→ Button „Teilnehmer auswählen“) oder die zugeordneten Funktionsstellen, Server oder Clients gleich mit abzumelden (→ Haken bei „Übernahme […] durch anderen Teilnehmer“ entfernen).

Klicken Sie anschließend auf **„Weiter“** um den Vorgang abzuschließen.

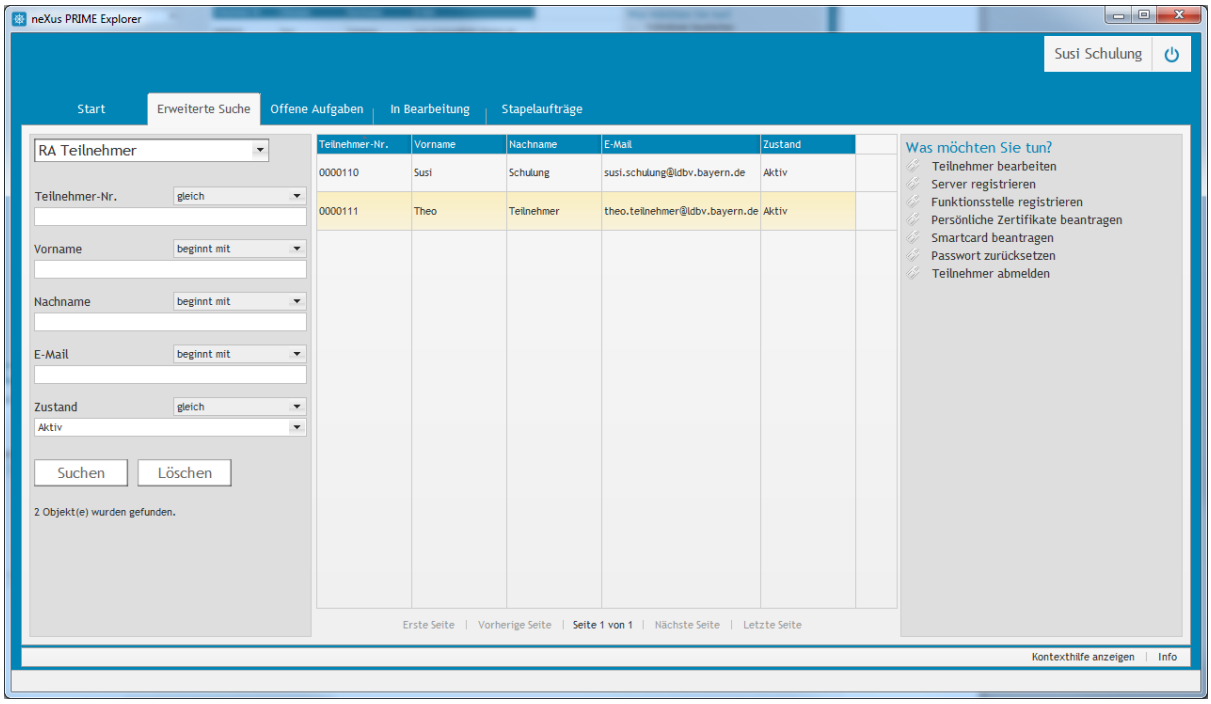
2.4 Einrichten und Pflegen von Funktionsstellen

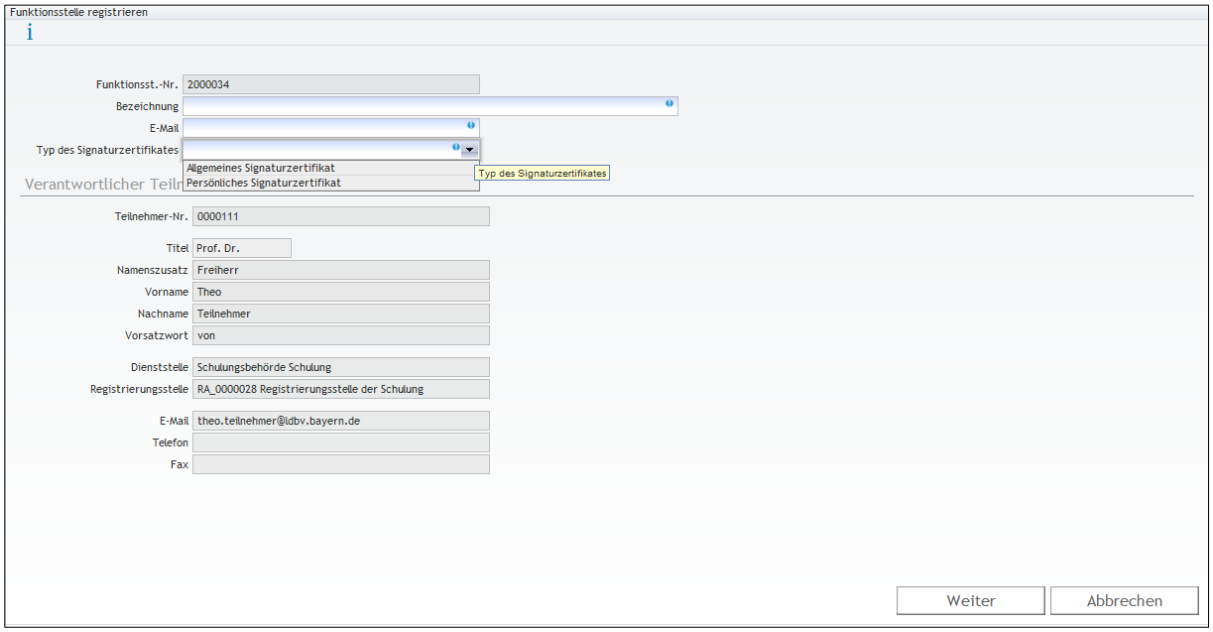
2.4.1 Einrichten einer Funktionsstelle mit gleichzeitiger Benennung eines Funktionsstellenverantwortlichen

Eine Funktionsstelle koordiniert innerhalb der Behörde bestimmte Aktivitäten. Sie besitzt i.A. eine eigene E-Mail Adresse, die von mehreren Mitarbeitern genutzt werden kann. Auch für Funktionsstellen können Zertifikate beantragt werden.

Für jedes Zertifikat einer Funktionsstelle muss ein Verantwortlicher benannt werden. Dieser muss bereits als Teilnehmer registriert sein. Er kann dann für die Funktion Zertifikate beantragen. Ein Teilnehmer kann für mehrere Funktionsstellen verantwortlich sein.

Markieren Sie, wie in Kapitel 2.3.1 beschrieben, den Teilnehmer aus der Liste, der als Zertifikatsverantwortlicher für die Funktionsstelle benannt wird. Klicken Sie dann auf **„Funktionsstelle registrieren“** unter „Was möchten Sie tun?“.





Geben Sie die **Bezeichnung** und **E-Mail-Adresse** der Funktionsstelle ein. Das Behördenkürzel wird bei der Zertifkatsveröffentlichung automatisch angefügt. Es genügt also wenn Sie hier nur die Bezeichnung der Funktionsstelle, z.B. „Poststelle“ angeben.

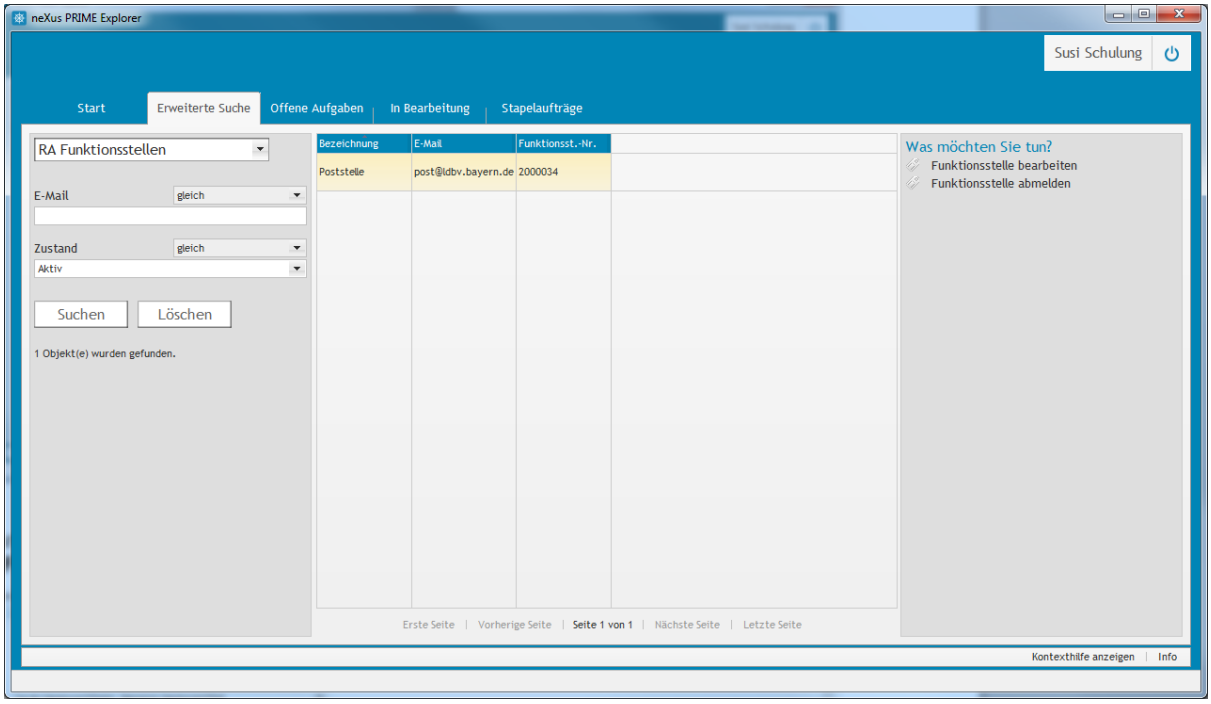
Mit dem **Typ des Signaturzertifikates** unterscheiden Sie die Zuordenbarkeit des Signierenden.

1) Allgemeines Signaturzertifikat: Das Zertifikat enthält die E-Mail Adresse der Funktionsstelle und deren Bezeichnung. Es gibt nur ein Signaturzertifikat, welches jeder Mitarbeiter der Funktion benutzt. Der Empfänger erkennt nur, welche Funktionsstelle unterschrieben hat, aber nicht welcher Mitarbeiter.
2) Persönliches Signaturzertifikat: Das Zertifikat enthält die E-Mail Adresse der Funktionsstelle und den Namen des Funktionsstellenmitarbeiters. Dazu hat jeder Mitarbeiter der Funktion sein eigenes Signaturzertifikat. Der Empfänger kann erkennen, welcher Mitarbeiter der Funktion signiert hat.

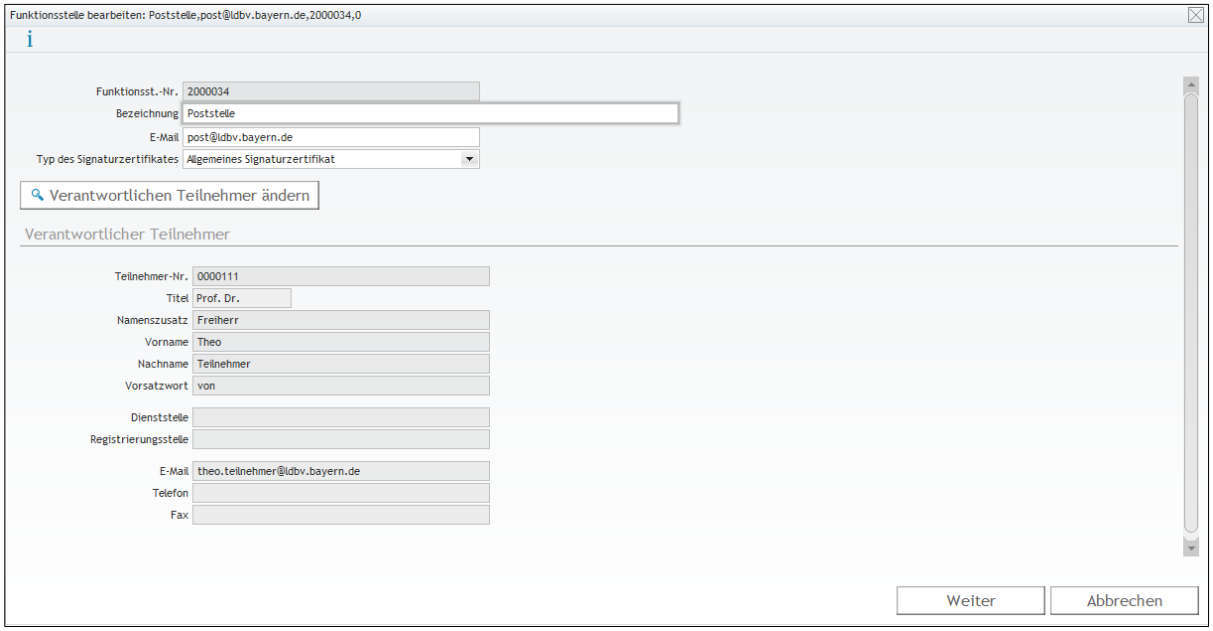
Hinweis: Wir bieten auch die Möglichkeit mehrere Funktionsstellen auf einmal im Zuge eines „Massenimports“ zu registrieren. Beachten Sie dazu das Kapitel 6.2.

2.4.2 Pflege der Funktionsstellendaten

Suchen Sie zuerst über den **Menüpunkt „Erweiterte Suche“** mit der **Abfrage „RA Funktionsstellen“** die zu bearbeitende Funktionsstelle.



Anschließend markieren Sie die Zeile mit der zu ändernden Funktionsstelle und klicken auf **„Funktionsstelle bearbeiten“** unter „Was möchten Sie tun?“

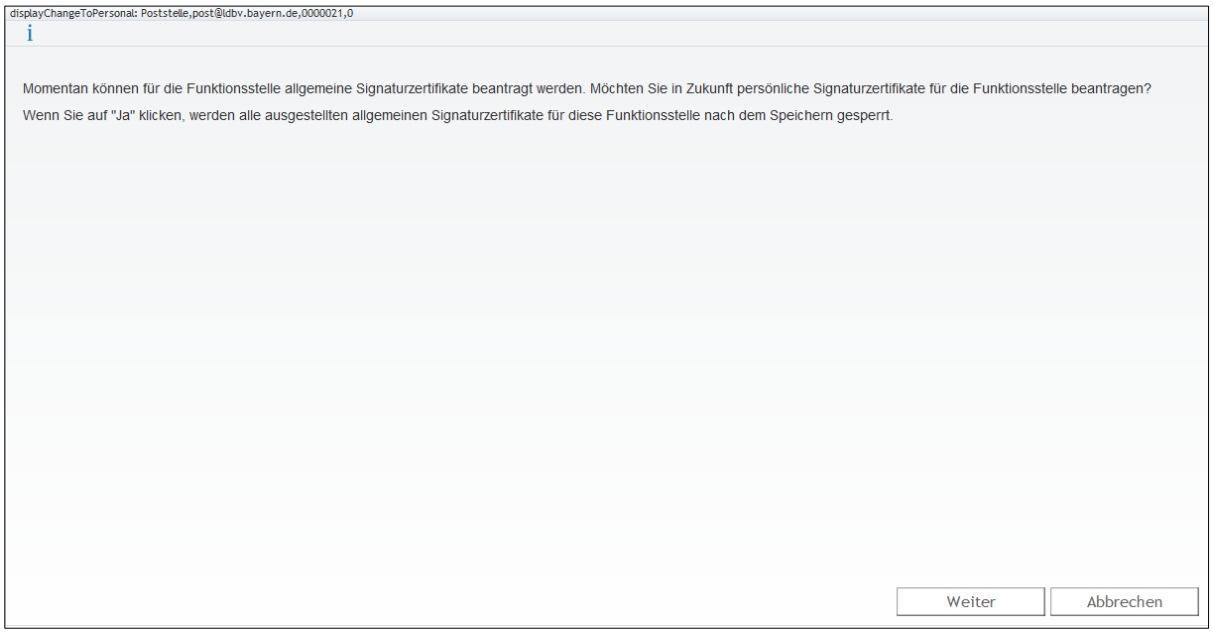


2.4.2.1 Ändern der Bezeichnung oder E-Mail Adresse

Sie können nun die Bezeichnung der Funktionsstelle und/oder deren E-Mail Adresse ändern. Bitte beachten Sie, dass dadurch gültige Zertifikate der Funktionsstelle gesperrt werden und neu beantragt werden müssen.

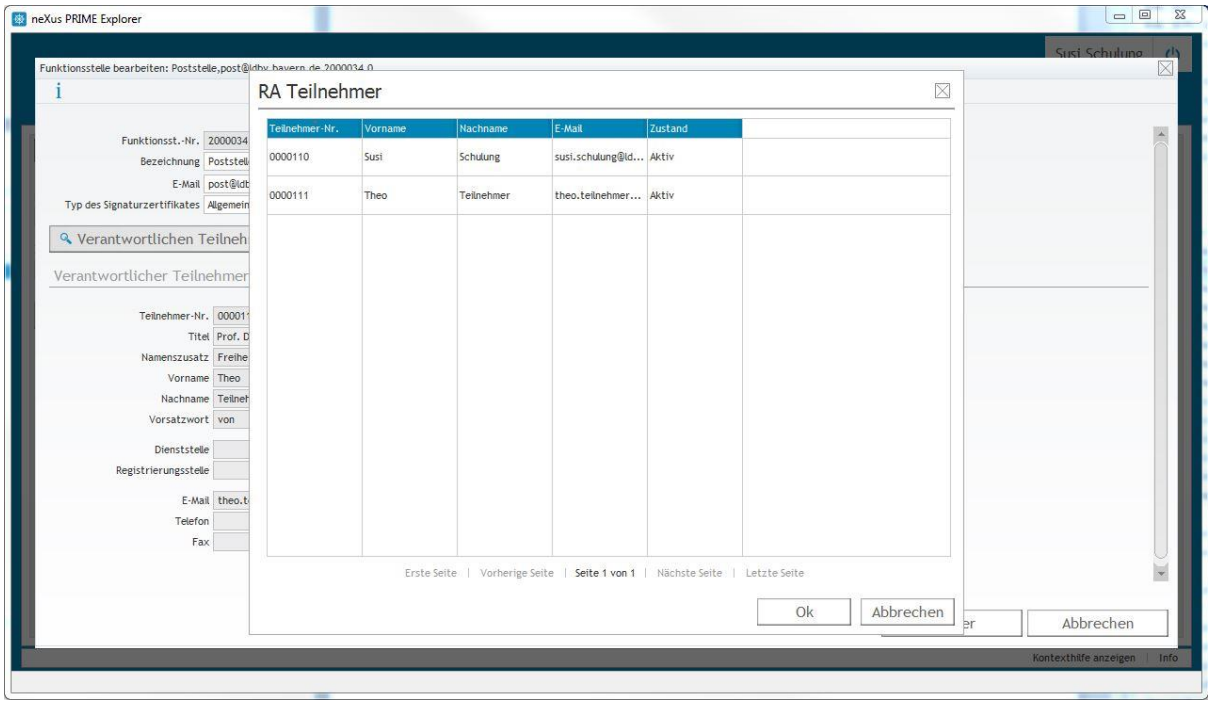
2.4.2.2 Ändern des Typs des Signaturzertifikates

Was die beiden Typen bedeuten, können Sie im Kapitel 2.4.1 nachlesen. Wenn Sie den Typ ändern, wird das bis dahin ausgestellte oder die bis dahin ausgestellten Zertifikate gesperrt und müssen neu beantragt werden.

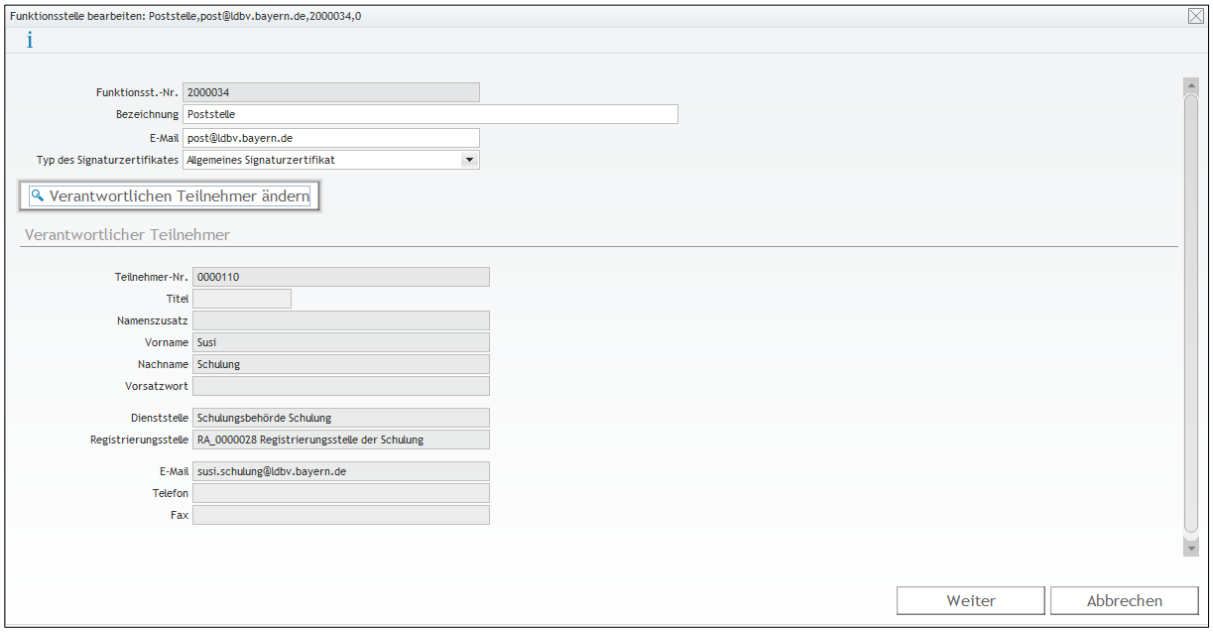


2.4.2.3 Ändern des Funktionsstellenverantwortlichen

Um den verantwortlichen Teilnehmer der Funktionsstelle zu ändern, klicken Sie auf die Schaltfläche **„Verantwortlichen Teilnehmer ändern“**.



Sie bekommen dann eine Liste aller registrierten Teilnehmer angezeigt und wählen aus dieser den neuen verantwortlichen Teilnehmer aus.

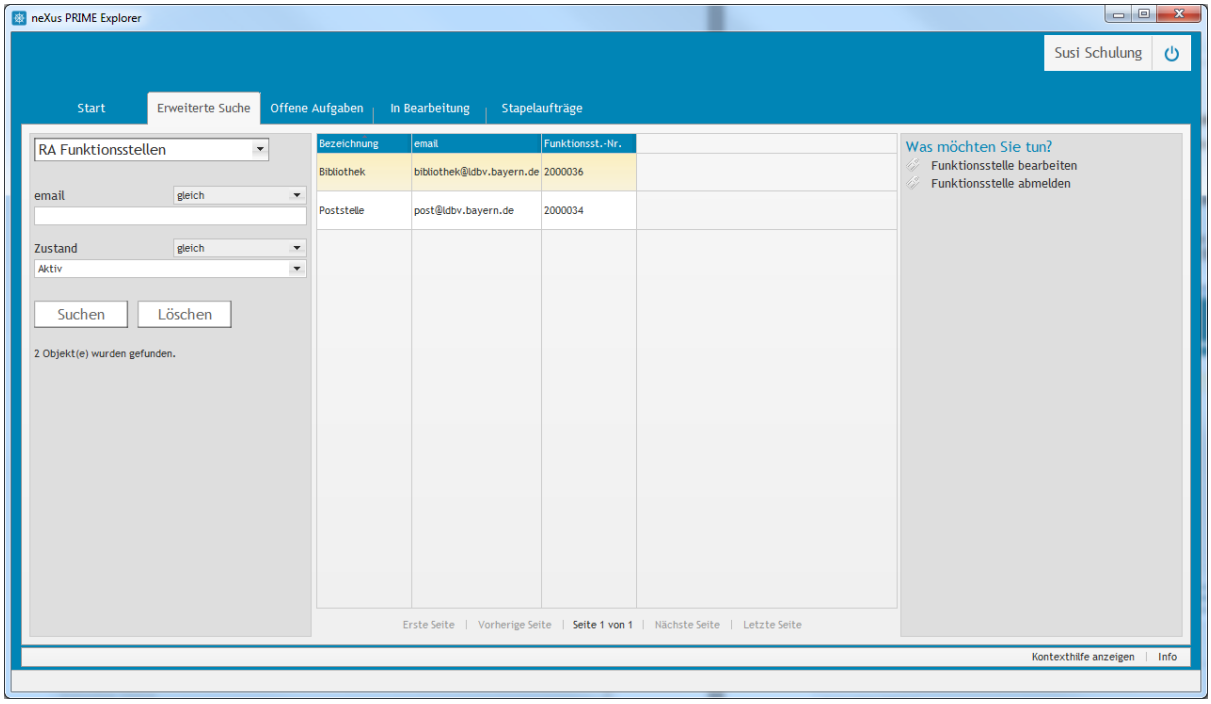


Um die Änderung zu speichern, klicken Sie anschließend noch auf „Weiter“.

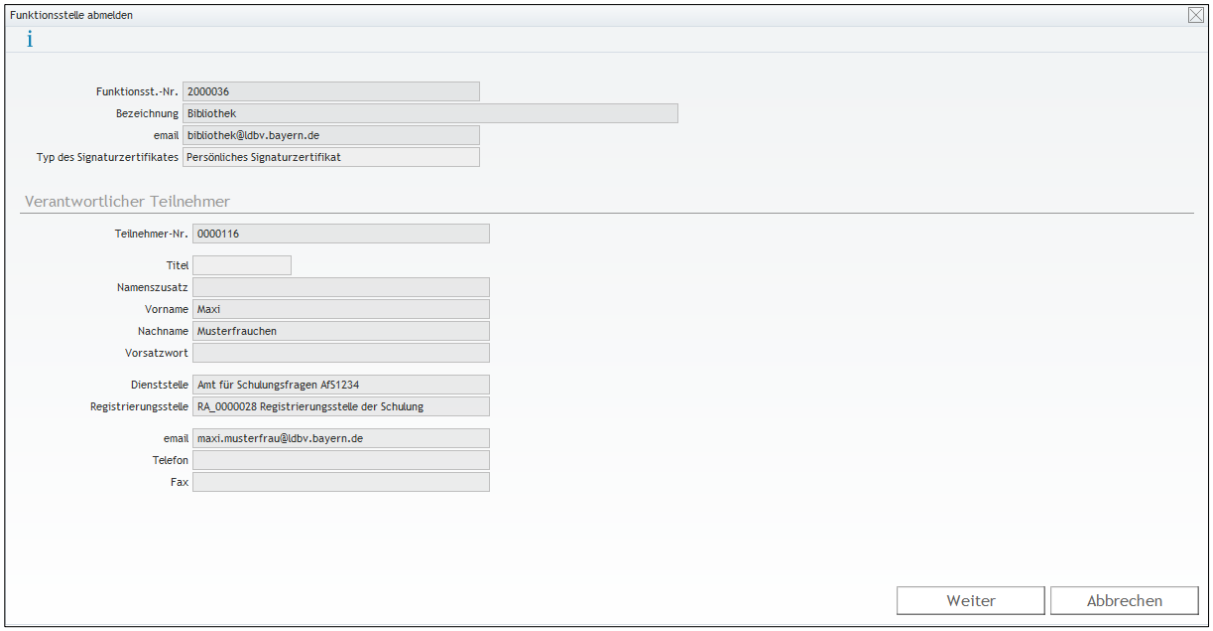
2.4.3 Funktionsstelle abmelden

Wenn Sie eine Funktionsstelle abschaffen oder sie aus anderen Gründen kein Zertifikat mehr bekommen soll, können Sie die Funktionsstelle aus dem Zertifikatsverwaltungssystem entfernen. Dabei werden eventuell vorhandene gültige Zertifikate gesperrt.

Suchen Sie zuerst über den **Menüpunkt „Erweiterte Suche“** mit der **Abfrage „RA Funktionsstellen“** die zu bearbeitende Funktionsstelle.



Markieren Sie die abzumeldende Funktionsstelle und klicken auf **„Funktionsstelle abmelden“** unter „Was möchten Sie tun?“.



Klicken Sie auf **„Weiter“** um den Vorgang abzuschließen.

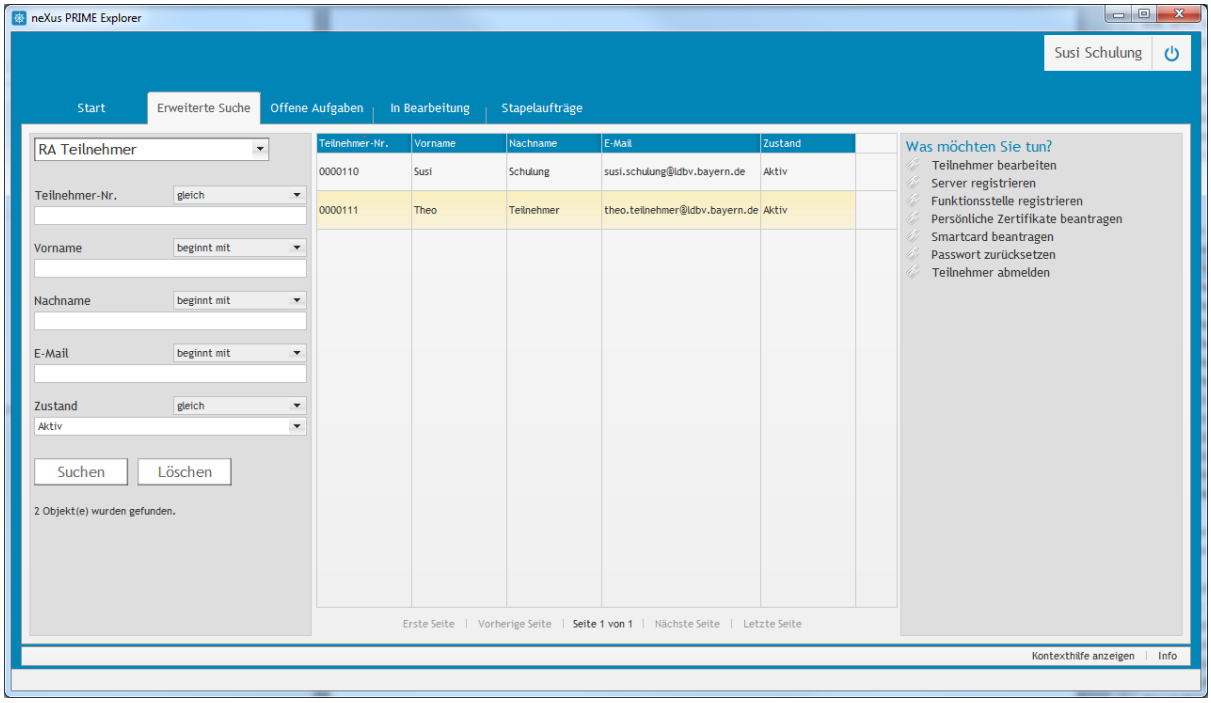
2.5 Einrichten und Pflegen von Servern

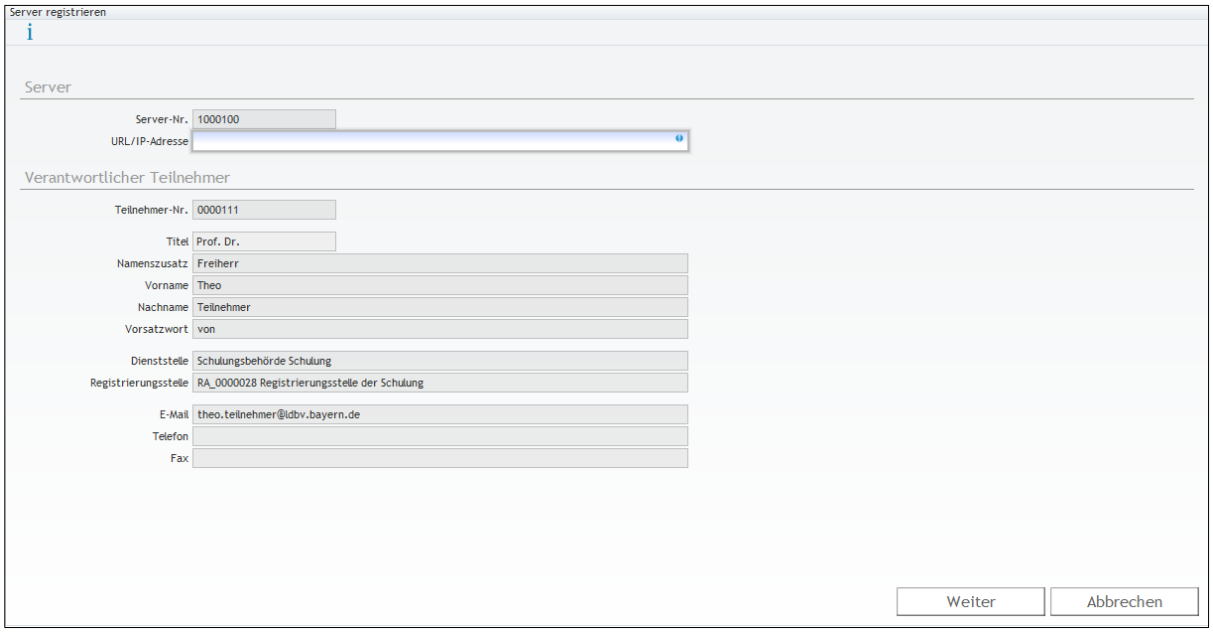
2.5.1 Anlegen eines Servers mit gleichzeitiger Benennung des Verantwortlichen

Um ein Server-Zertifikat zu beantragen, muss der entsprechende Server zunächst registriert und ein Verantwortlicher dafür benannt werden. Dieser muss bereits als Teilnehmer registriert sein.

Als Verantwortlicher für ein Server-Zertifikat erhält dieser dann die Möglichkeit Zertifikate für „seinen“ Server zu beantragen.

Markieren Sie, wie in Kapitel 2.3.1 beschrieben, den Teilnehmer aus der Liste, der als Zertifikatsverantwortlicher für den Server benannt wird. Klicken Sie dann auf **„Server registrieren“** unter „Was möchten Sie tun?“.

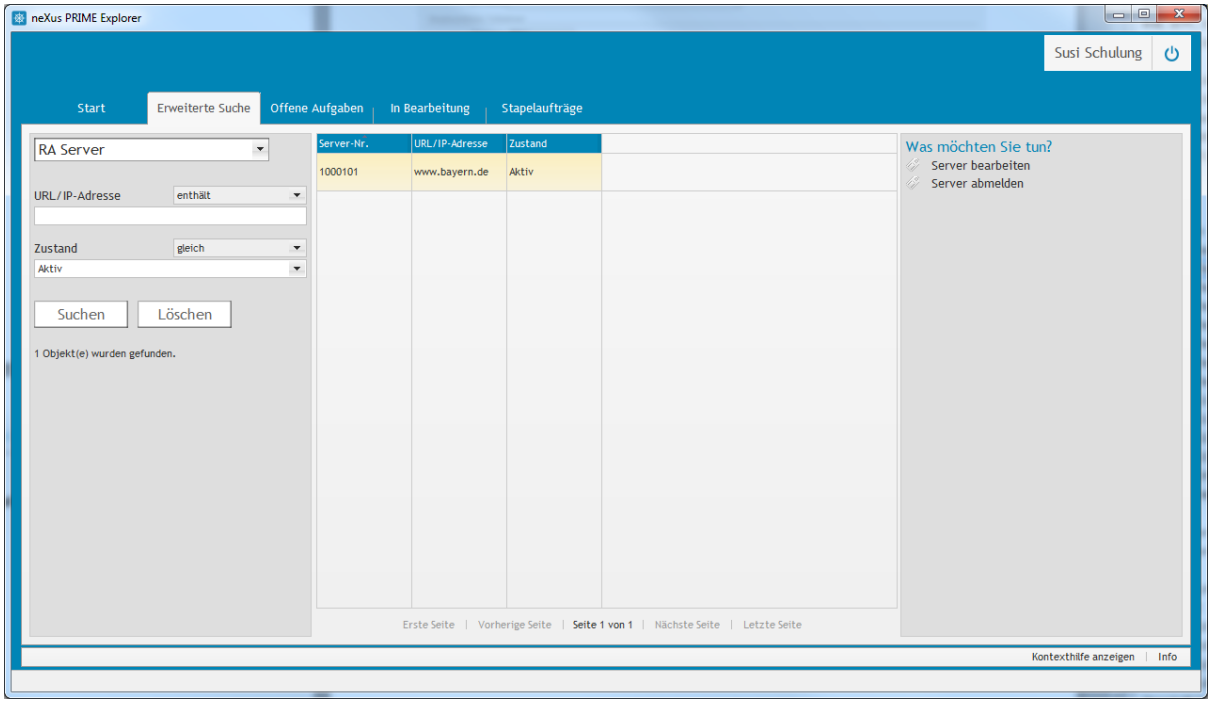




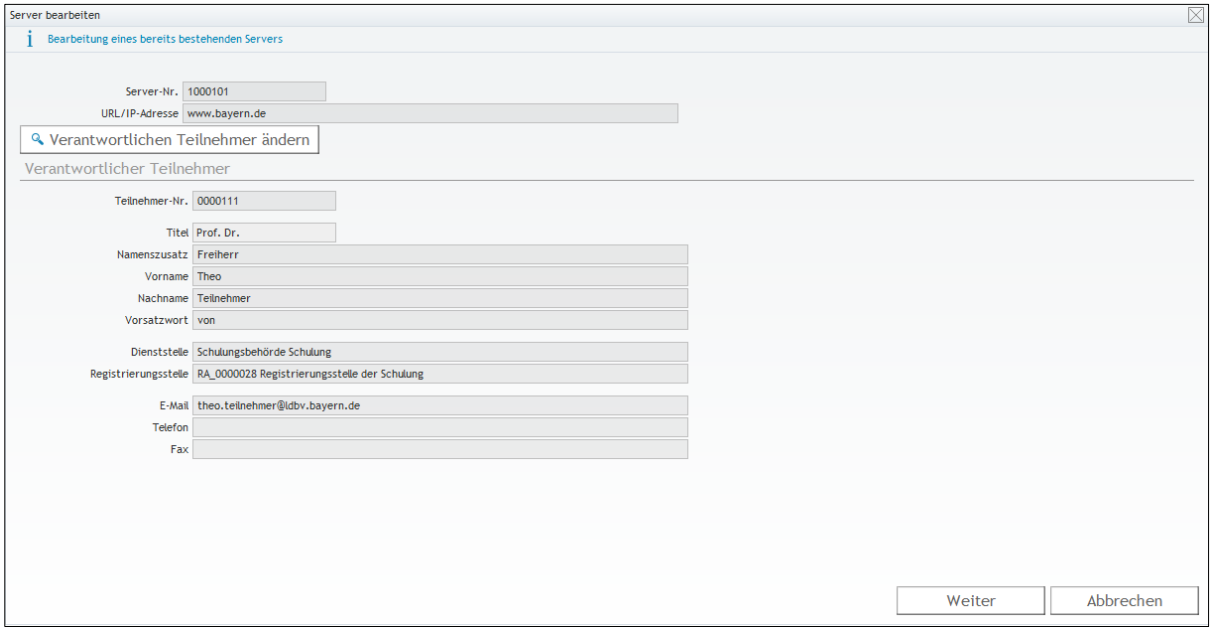
Als einziges Merkmal erfassen Sie die URL oder IP-Adresse unter der der Server erreichbar sein soll. Falls das Serverzertifikat später mehrere URLs oder IP-Adressen beinhalten soll, erfassen Sie hier nur die Hauptadresse.

2.5.2 Pflege der Serverdaten

Suchen Sie zuerst über den **Menüpunkt „Erweiterte Suche“** mit der **Abfrage „RA Server“** den zu bearbeitenden Server.

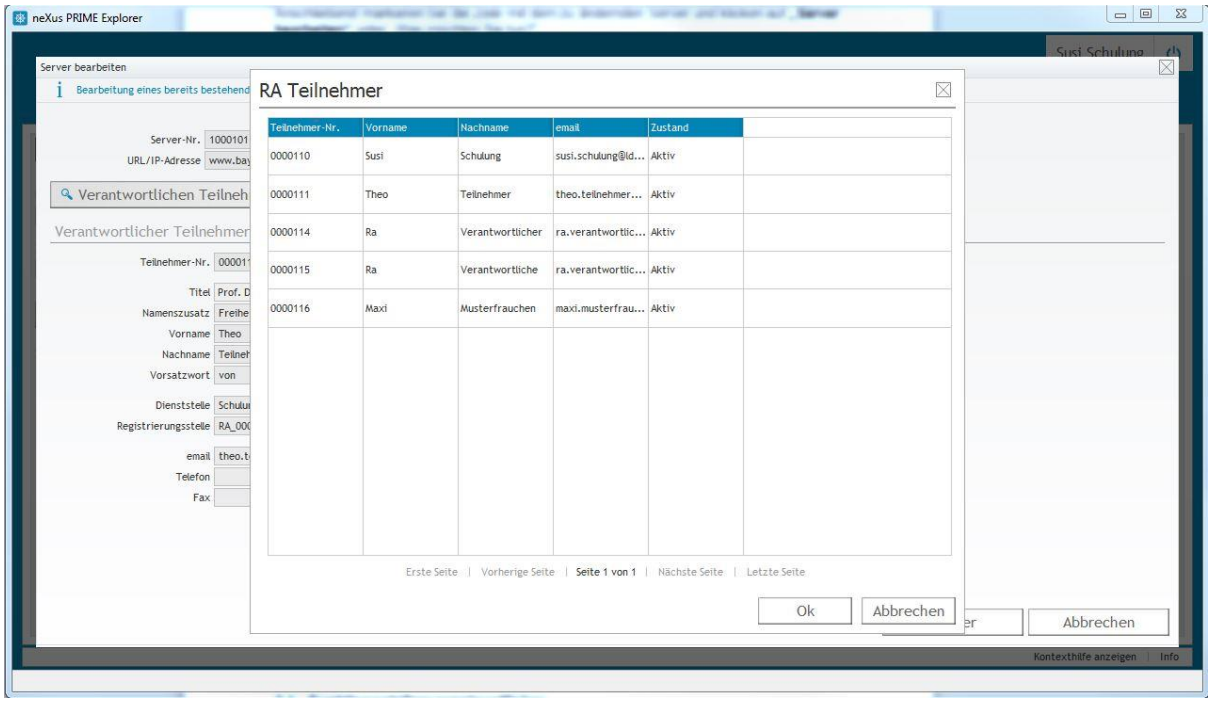


Anschließend markieren Sie die Zeile mit dem zu ändernden Server und klicken auf **„Server bearbeiten“** unter „Was möchten Sie tun?“



Sie können nun den Verantwortlichen für diesen Server ändern. Sollte sich die URL oder IP-Adresse des Servers ändern, melden Sie den Server bitte ab (siehe Kapitel 2.5.3) und registrieren ihn neu (Kapitel 2.5.1).

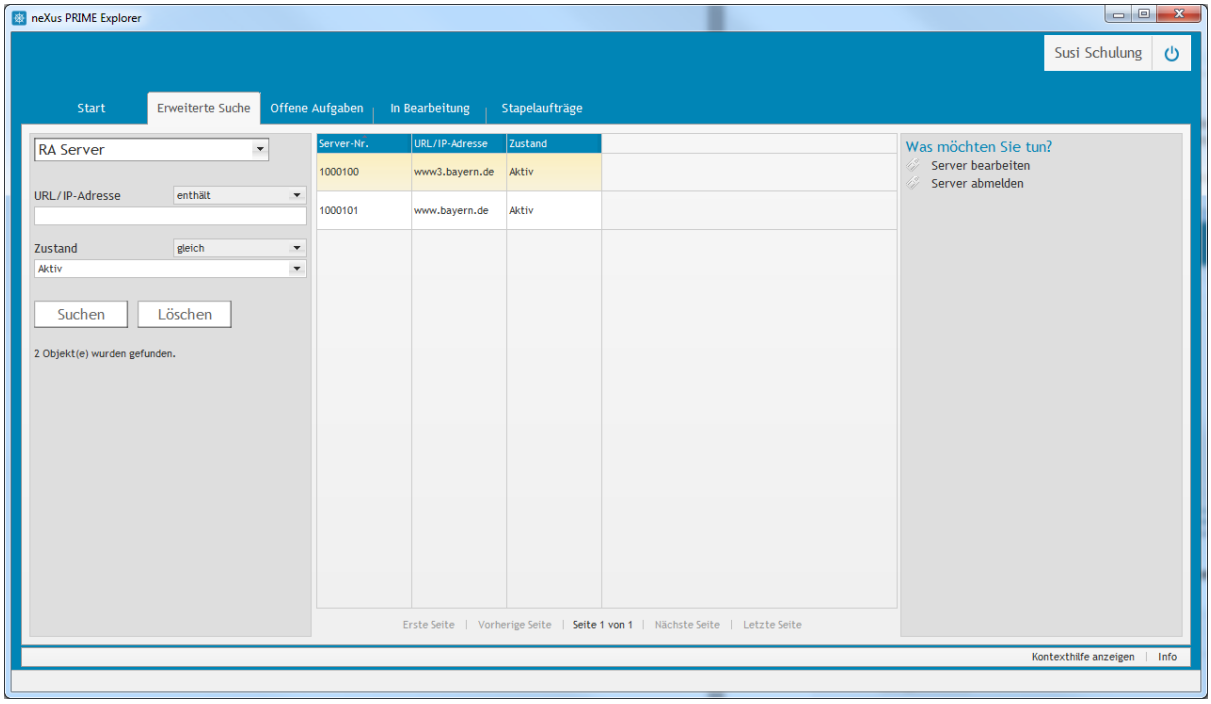
Um den Serververantwortlichen zu ändern, klicken Sie auf die Schaltfläche **„Verantwortlichen Teilnehmer ändern“**. Wählen Sie aus der Liste den neuen Verantwortlichen aus und speichern die Änderung ab, in dem Sie auf „Weiter“ klicken.


neXus PRIME Explorer
Server bearbeiten
Bearbeitung eines bereits bestehend
Server-Nr.
URL/IP-Adresse
Verantwortlichen Teilneh
Verantwortlicher Teilnehmer
Teilnehmer-Nr.
Titel
Namenszusatz
Vorname
Nachname
Vorsatzwort
Dienststelle
Registrierungsstelle
email
Telefon
Fax
RA Teilnehmer
Teilnehmer-Nr.
Vorname
Nachname
email
Zustand
0000110
Susi
Schulung
susi.schulung@ld...
Aktiv
0000111
Theo
Teilnehmer
theo.teilnehmer...
Aktiv
0000114
Ra
Verantwortlicher
ra.verantwortlic...
Aktiv
0000115
Ra
Verantwortliche
ra.verantwortlic...
Aktiv
0000116
Maxi
Musterfrauchen
maxi.musterfrau...
Aktiv
Erste Seite | Vorherige Seite | Seite 1 von 1 | Nächste Seite | Letzte Seite
Ok
Abbrechen
Abbrechen
Kontexthilfe anzeigen | Info

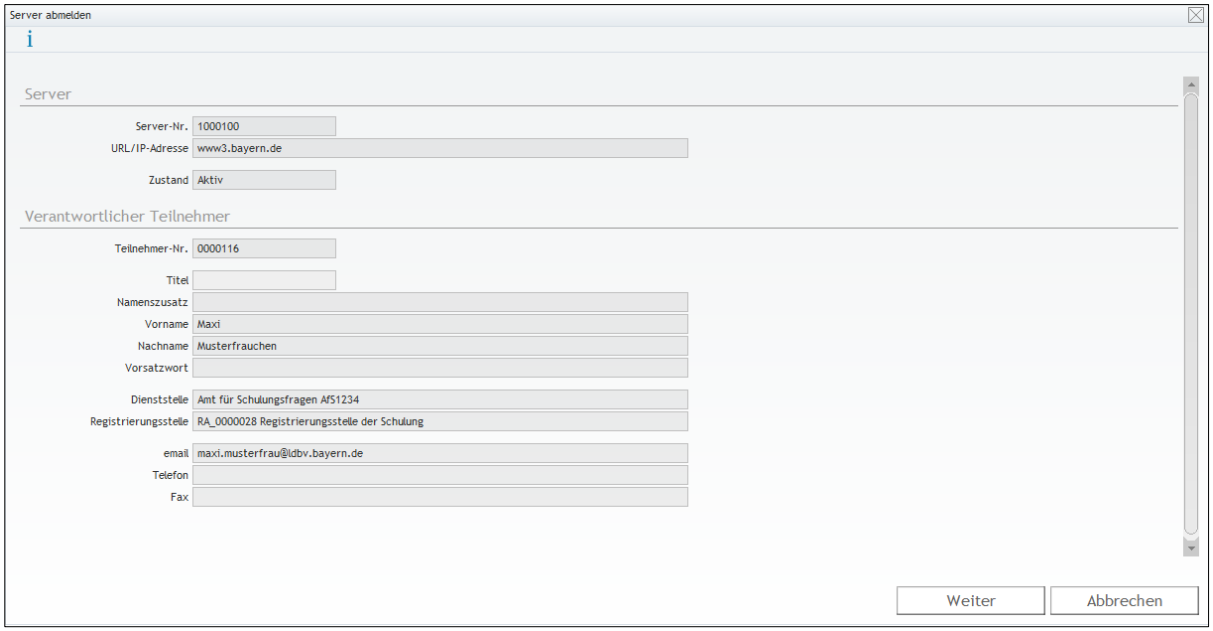
2.5.3 Server abmelden

Wenn Sie einen Server ausmustern oder er aus anderen Gründen kein Zertifikat mehr bekommen soll, können Sie ihn aus dem Zertifikatsverwaltungssystem entfernen. Dabei wird ein eventuell vorhandenes gültiges Zertifikat gesperrt.

Suchen Sie zuerst über den **Menüpunkt „Erweiterte Suche“** mit der **Abfrage „RA Server“** den zu bearbeitenden Server.



Markieren Sie den abzumeldenden Server und klicken auf **„Server abmelden“** unter „Was möchten Sie tun?“.



Klicken Sie auf **„Weiter“** um den Vorgang abzuschließen.

3 Tätigkeiten eines Anwenders

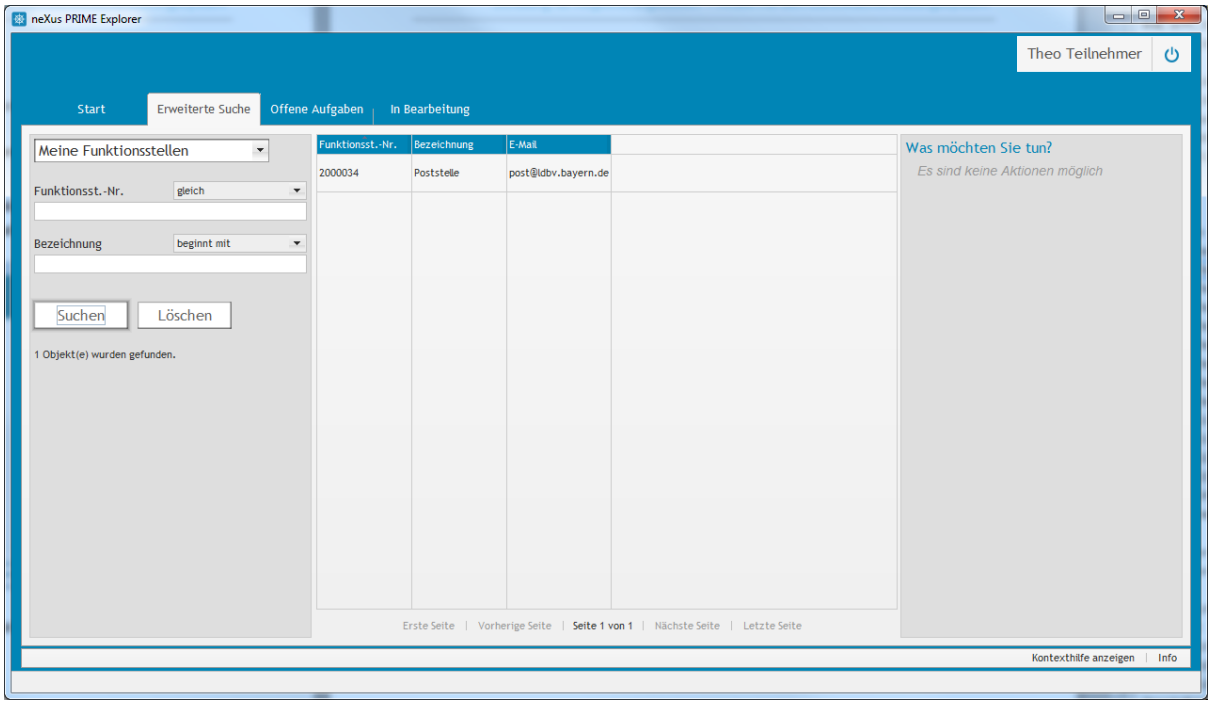
3.1 Funktionsstellenverantwortlicher

Der Funktionsstellen-Verantwortliche kann seinen Funktionsstellen neue Funktionsstellen-Mitarbeiter zuweisen.

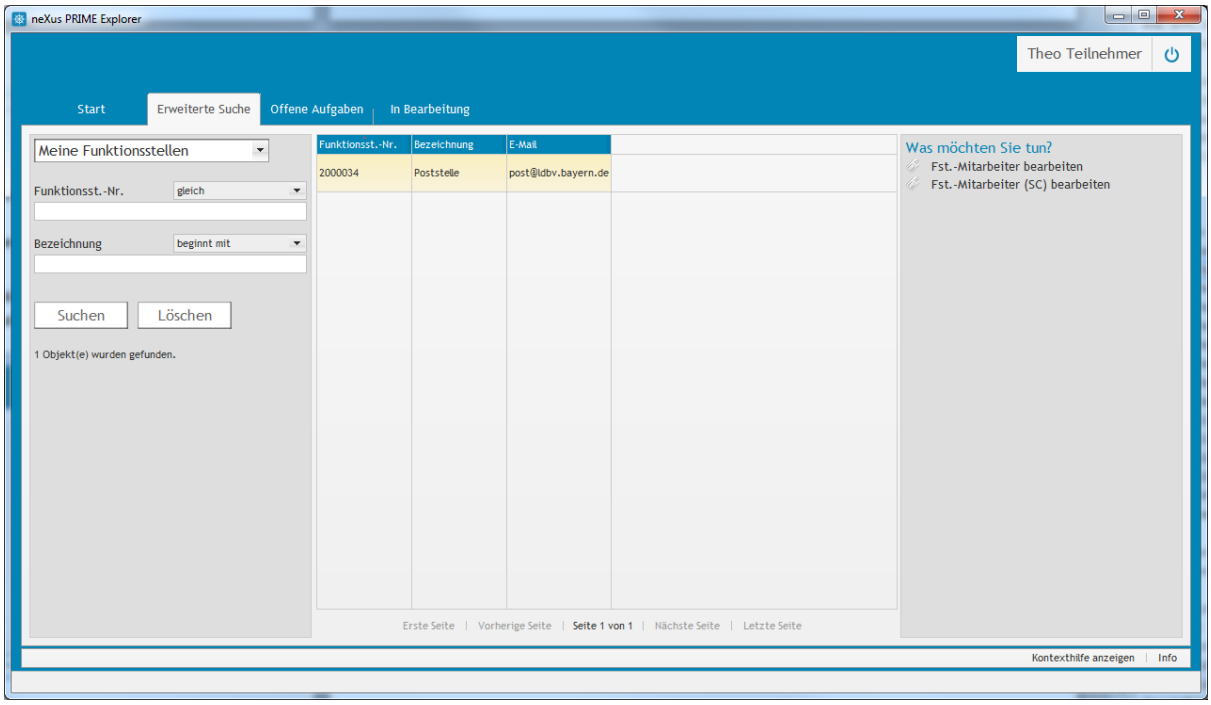
3.1.1 Registrieren/Abmelden von Funktionsstellen-Mitarbeitern (persönliche Signatur)

Voraussetzung: Die Funktionsstelle hat den Signaturzertifikatstyp **Persönliche Signaturzertifikate**.

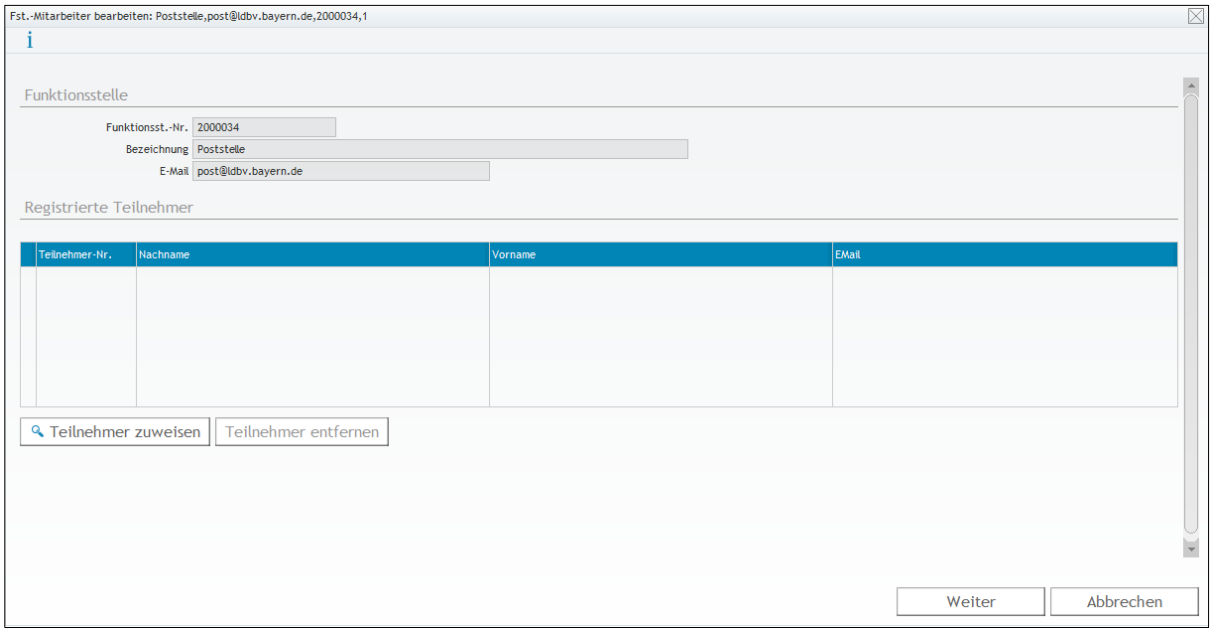
Suchen Sie zuerst über den **Menüpunkt „Erweiterte Suche“** mit der **Abfrage „Meine Funktionsstellen“** die zu bearbeitende Funktionsstelle.



Markieren Sie die zu bearbeitende Funktionsstelle in der Auswahlliste. Anschließend werden Ihnen die möglichen Aktionen für diese Funktionsstelle eingeblendet.



Klicken Sie auf **„Fst.-Mitarbeiter bearbeiten“** unter „Was möchten Sie tun?“.

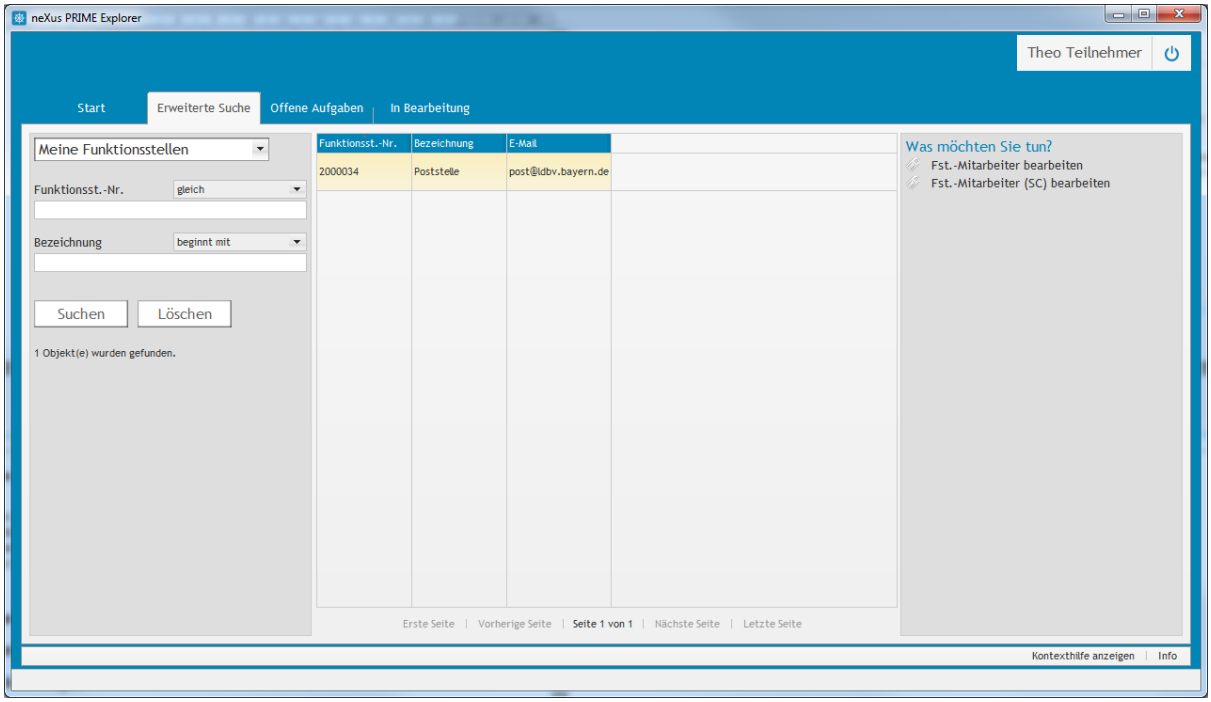


Mit der Schaltfläche **„Teilnehmer zuweisen“** fügen Sie Teilnehmer hinzu, die dann persönliche Signaturzertifikate für diese Funktion beantragen dürfen. Den Unterschied zwischen persönlichen und allgemeinen Signaturzertifikaten einer Funktionsstelle können Sie im Kapitel 2.4.1 nachlesen.

Sobald Sie einen Teilnehmer aus der Liste markieren und auf die Schaltfläche **„Teilnehmer entfernen“** klicken wird das persönliche Signaturzertifikat der Funktion dieses Teilnehmers gesperrt und er kann kein neues Zertifikat beantragen.

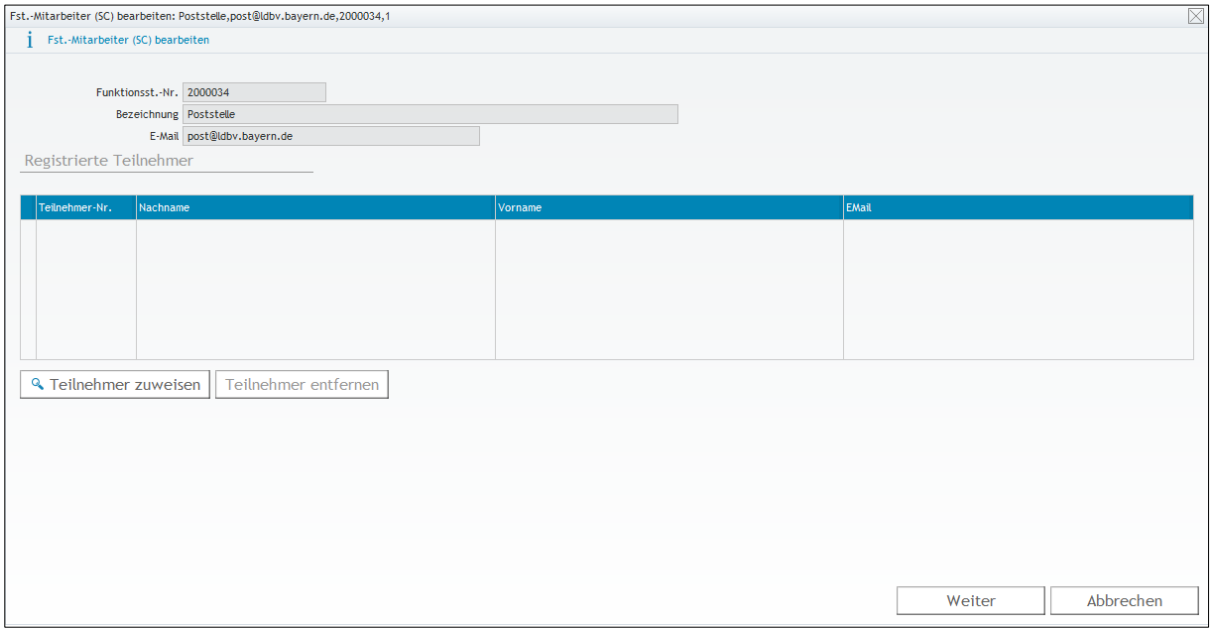
3.1.2 Registrieren/Abmelden von Funktionsstellen-Mitarbeitern für Smartcards

Markieren Sie, wie in Kapitel 3.1.1 beschrieben, die Funktionsstelle aus der Liste, der Sie Teilnehmer berechtigen möchten, damit diese Zertifikate dieser Funktionsstelle auf ihre Smartcard schreiben dürfen. Klicken Sie dann auf **„Fst.-Mitarbeiter (SC) bearbeiten“** unter „Was möchten Sie tun?“.



Mit der Schaltfläche **„Teilnehmer zuweisen“** fügen Sie Teilnehmer hinzu, die dann Zertifikate für diese Funktion auf Ihrer Smartcard beantragen dürfen.

Sobald Sie einen Teilnehmer aus der Liste markieren und auf die Schaltfläche **„Teilnehmer entfernen“** klicken ist es diesem Teilnehmer nicht mehr möglich auf einer neu beantragten Smartcard Funktionsstellenzertifikate zu schreiben.

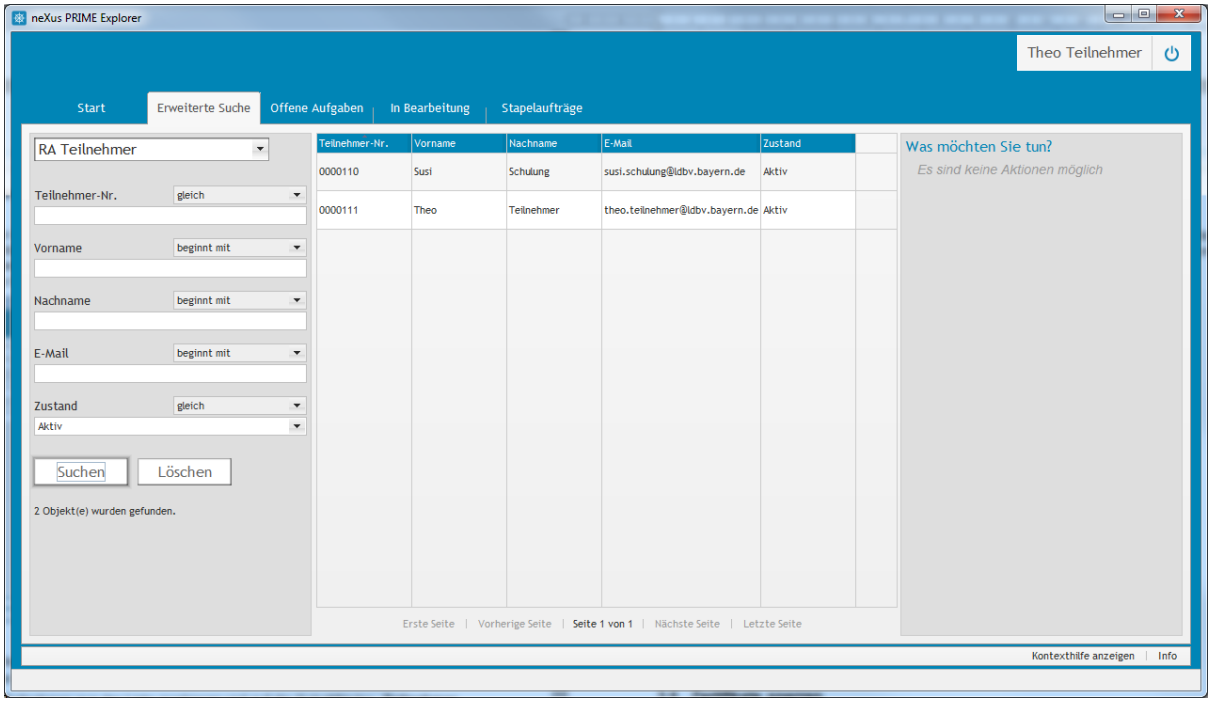


3.2 Clientverantwortlicher

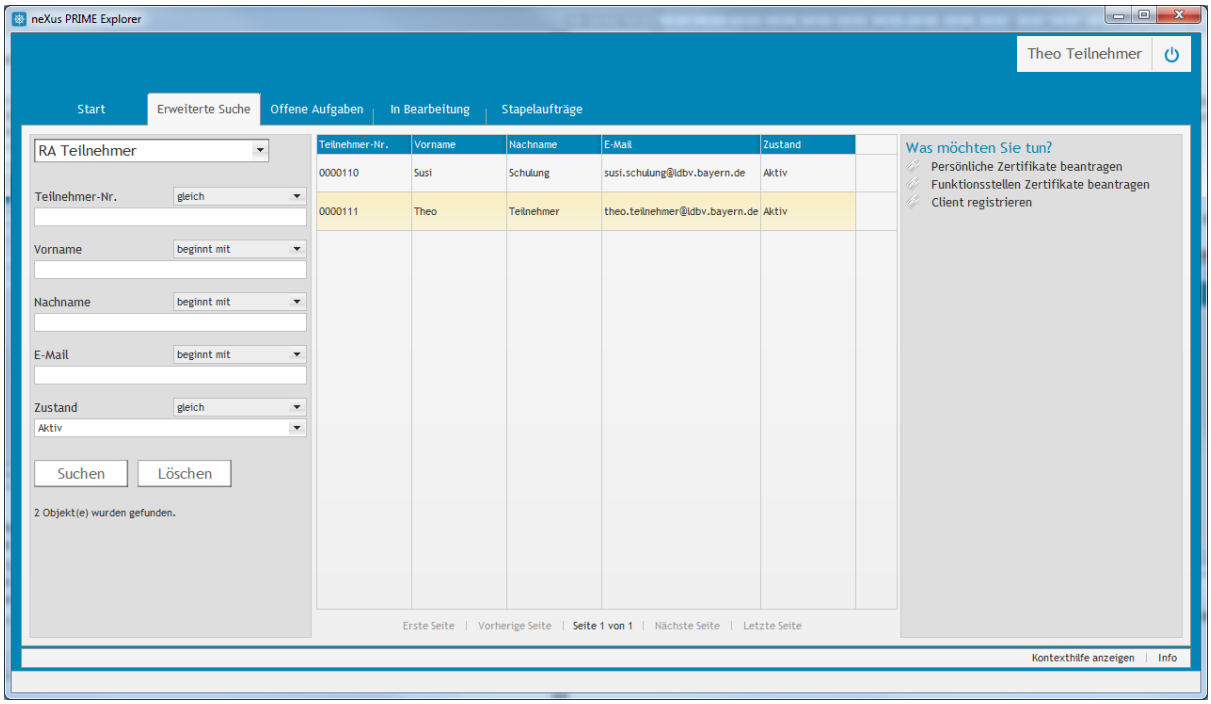
Der Clientverantwortliche ist eine besondere Rolle, die von der Registrierungsstelle zugewiesen werden muss. Teilnehmer mit dieser Rolle haben die Möglichkeit Dienstgeräte, die sich mit einem Zertifikat authentifizieren sollen, zu registrieren. Dabei weisen Sie jedem Dienstgerät (Client) einen Zertifikatsverantwortlichen zu, der anschließend ein Zertifikat beantragen kann (Kapitel 3.3.4).

3.2.1 Client registrieren

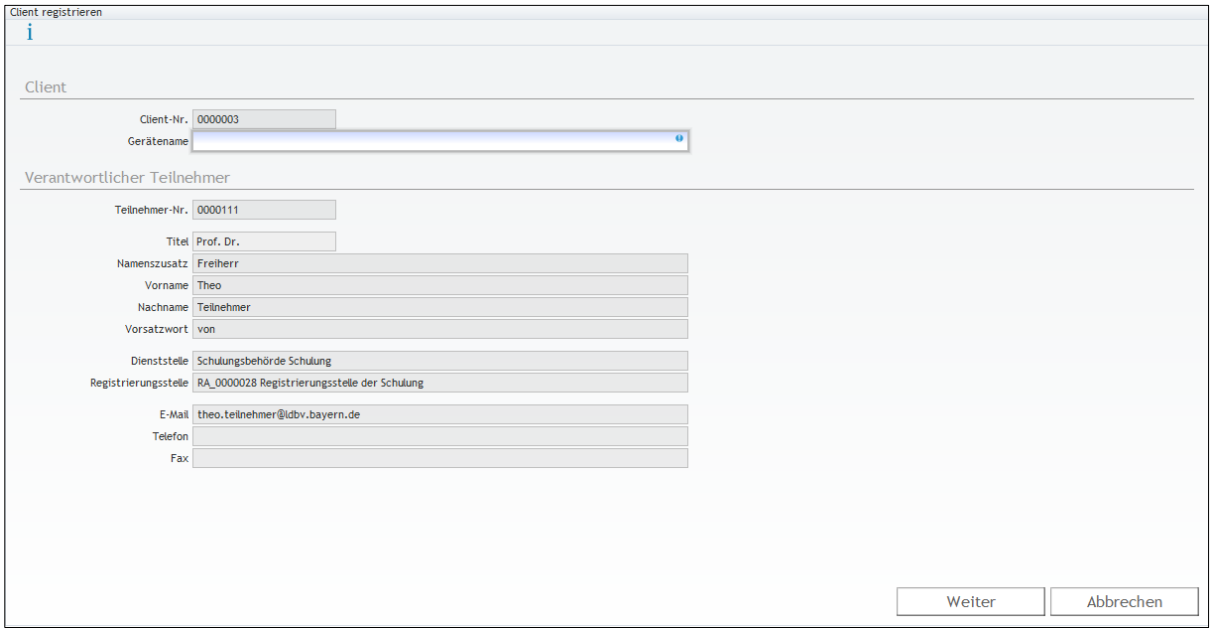
Suchen Sie zuerst über den **Menüpunkt „Erweiterte Suche“** mit der **Abfrage „RA Teilnehmer“** den Zertifikatsverantwortlichen aus einer Liste aller registrierter Teilnehmer der eigenen Registrierungsstelle.



Markieren Sie Zertifikatverantwortlichen in der Auswahlliste. Anschließend werden Ihnen die möglichen Aktionen eingeblendet.



Klicken Sie auf **„Client registrieren“** unter „Was möchten Sie tun?“.

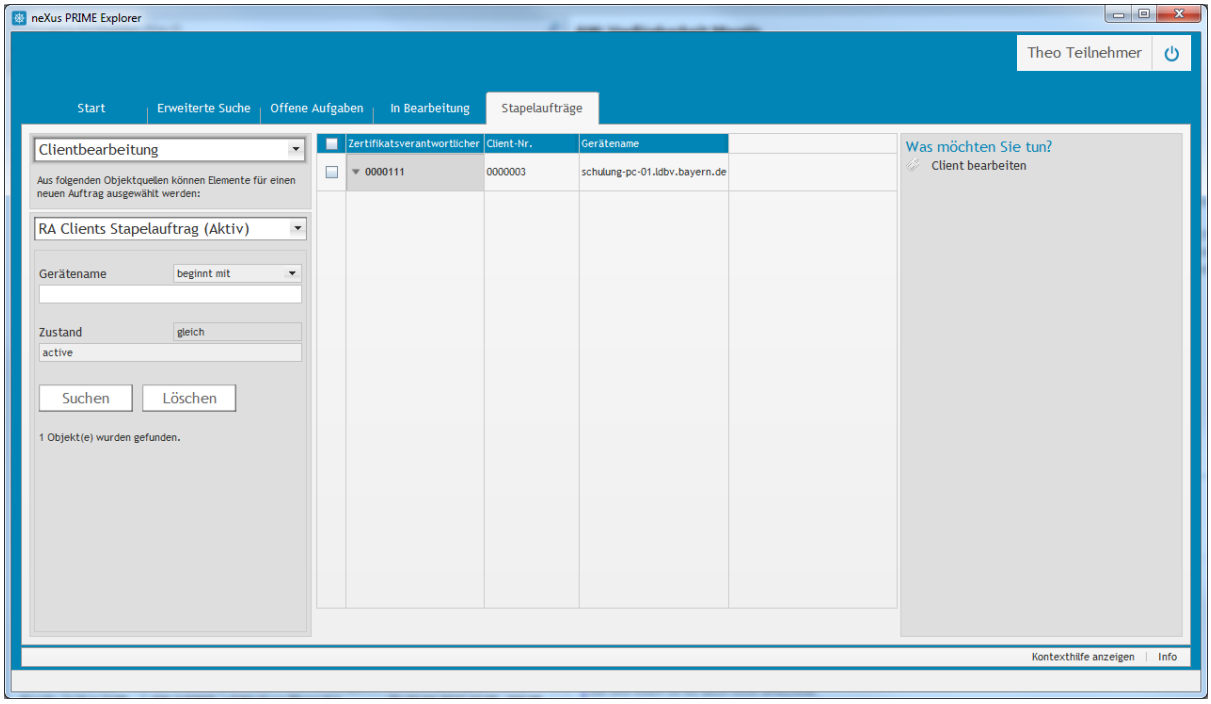


Erfassen Sie nun noch den FQDN des Clients und klicken zum Abschluss auf **„Weiter“**.

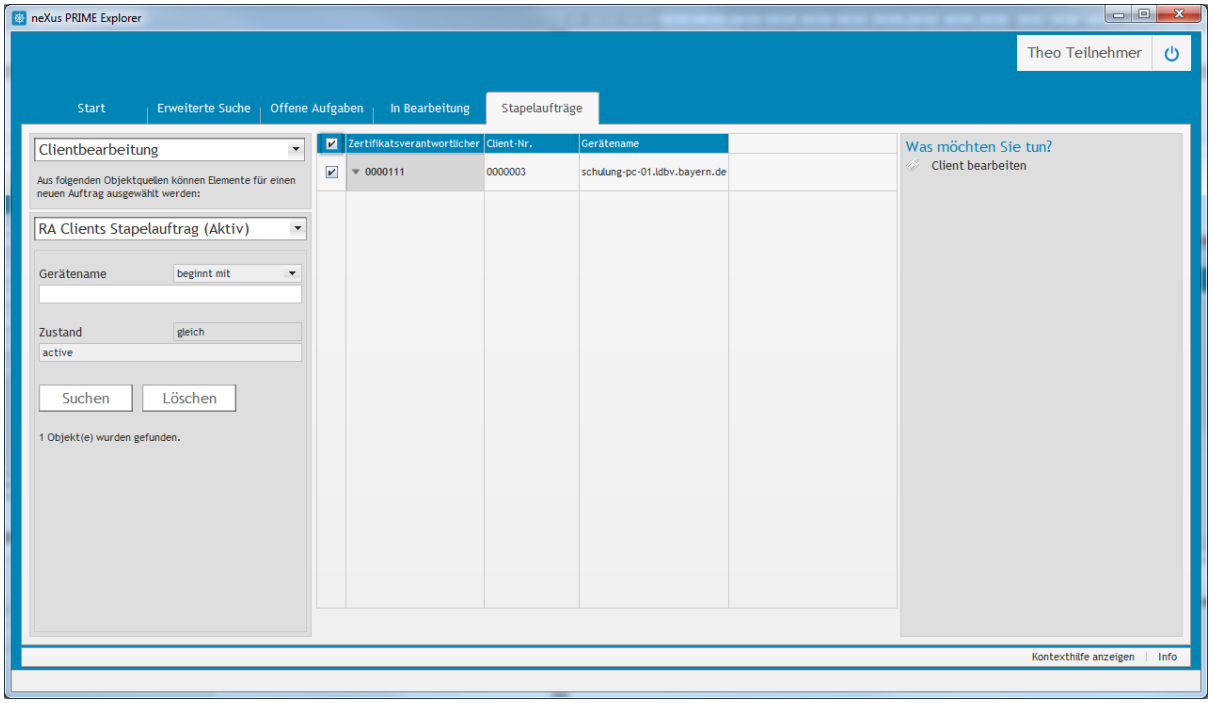
Hinweis: Wir bieten auch die Möglichkeit mehrere Clients auf einmal im Zuge eines „Massenimports“ zu registrieren. Beachten Sie dazu das Kapitel 6.3.

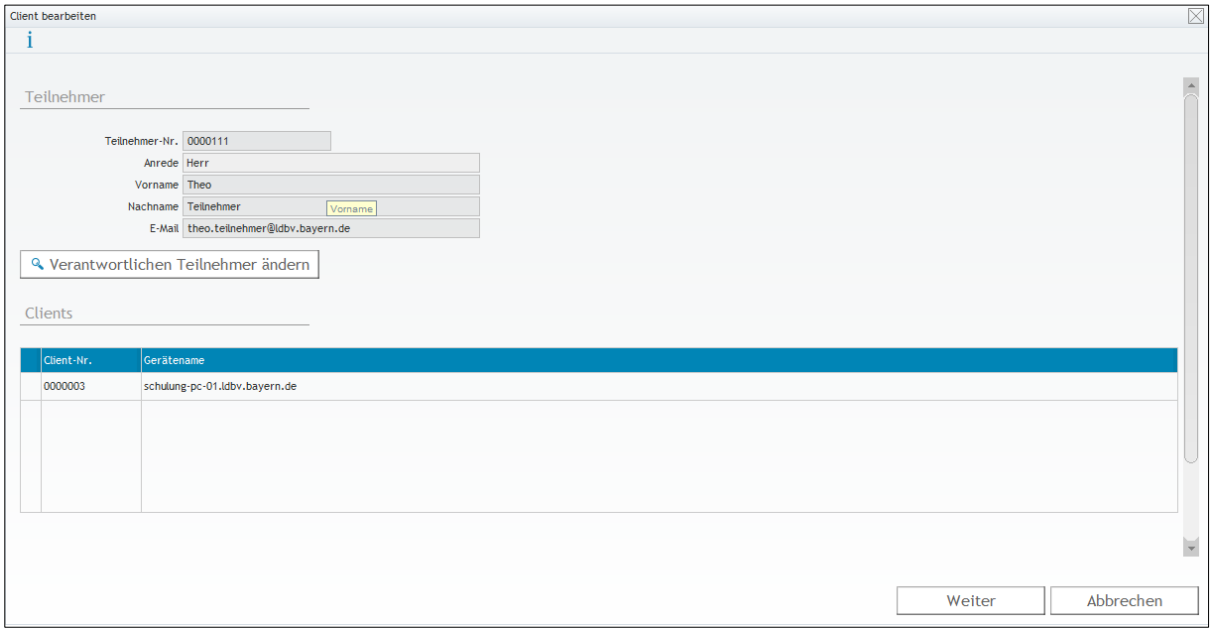
3.2.2 Client bearbeiten

Suchen Sie zuerst über den **Menüpunkt „Stapelaufträge“** mit der **Abfrage „Clientbearbeitung“** den oder die zu bearbeitenden Client(s).

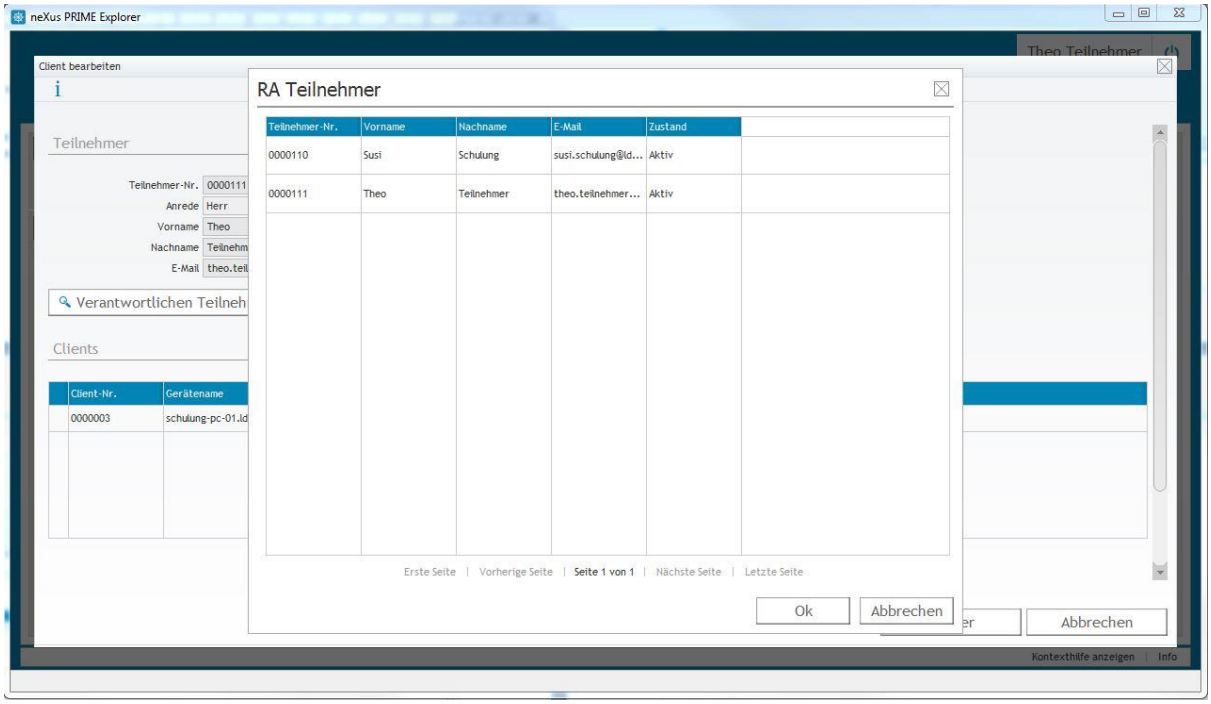


Setzen Sie bei einem oder mehreren Clients den Haken in der ersten Spalte und klicken auf **„Client bearbeiten“** unter „Was möchten Sie tun?“.





Sie haben jetzt die Möglichkeit für alle aufgeführten Clients den Verantwortlichen zu ändern. Klicken Sie dazu auf **„Verantwortlichen Teilnehmer ändern“**.



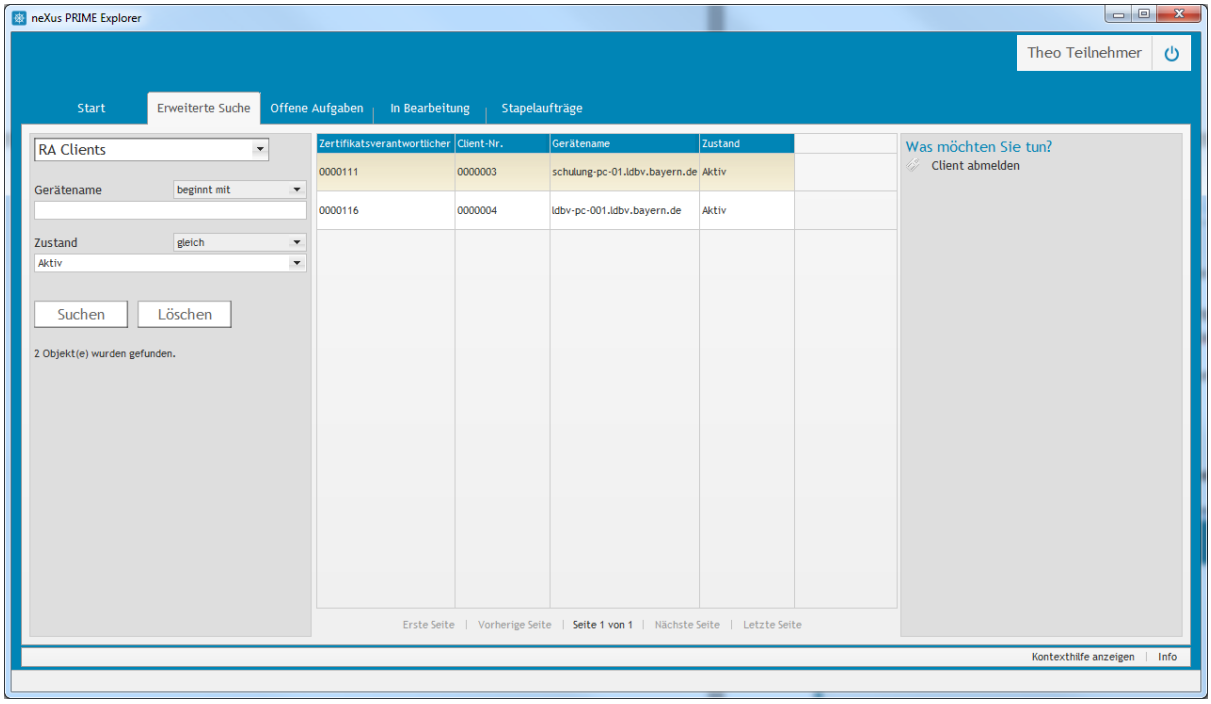
Sie bekommen dann eine Liste aller registrierten Teilnehmer angezeigt und wählen aus dieser den neuen verantwortlichen Teilnehmer aus.

Um die Änderung zu speichern, klicken Sie anschließend noch auf „Weiter“.

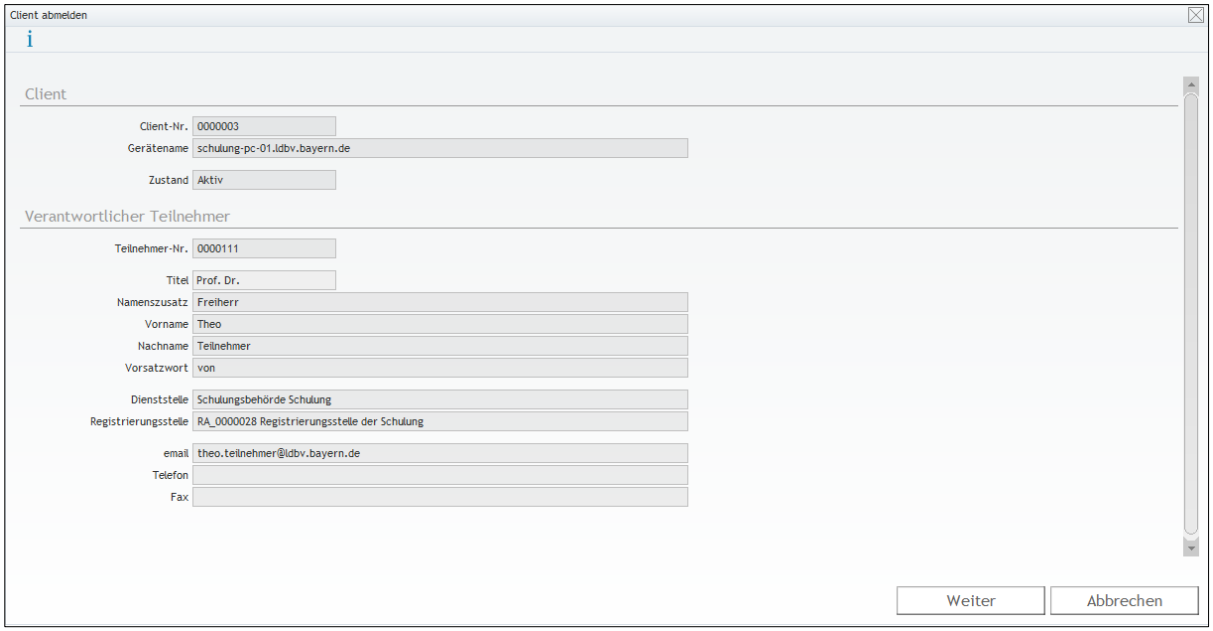
3.2.3 Client abmelden

Wenn Sie ein Dienstgerät ausmustern oder es aus anderen Gründen kein Zertifikat mehr bekommen soll, können Sie es aus dem Zertifikatsverwaltungssystem entfernen. Dabei wird ein eventuell vorhandenes gültiges Zertifikat gesperrt.

Suchen Sie zuerst über den **Menüpunkt „Erweiterte Suche“** mit der **Abfrage „RA Clients“** den zu bearbeitenden Client.



Markieren Sie den abzumeldenden Client und klicken auf **„Client abmelden“** unter „Was möchten Sie tun?“.



Klicken Sie auf **„Weiter“** um den Vorgang abzuschließen.

3.3 Zertifikate beantragen

Sie können Zertifikate der Bayerischen Verwaltungs-PKI auf drei unterschiedliche Arten bekommen.

1.) Beantragung als Softtoken über das Zertifikatsverwaltungssystem.

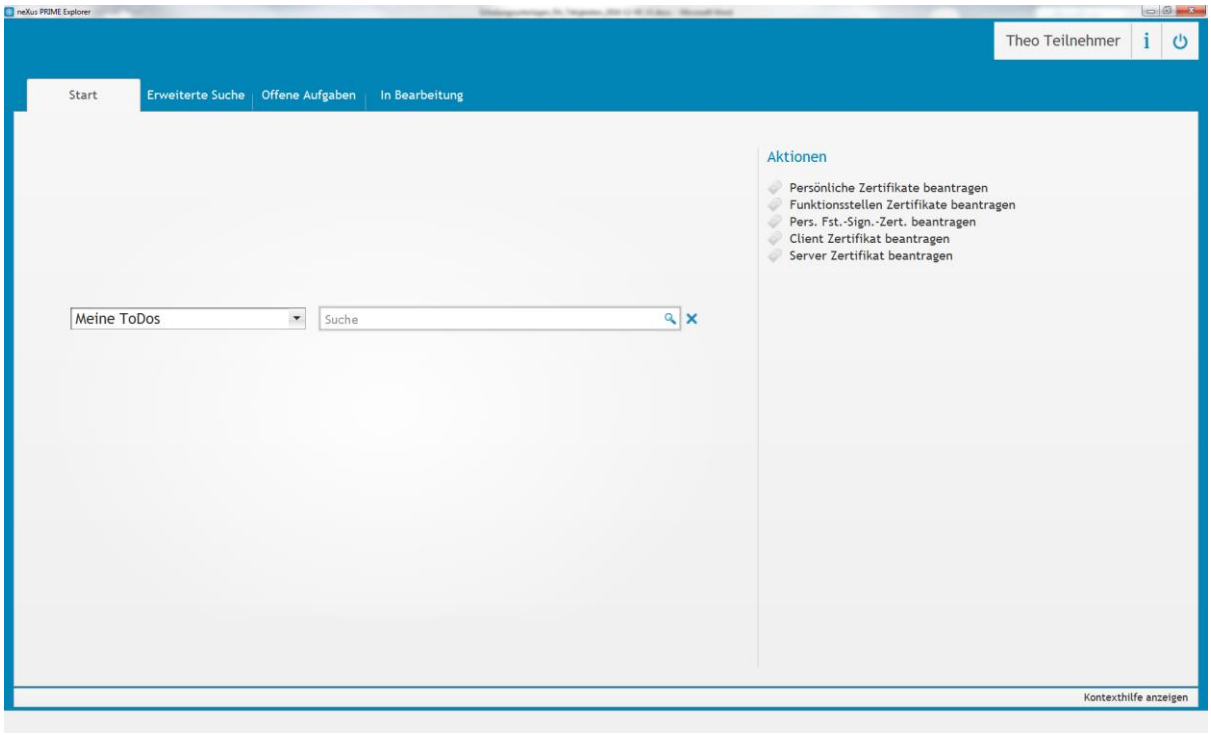
2.) Automatische Beantragung als Softtoken durch den Autoenrollment Mechanismus des Microsoft Betriebssystems.

3.) Beantragung einer Smartcard (kein Server- und Clientzertifikat)

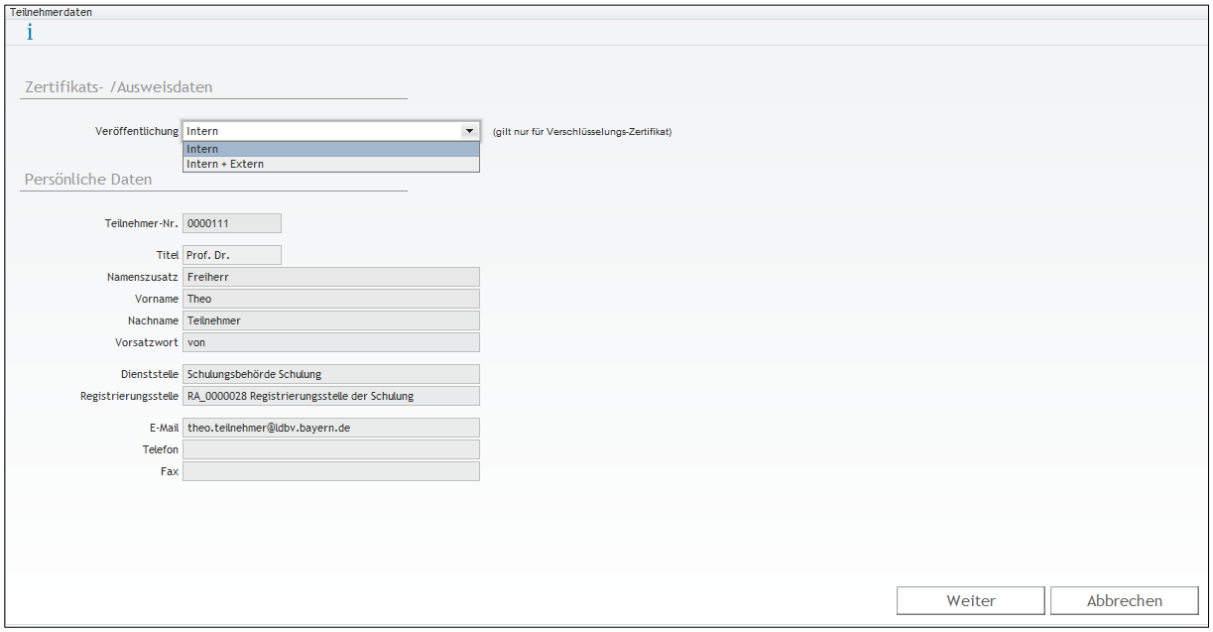
In diesem Kapitel wird nur der erste Fall betrachtet.

3.3.1 Persönliche Zertifikate

Rufen Sie auf der Startseite unter **Aktionen** den Punkt **„Persönliche Zertifikate beantragen“** auf.



Wählen Sie nun noch die gewünschte **Veröffentlichung** für das Verschlüsselungszertifikat aus. **Intern** bedeutet, dass das Zertifikat nur im Behördennetz abrufbar sein wird. **Intern + Extern** erwirkt zudem eine Veröffentlichung im Internet.



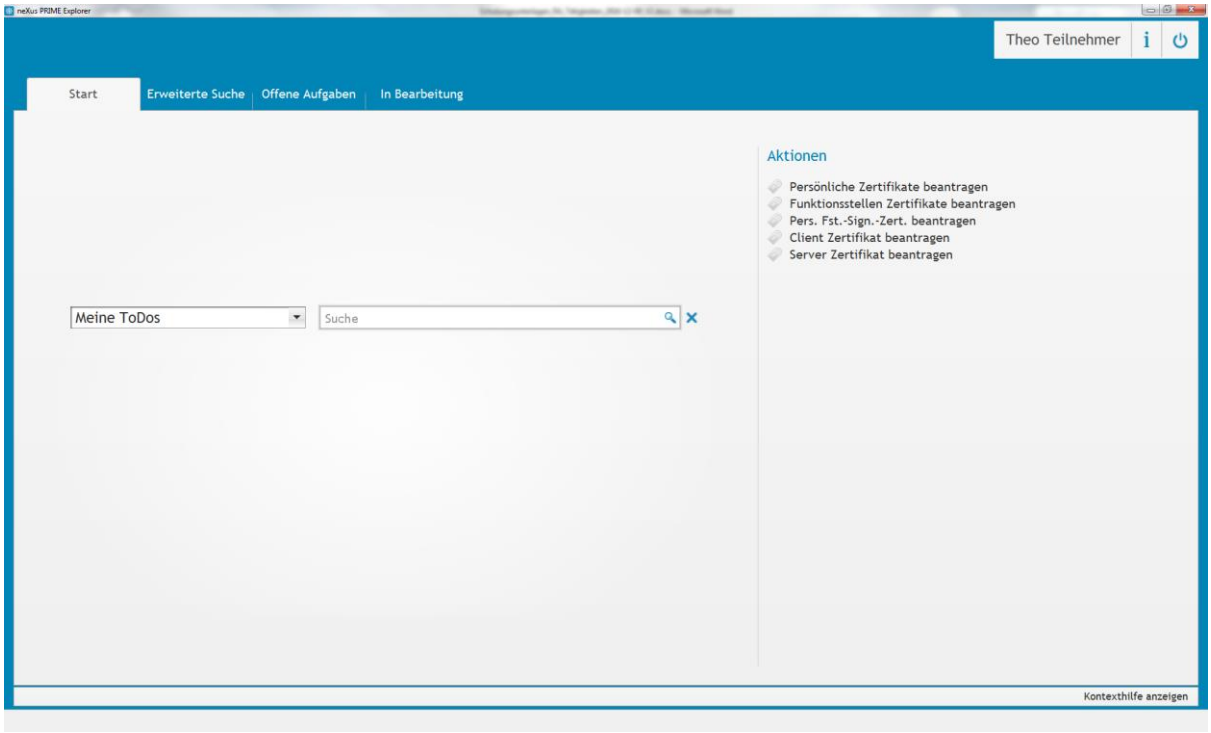
Das Zertifikatsverwaltungssystem prüft nun, ob Sie bereits gültige Zertifikate besitzen und stellt Ihnen bei Bedarf ein neues Signatur-, Verschlüsselungs- oder Authentifizierungszertifikat aus. Das oder die Zertifikat(e) werden anschließend als Anhang einer E-Mail an Ihre E-Mail Adresse geschickt.

Die Zertifikatsdatei wird dabei mit einem Passwort gesichert. Dieses können Sie, wie im Kapitel 3.4 beschrieben, auslesen.

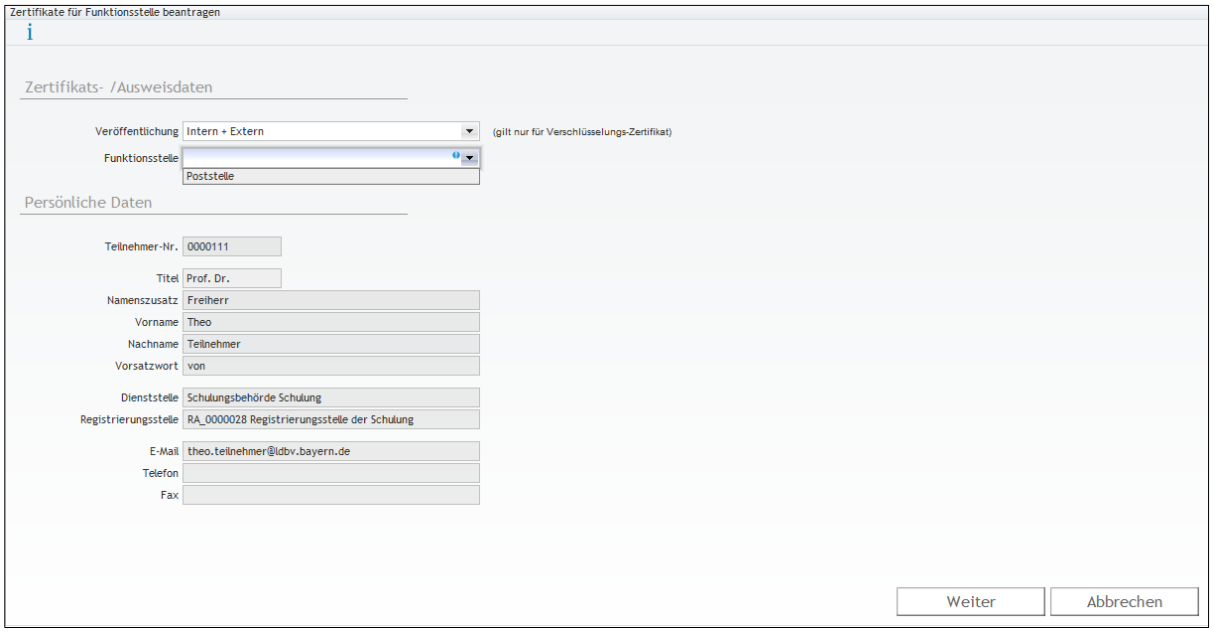
Die Zertifikate haben eine Laufzeit von drei Jahren und werden automatisch verlängert, so dass Sie zwei Wochen vor Ablauf ein neues Zertifikat per E-Mail zugeschickt bekommen.

3.3.2 Funktionsstellenzertifikate

Rufen Sie auf der Startseite unter **Aktionen** den Punkt **„Funktionsstellen Zertifikate beantragen“** auf.



Wählen Sie nun noch die gewünschte **Veröffentlichung** für das Verschlüsselungszertifikat sowie die Funktionsstelle, auf die sich der Zertifikatsantrag bezieht, aus. **Intern** bedeutet, dass das Zertifikat nur im Behördennetz abrufbar sein wird. **Intern + Extern** erwirkt zudem eine Veröffentlichung im Internet.



Das Zertifikatsverwaltungssystem prüft nun, ob Sie bereits gültige Zertifikate besitzen und stellt Ihnen bei Bedarf ein neues Verschlüsselungs- oder Authentifizierungszertifikat aus. Das oder die Zertifikat(e) werden anschließend als Anhang einer E-Mail an die E-Mail Adresse des Verantwortlichen geschickt.

Die Zertifikatsdatei wird dabei mit einem Passwort gesichert. Dieses können Sie, wie im Kapitel 3.4 beschrieben, auslesen.

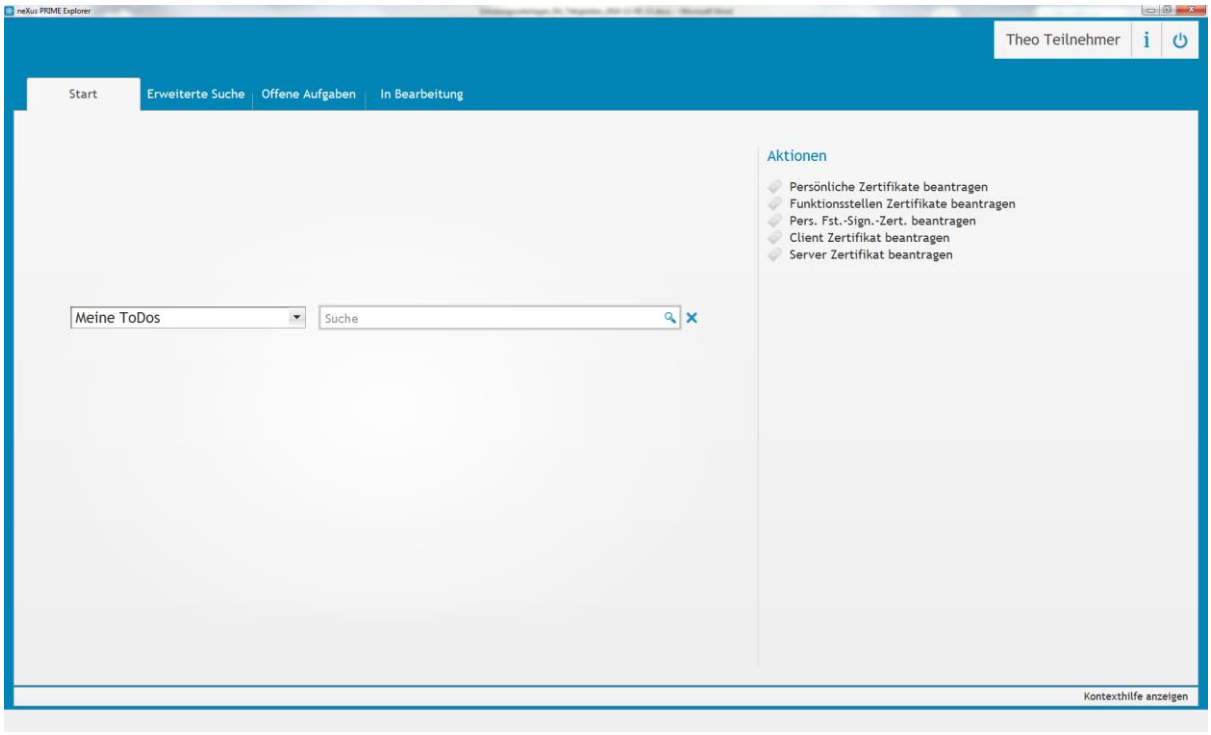
Die Zertifikate haben eine Laufzeit von drei Jahren und werden automatisch verlängert, so dass Sie zwei Wochen vor Ablauf ein neues Zertifikat per E-Mail zugeschickt bekommen.

3.3.2.1 Allgemeine Signatur

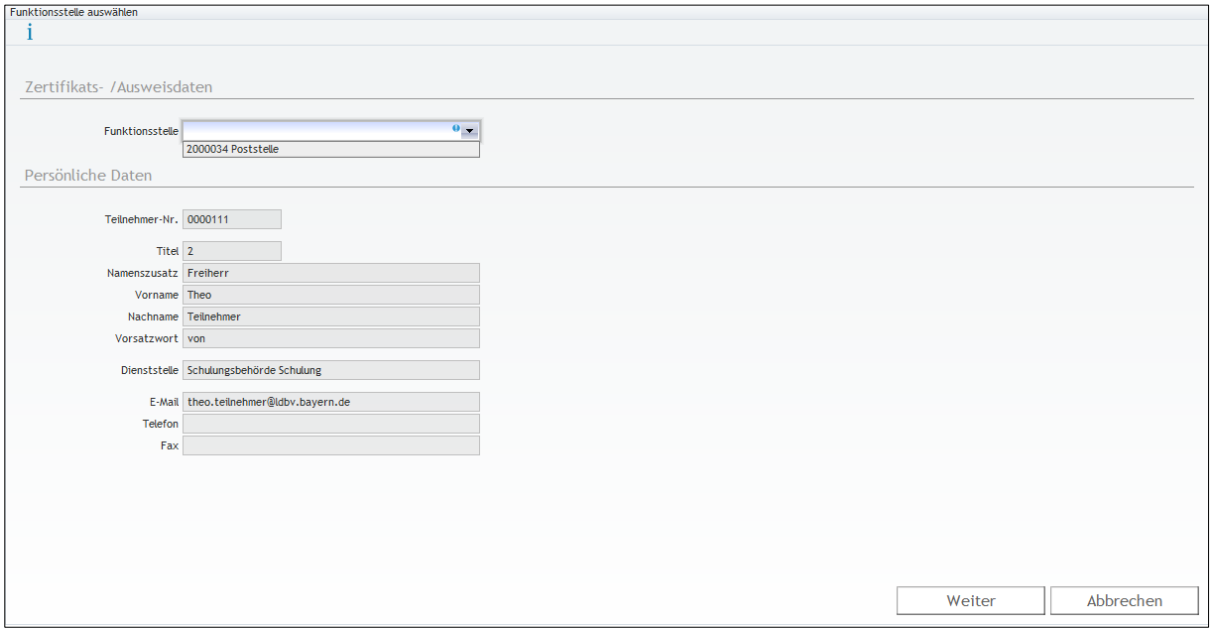
Wenn die ausgewählte Funktionsstelle den Signaturtyp „Allgemeines Signaturzertifikat“ (siehe 1) – Kapitel 2.4.1) hat, wird in dem im vorherigen Kapitel beschriebenen Ablauf auch (bei Bedarf) ein Signaturzertifikat erzeugt.

3.3.2.2 Persönliche Signatur

Wenn Sie von einem Funktionsstellenverantwortlichen für eine oder mehrere Funktionsstellen vom Typ „Persönliches Signaturzertifikat“ (siehe 2) - Kapitel 2.4.1) berechtigt wurden (siehe Kapitel 3.1.1), rufen Sie auf der Startseite unter **Aktionen** den Punkt **„Pers. Fst.-Sign.-Zert. beantragen“** auf.



Wählen Sie nun noch die passende Funktionsstelle aus und klicken Sie auf **„Weiter“**.



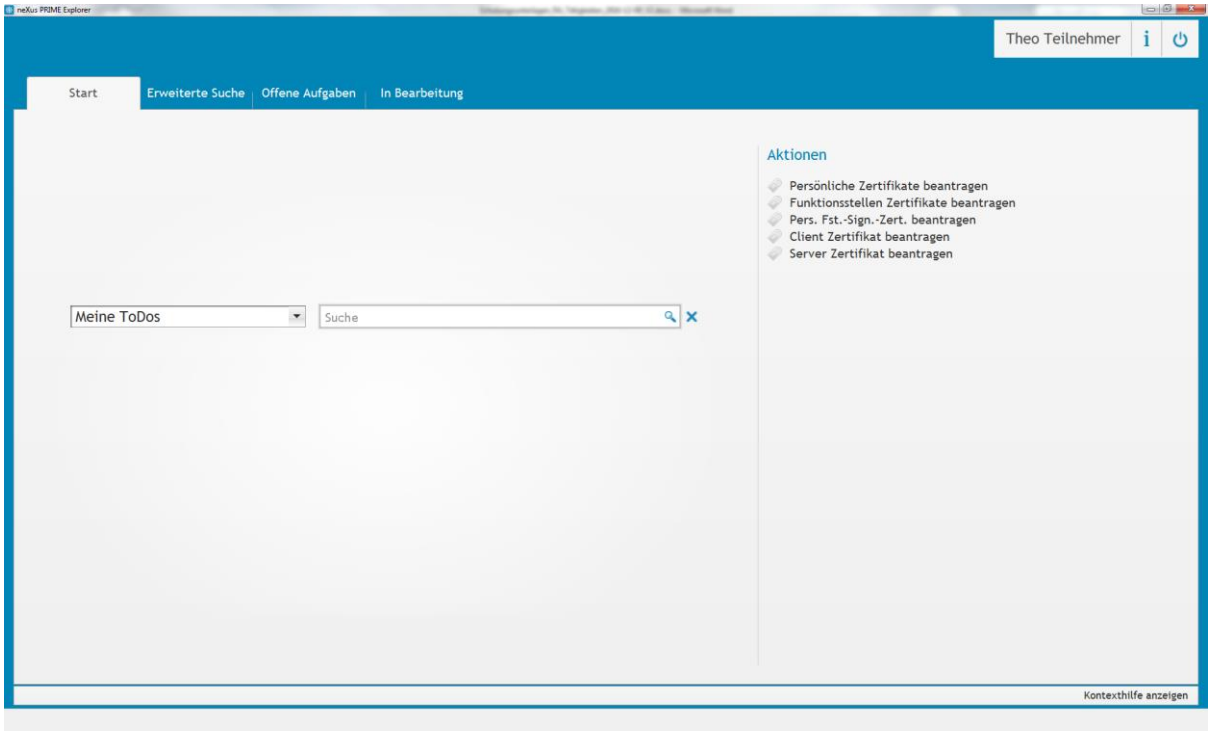
Das Zertifikatsverwaltungssystem prüft nun, ob Sie bereits ein gültiges Signaturzertifikat für diese Funktionsstelle besitzen. Ist das nicht der Fall, wird ein neues Signaturzertifikat generiert und anschließend als Anhang einer E-Mail an die E-Mail Adresse des Verantwortlichen geschickt.

Die Zertifikatsdatei wird dabei mit einem Passwort gesichert. Dieses können Sie, wie im Kapitel 3.4 beschrieben, auslesen.

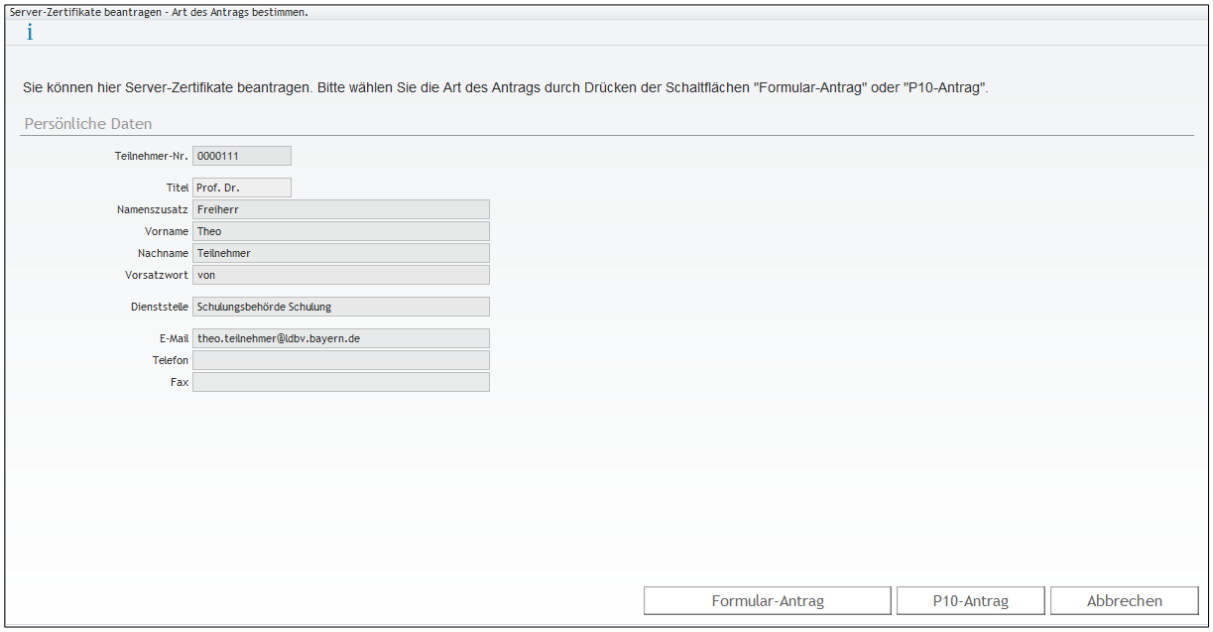
Das Zertifikat hat eine Laufzeit von drei Jahren und wird automatisch verlängert, so dass Sie zwei Wochen vor Ablauf ein neues Zertifikat per E-Mail zugeschickt bekommen.

3.3.3 Serverzertifikate

Rufen Sie auf der Startseite unter **Aktionen** den Punkt **„Server Zertifikat beantragen“** auf.



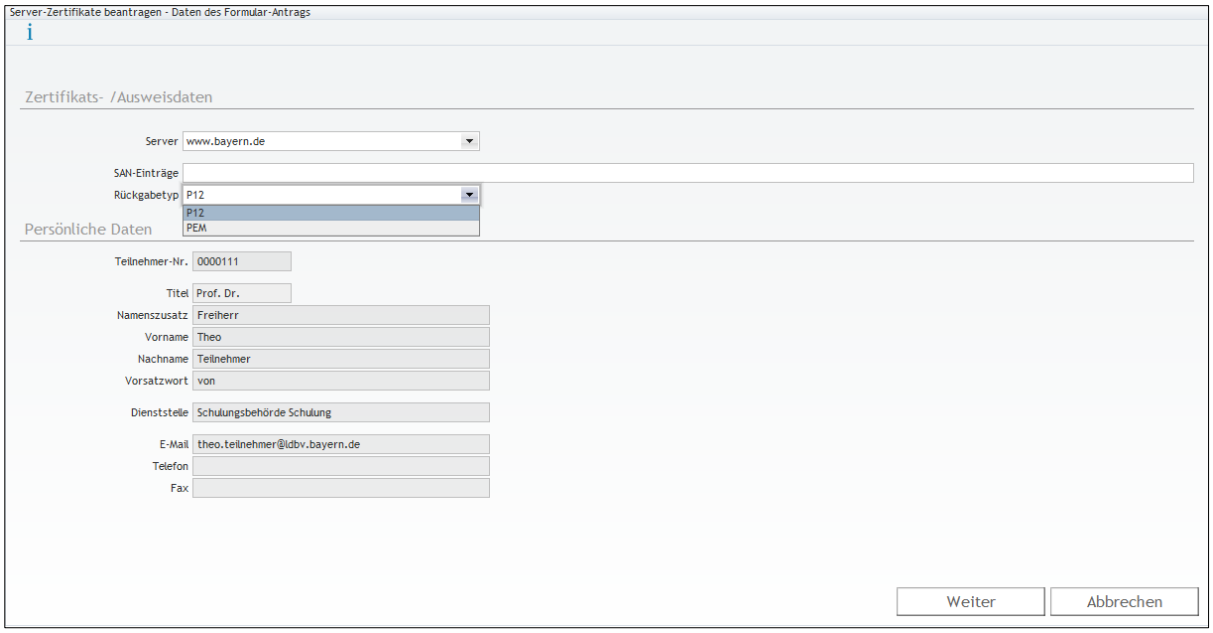
Als nächsten Schritt muss durch Klick auf den entsprechenden Button entschieden werden, ob ein Request (P10-Antrag) eingereicht oder das Serverzertifikat mit zentraler Schlüsselgenerierung (Formular-Antrag) erzeugt werden soll.



Formular-Antrag:

Beantragung unter Angabe des DNS-Namen des Servers. Optional ist es möglich weitere URLs oder IP Adressen im Feld *SAN-Einträge* anzugeben. Die einzelnen Einträge müssen mittels Semikolon (ohne Leerzeichen) voneinander getrennt werden.

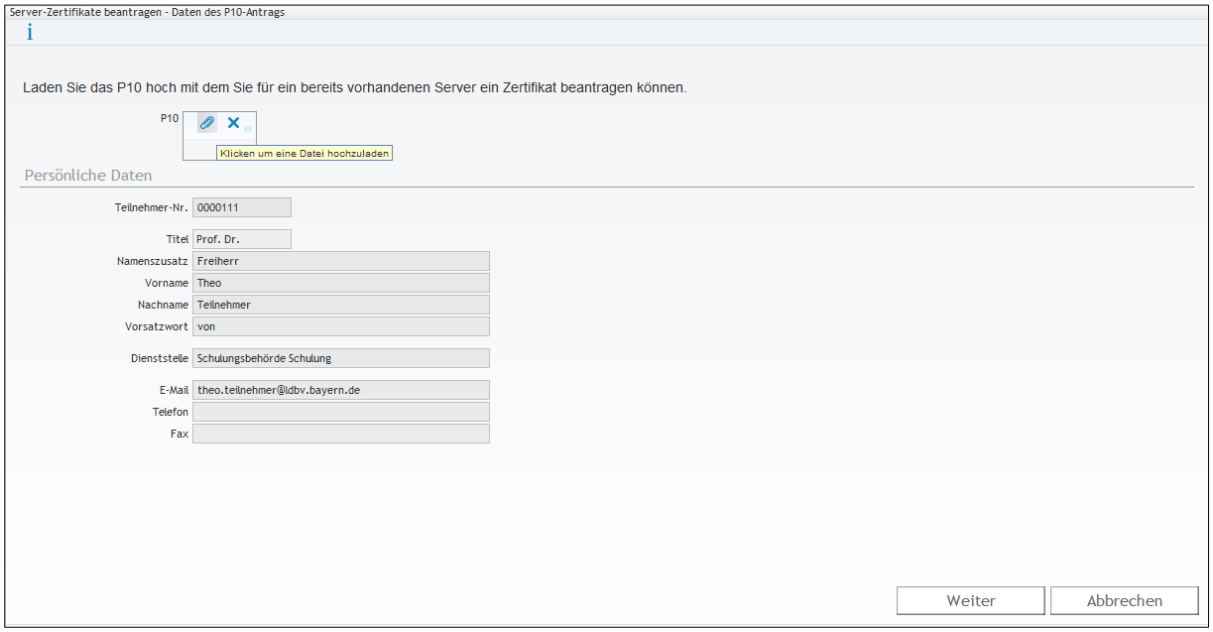
Der private Schlüssel wird durch die CA/Zertifizierungsstelle erstellt und per E-Mail an den Verantwortlichen verschickt. Je nach Auswahl entweder als P12 oder PEM Datei.



P10-Antrag:

Der Zertifikatsantrag erfolgt in diesem Fall über eine PKCS#10-Datei, die im Feld P10 hochgeladen werden kann.

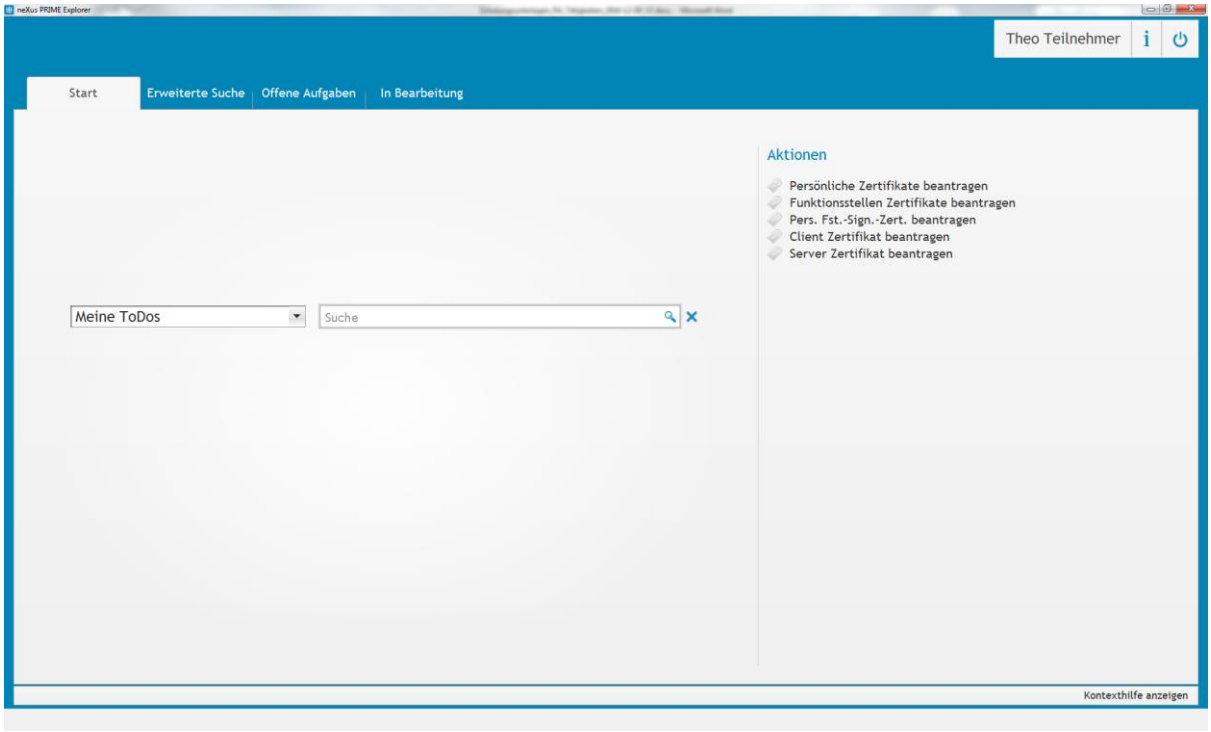
Der private Schlüssel wird vorher clientseitig erzeugt und dort abgelegt. Zusätzlich wird eine Datei erzeugt, die einen PKCS#10-Request enthält. Diese Request-Datei muss dem Zertifikatsantrag beigelegt werden.



Hinweis: Anders als bei einem Formularantrag, wird nach Ablauf der Gültigkeit des Zertifikats kein Antrag zur automatischen Zertifikatsverlängerung angestoßen.

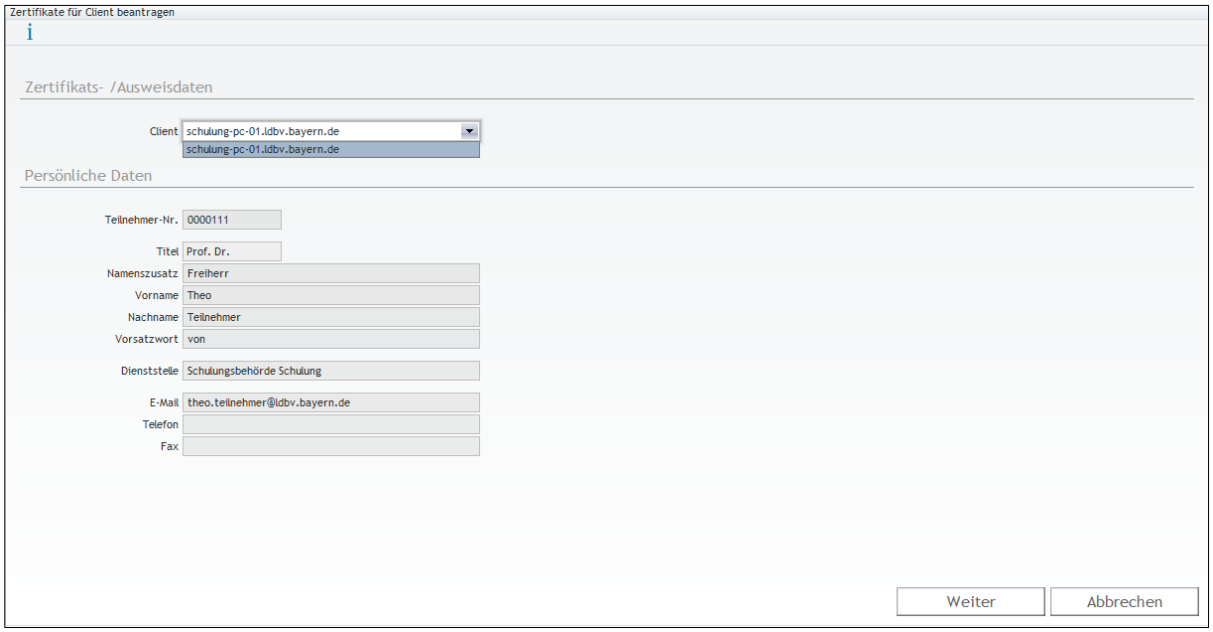
3.3.4 Clientzertifikate

Rufen Sie auf der Startseite unter **Aktionen** den Punkt **„Client Zertifikat beantragen“** auf.



Hinweis: Diese Aktion steht nur zur Verfügung, wenn Sie Zertifikatsverantwortlicher wenigstens eines Clients sind (siehe Kapitel 3.2.1)

Wählen Sie aus der Drop-Down Liste den Client aus, für den Sie ein Zertifikat beantragen möchten und klicken Sie auf **„Weiter“**.



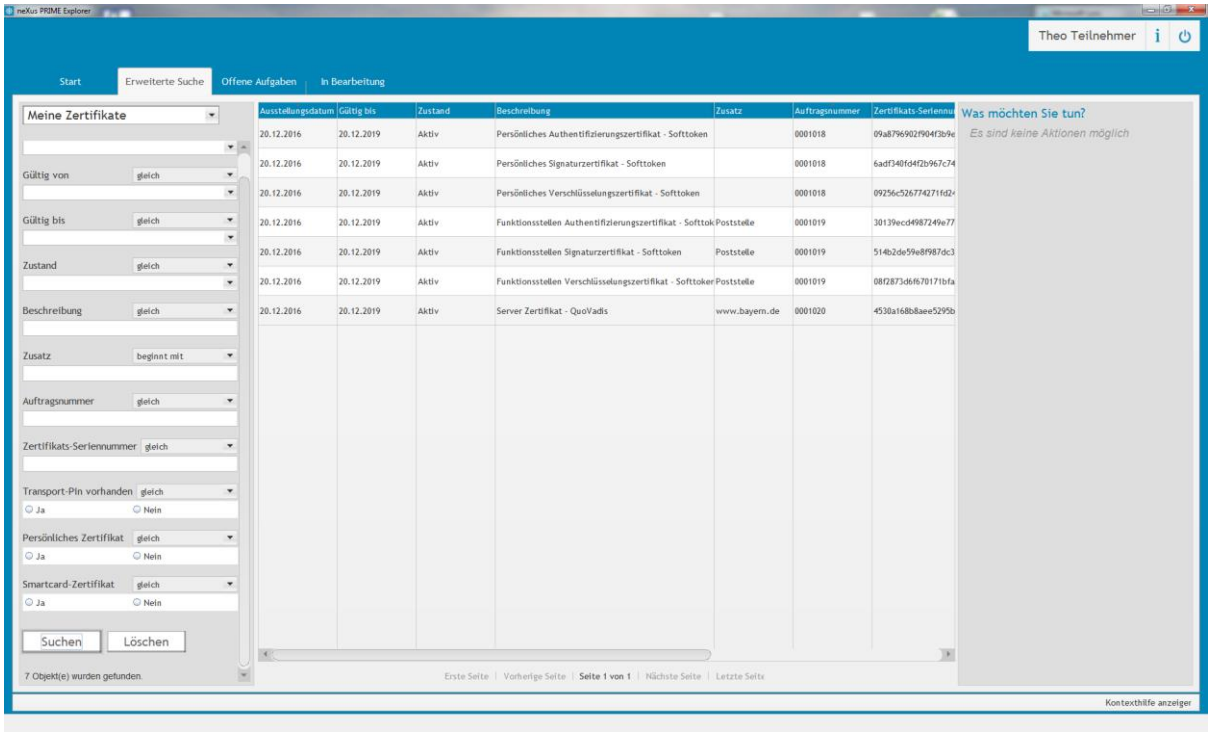
Das Zertifikatsverwaltungssystem prüft nun, ob Sie bereits ein gültiges Zertifikat für diesen Client besitzen. Ist das nicht der Fall, wird ein neues Zertifikat generiert und anschließend als Anhang einer E-Mail an die E-Mail Adresse des Zertifikatsverantwortlichen geschickt.

Die Zertifikatsdatei wird dabei mit einem Passwort gesichert. Dieses können Sie, wie im Kapitel 3.4 beschrieben, auslesen.

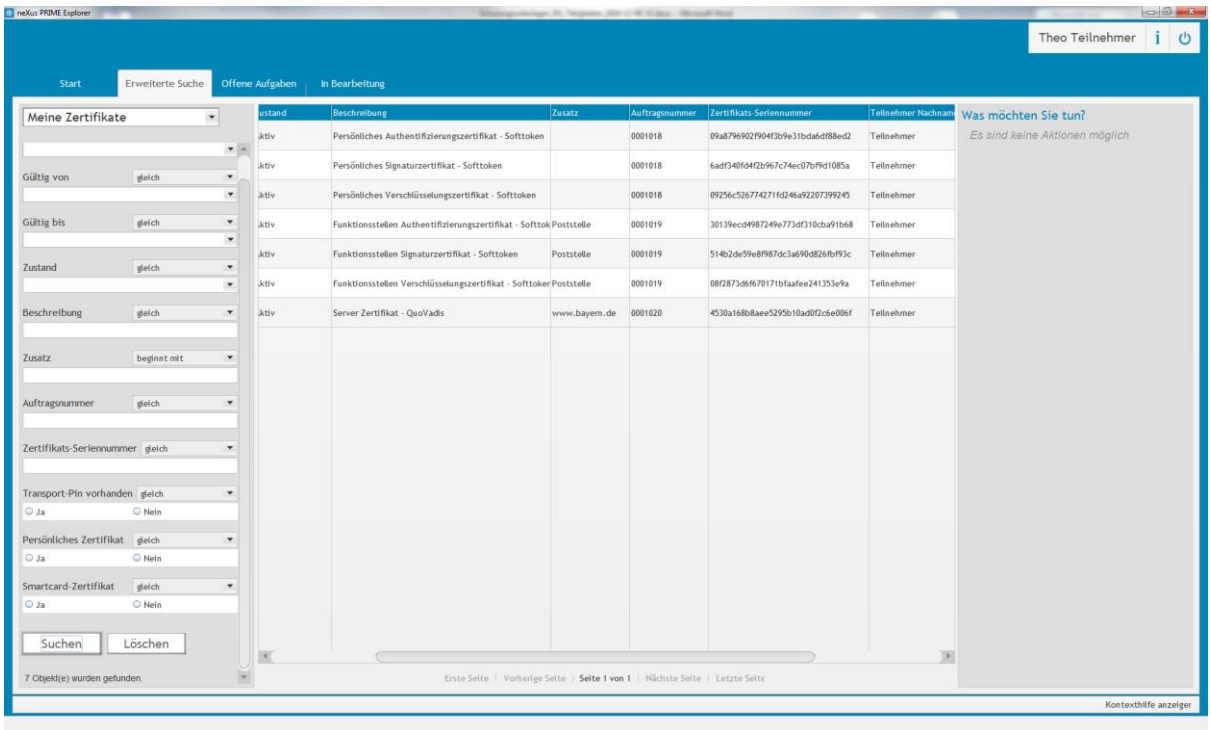
Das Zertifikat hat eine Laufzeit von einem Jahr und wird automatisch verlängert, so dass Sie zwei Wochen vor Ablauf ein neues Zertifikat per E-Mail zugeschickt bekommen.

3.4 Zertifikate anzeigen

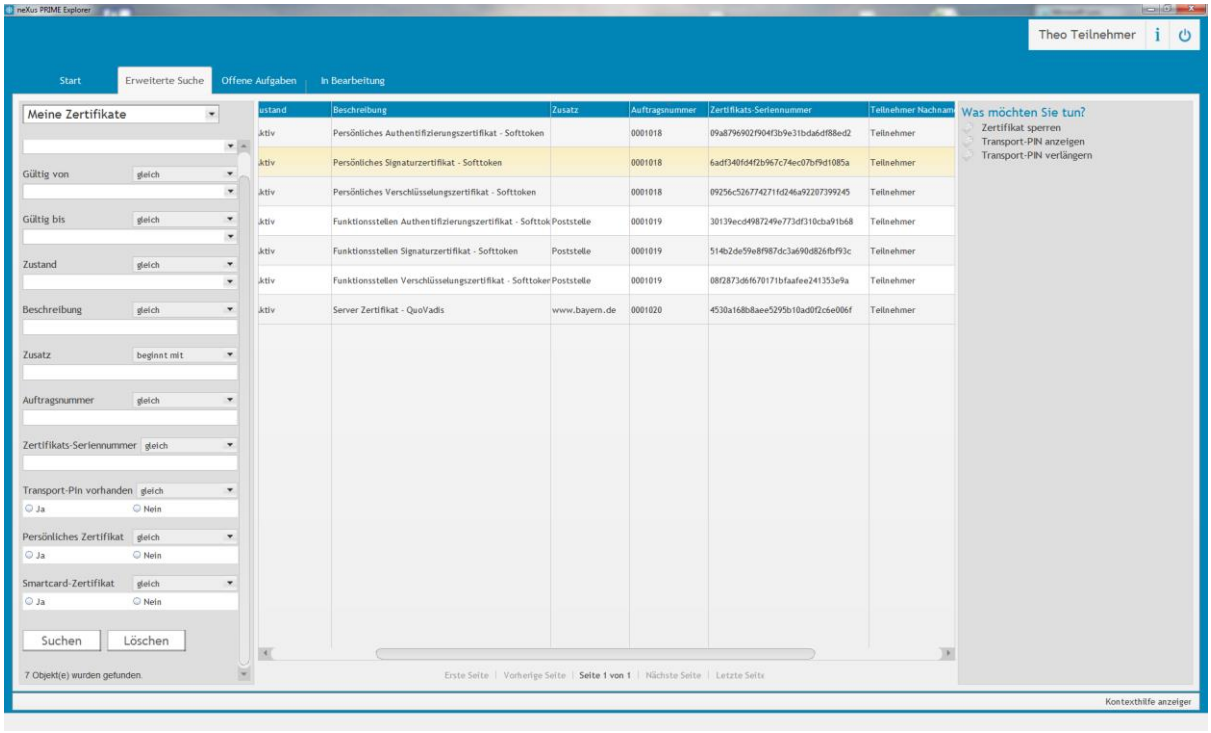
Lassen Sie sich über den **Menüpunkt „Erweiterte Suche“** mit der **Abfrage „Meine Zertifikate“** eine Übersicht aller, Ihnen zugeordneten, Zertifikate anzeigen.



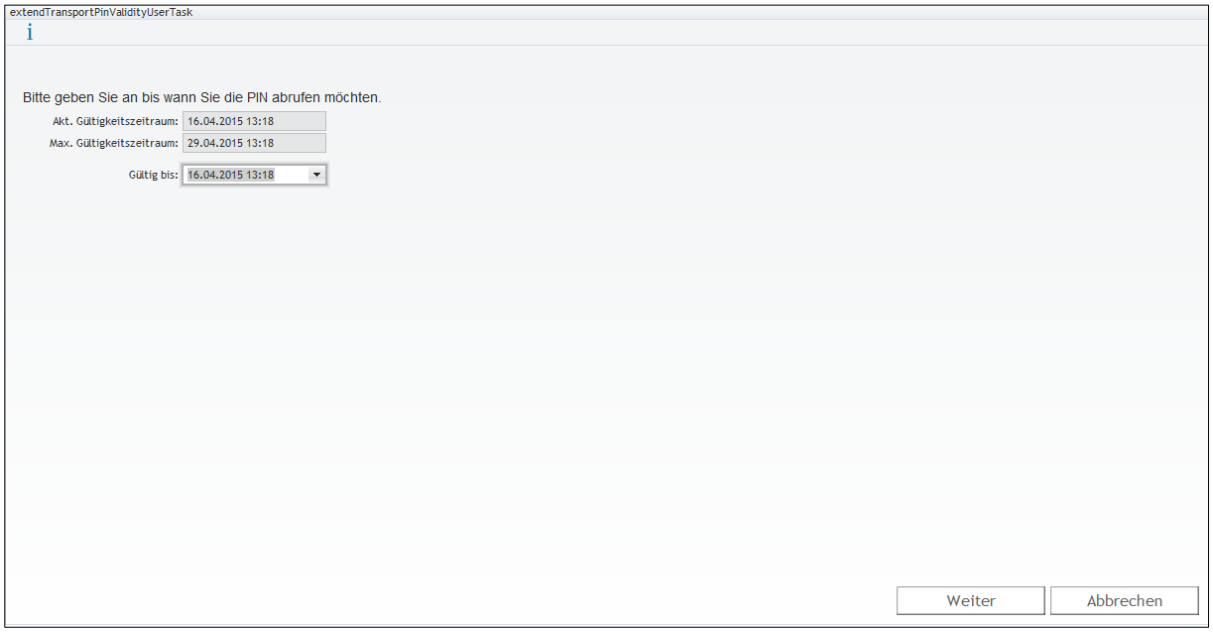
In der Spalte „Zusatz“ wird die Funktionsstellenbezeichnung oder die Server-URL sowie die Clientbezeichnung angezeigt, so dass Sie die Zertifikate leicht voneinander unterscheiden können. Gleichzeitig können Sie das Suchergebnis mit einer Vielzahl von Parametern auf der linken Seite einschränken.



Um sich die Transport-PIN anzeigen zu lassen, markieren Sie ein Zertifikat und klicken auf **„Transport-PIN anzeigen“** unter „Was möchten Sie tun?“.

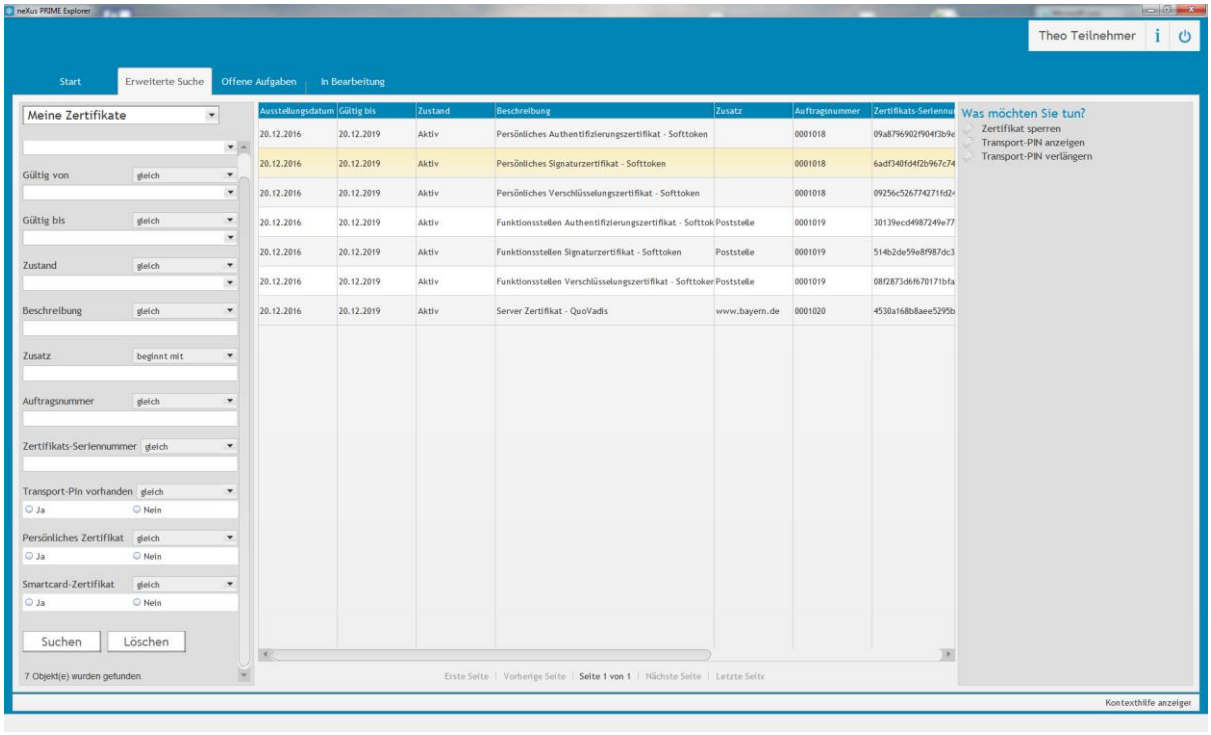


Die Transport-PIN wird nun nach 24h gelöscht. Die Speicherdauer kann um maximal 14 Tage verlängert werden, wenn Sie das Zertifikat markieren und auf **„Transport-PIN verlängern“** klicken.

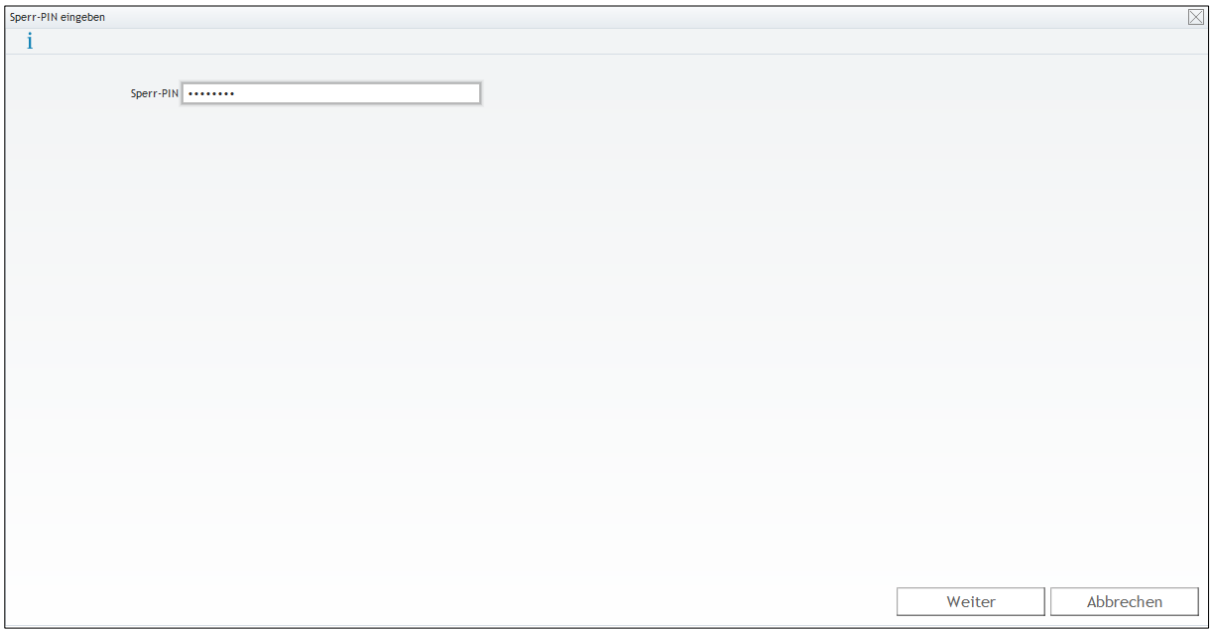

extendTransportPinValidityUserTask
Bitte geben Sie an bis wann Sie die PIN abrufen möchten.
Akt. Gültigkeitszeitraum:
16.04.2015 13:18
Max. Gültigkeitszeitraum:
29.04.2015 13:18
Gültig bis:
16.04.2015 13:18
Weiter
Abbrechen

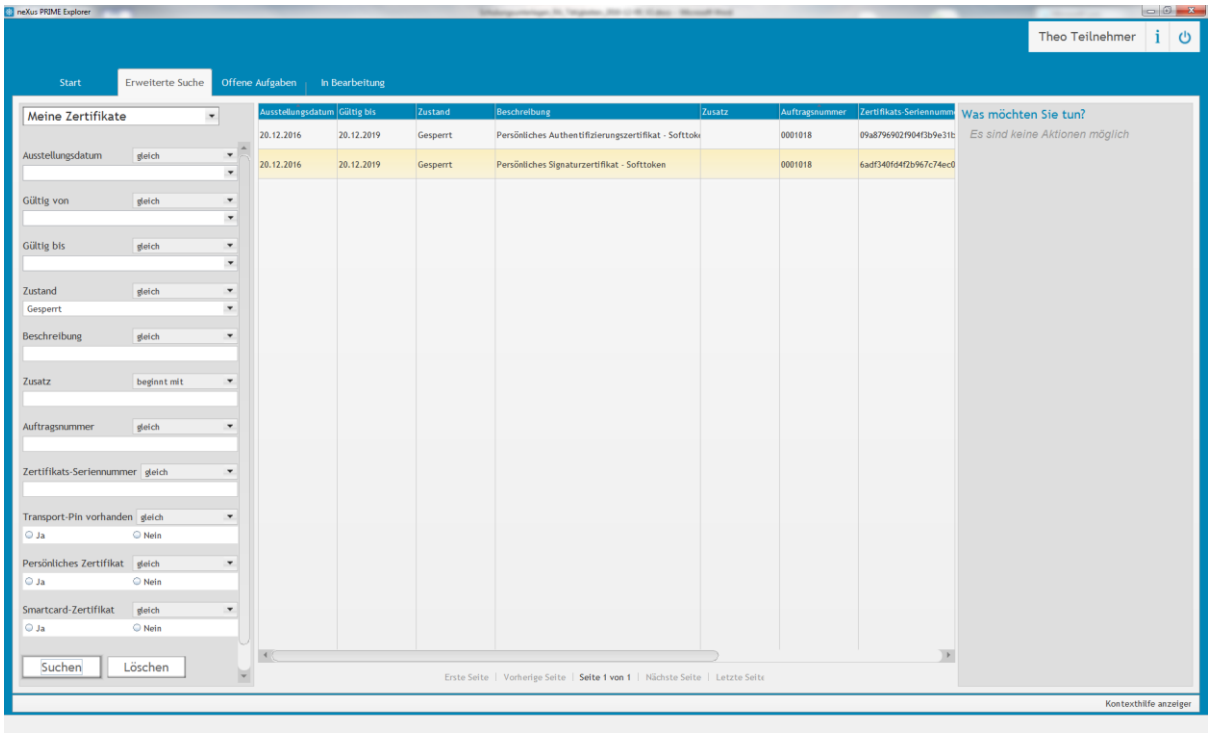
3.5 Zertifikate sperren

Wählen Sie, wie in Kapitel 3.4 beschrieben, ein Zertifikat aus und klicken auf **„Zertifikat sperren“** unter „Was möchten Sie tun?“.



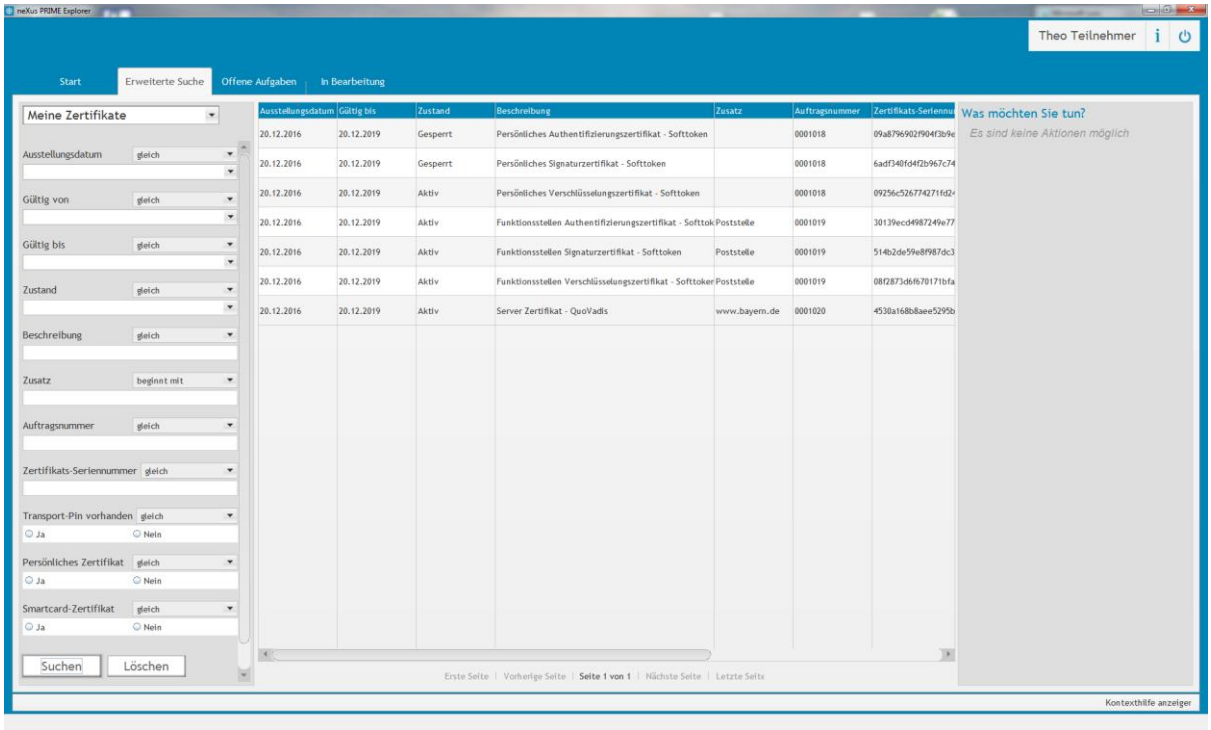
Um das Zertifikat endgültig zu sperren, müssen Sie die Sperr-PIN von Ihrem Registrierungsbrief eingeben.



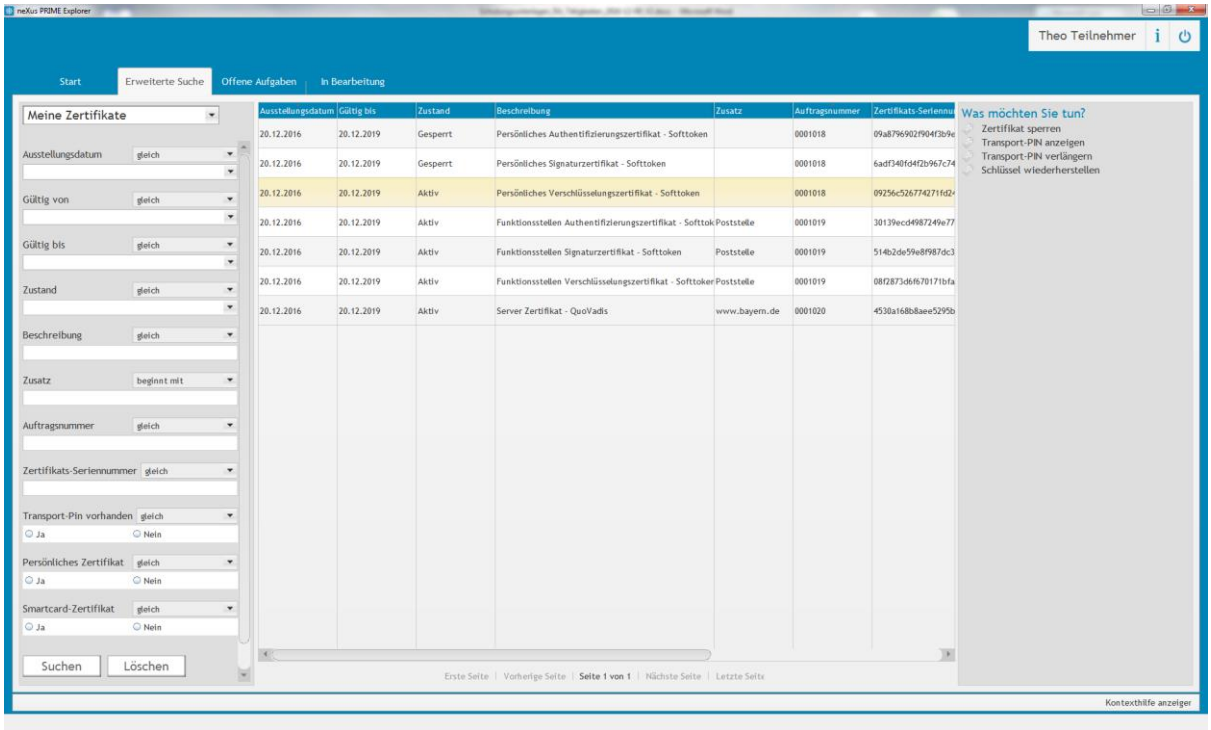

Theo Teilnehmer
Start
Erweiterte Suche
Offene Aufgaben
In Bearbeitung
Meine Zertifikate
Ausstellungsdatum
Gültig von
Gültig bis
Zustand
Gesperrt
Beschreibung
Zusatz
Auftragsnummer
Zertifikats-Seriennummer
Transport-Pin vorhanden
Persönliches Zertifikat
Smartcard-Zertifikat
Suchen
Löschen
Ausstellungsdatum
Gültig bis
Zustand
Beschreibung
Zusatz
Auftragsnummer
20.12.2016
20.12.2019
Gesperrt
Persönliches Authentifizierungszertifikat - Softtok
0001018
20.12.2016
20.12.2019
Gesperrt
Persönliches Signaturzertifikat - Softtoken
0001018
Was möchten Sie tun?
Es sind keine Aktionen möglich
Kontexthilfe anzeigen

3.6 Schlüsselwiederherstellung (Key Recovery)

Lassen Sie sich über den **Menüpunkt „Erweiterte Suche“** mit der **Abfrage „Meine Zertifikate“** eine Übersicht aller, Ihnen zugeordneten, Zertifikate anzeigen.

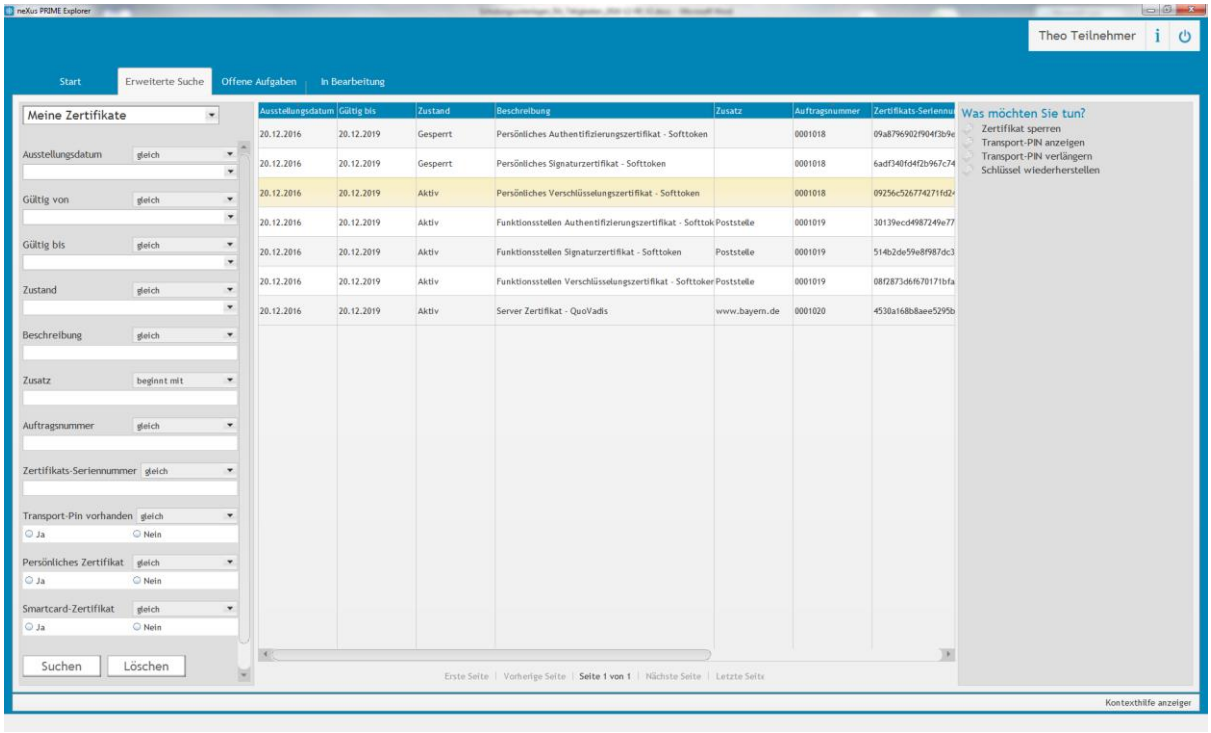


Wenn Sie ein Verschlüsselungszertifikat (ENCRYPTION) markieren, können Sie den Punkt **„Schlüssel wiederherstellen“** unter „Was möchten Sie tun?“ aufrufen.



Anschließend wird das Zertifikat im Hintergrund wiederhergestellt und als Anhang einer E-Mail verschickt.

Auch das wiederhergestellte Zertifikat ist mit einer Transport-PIN verschlüsselt, die Sie, wie im Kapitel 3.4 beschrieben, anzeigen lassen können.



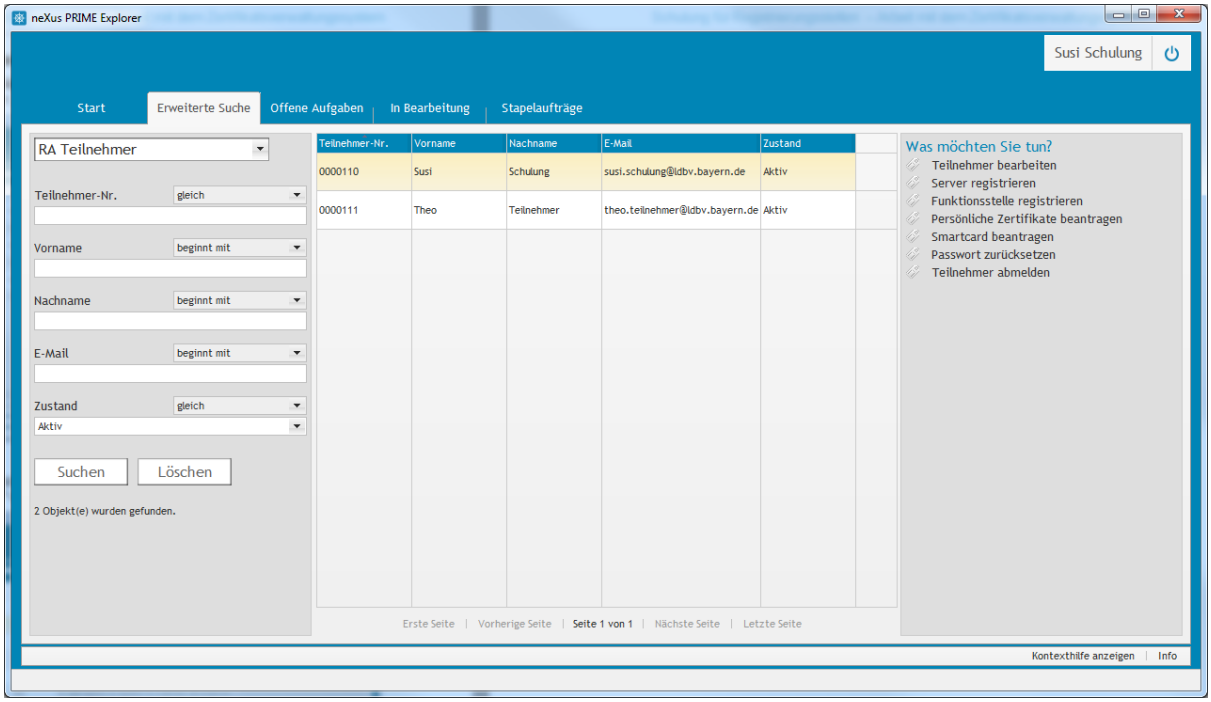
4 Sonderfunktionen

4.1 Schlüsselhinterlegung (Key Escrow)

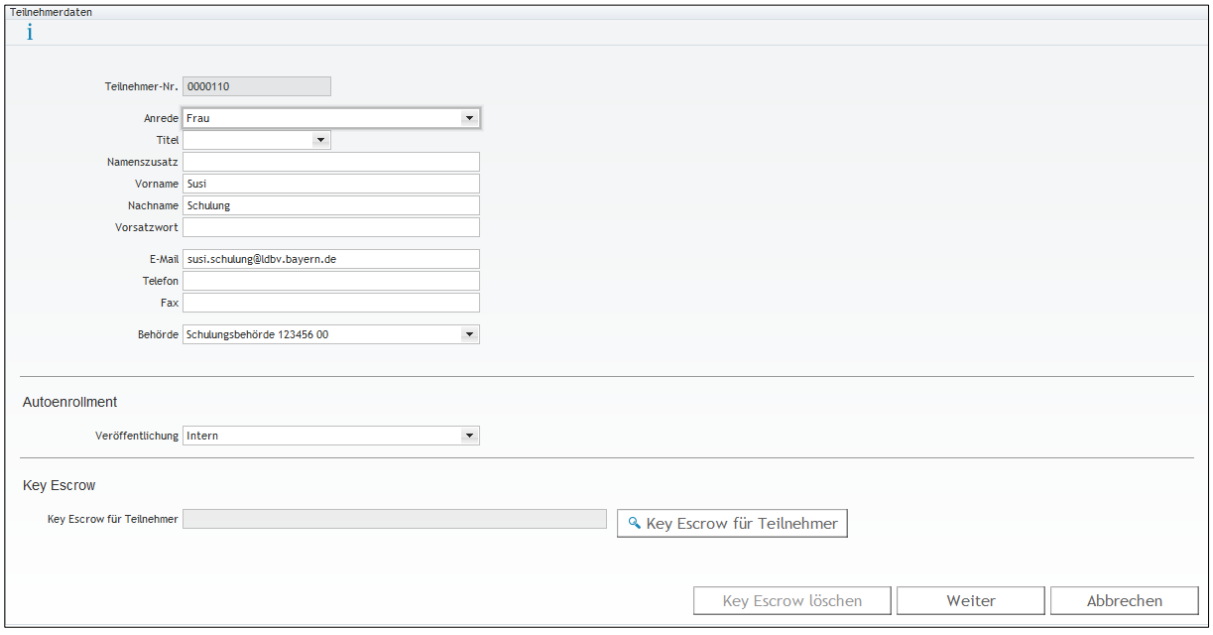
Key Escrow ist ein Key Recovery (siehe Kapitel 3.6) für den Schlüssel eines Dritten. So kann z.B. ein Vorgesetzter auf den Schlüssel eines Mitarbeiters zugreifen, wenn dieser länger verhindert ist.

Da dieser Vorgang äußerst sensibel ist (Zugriff auf den privaten Schlüssel eines Anderen) muss er von einem Mitarbeiter der Registrierungsstelle autorisiert werden.

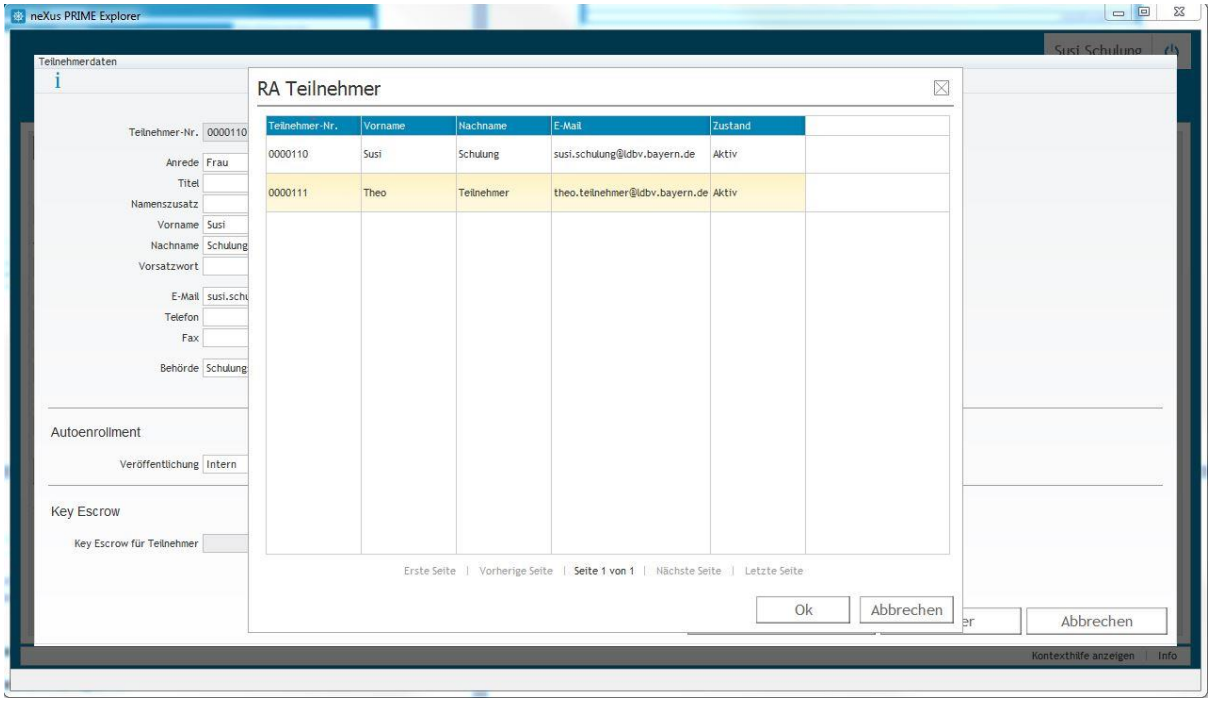
Lassen Sie sich dazu über den **Menüpunkt „Erweiterte Suche“** mit der **Abfrage „RA Teilnehmer“** eine Übersicht aller registrierten Teilnehmer anzeigen und wählen den Teilnehmer aus, der auf das Schlüsselmaterial eines anderen zugreifen soll.



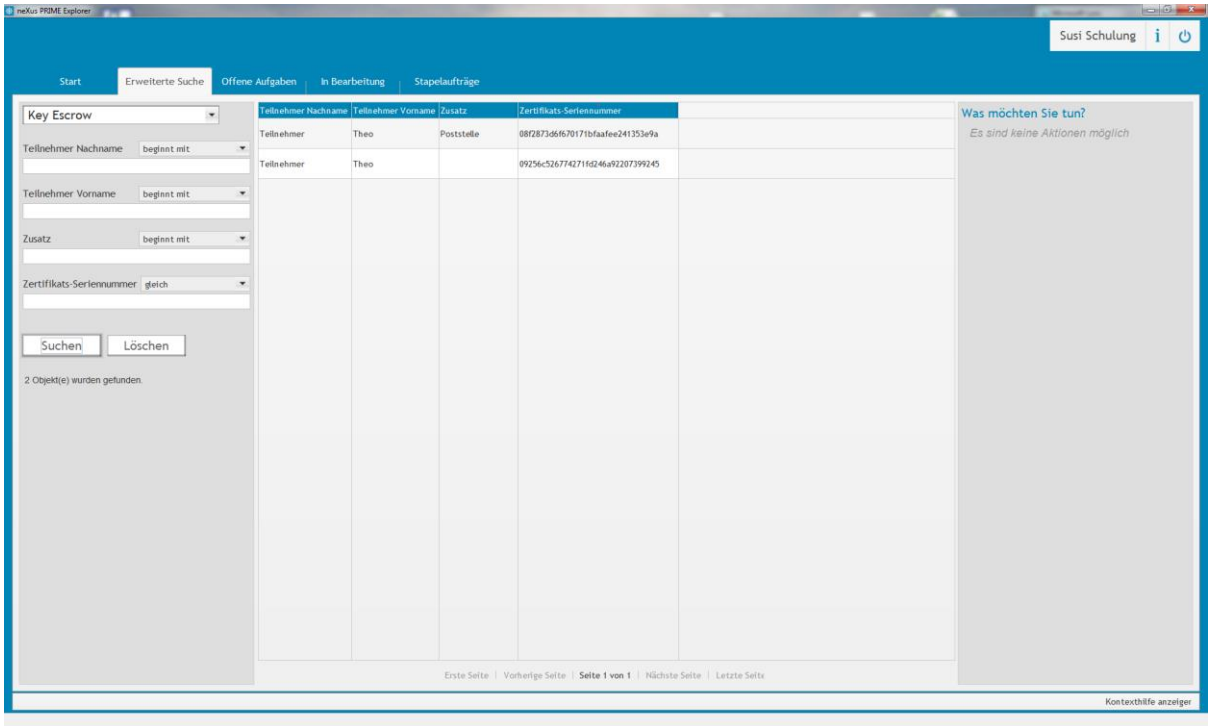
Klicken Sie auf **„Teilnehmer bearbeiten“** unter „Was möchten Sie tun?“.



Klicken Sie weiterhin auf die Schaltfläche **„Key Escrow für Teilnehmer“** um den Teilnehmer auszuwählen, auf dessen Schlüsselmaterial zugegriffen werden soll.



Um die Schlüsselwiederherstellung anzustoßen, muss sich nun der im ersten Schritt berechtigte Teilnehmer anmelden und unter dem **Menüpunkt „Erweiterte Suche“** mit der **Abfrage „Key Escrow“** eine Übersicht aller wiederherstellbaren Zertifikate anzeigen lassen.

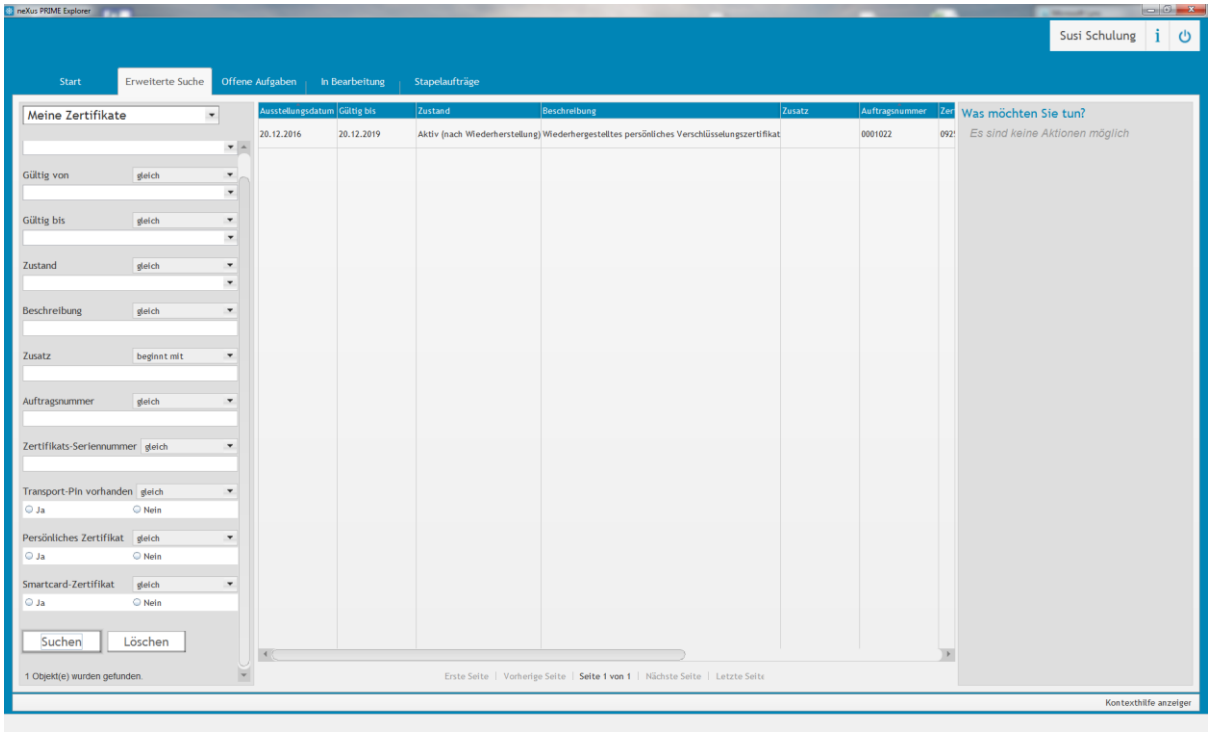


Wählen Sie das wiederherzustellende Zertifikat aus und klicken auf **„Schlüssel wiederherstellen“** unter „Was möchten Sie tun?“.

Hinweis: Falls Sie sich selbst berechtigt haben, müssen Sie sich eventuell neu anmelden um die Zertifikate zu sehen.

Im Hintergrund läuft nun die Wiederherstellung des Zertifikats.

Auch das wiederhergestellte Zertifikat ist mit einer Transport-PIN verschlüsselt, die Sie, wie im Kapitel 3.4 beschrieben, anzeigen lassen können.



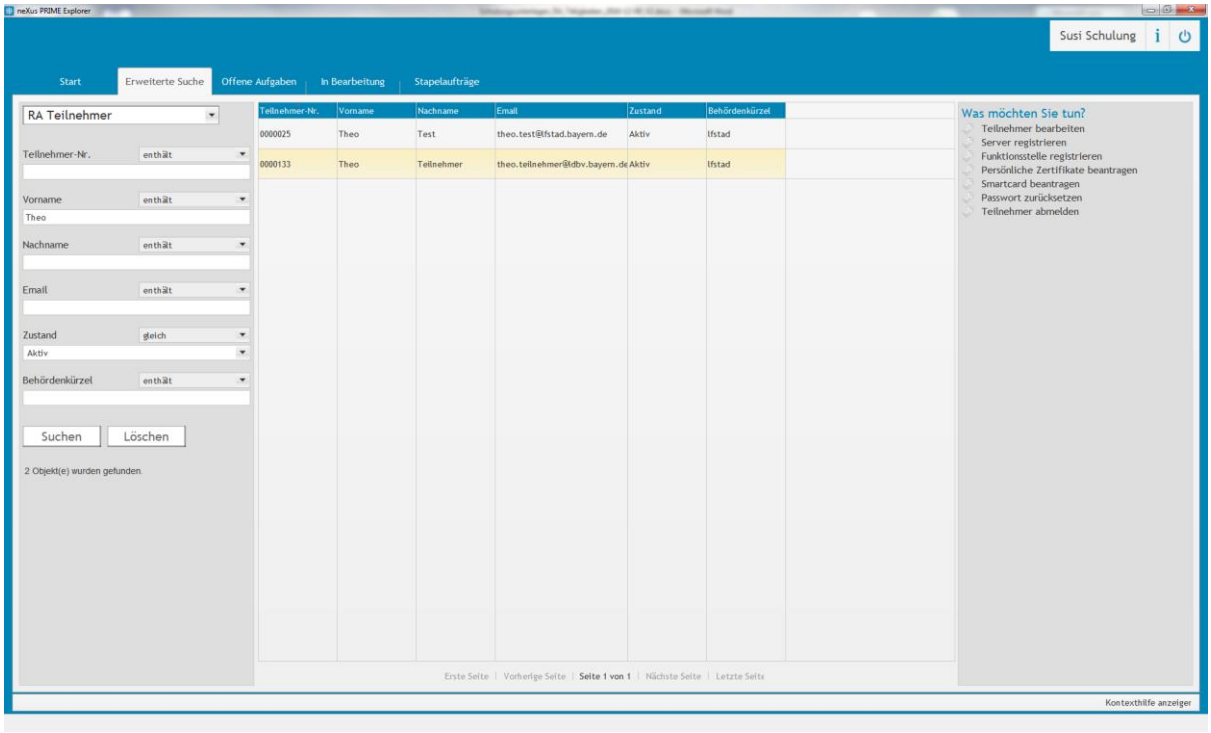
4.2 Zertifikate für einen Teilnehmer beantragen

Als Mitarbeiter einer Registrierungsstelle haben Sie die Möglichkeit Zertifikate für Ihre registrierten Teilnehmer zu beantragen.

Diese Funktion ist für den Fall gedacht, dass Ihre Teilnehmer keinen Zugriff auf das Zertifikatsverwaltungssystem haben (z.B. kein Behördennetzzugriff) und daher die Zertifikate nicht selbst beantragen können.

In dem Fall wird durch die Wurzel-Registrierungsstelle ein Brief mit der Transport-PIN gedruckt und an den Teilnehmer versandt – ein Auslesen der PIN durch den Teilnehmer selbst ist nicht möglich.

Lassen Sie sich dazu über den **Menüpunkt „Erweiterte Suche“** mit der **Abfrage „RA Teilnehmer“** eine Übersicht aller registrierten Teilnehmer anzeigen und wählen den Teilnehmer aus, für den Sie Zertifikate beantragen möchten.



Klicken Sie auf **„Persönliche Zertifikate beantragen“** unter „Was möchten Sie tun?“.

Hinweis: Sie sehen den Punkt nur sofern der Teilnehmer nicht schon alle gültigen Zertifikate besitzt.

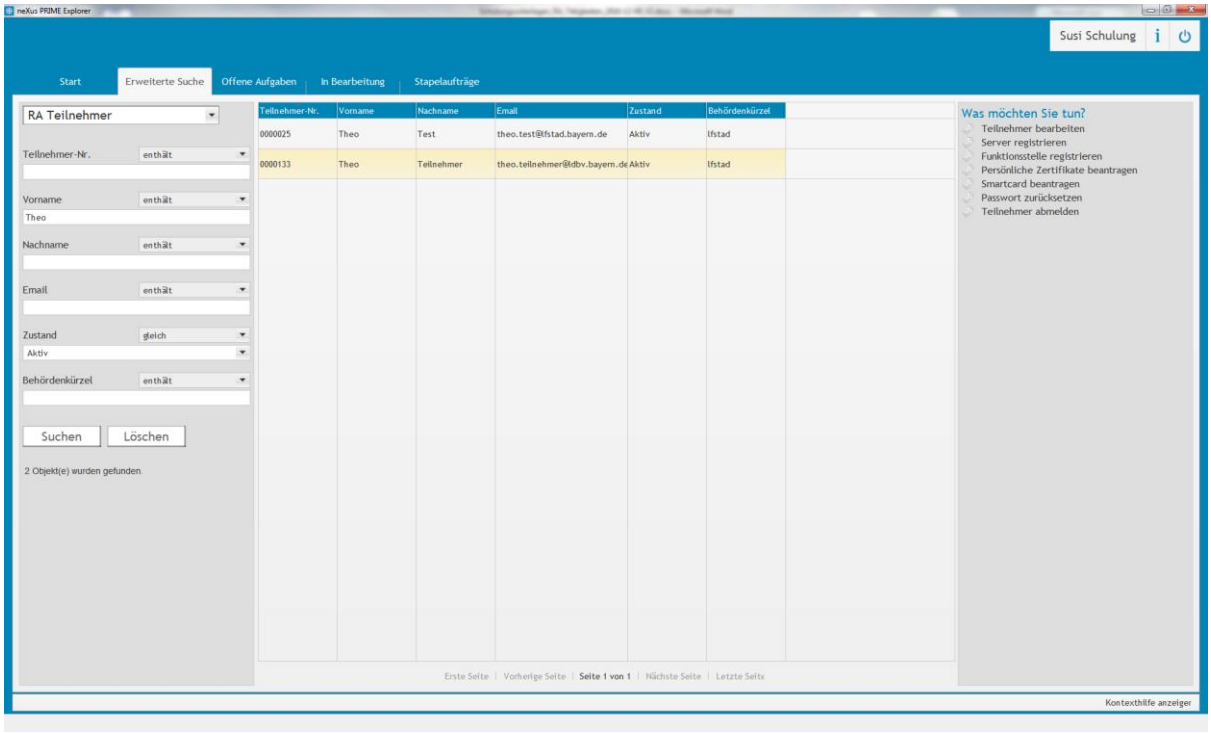
4.3 Zertifikate für die Funktionsstelle eines Teilnehmers beantragen

Als Mitarbeiter einer Registrierungsstelle haben Sie die Möglichkeit Zertifikate für, auf Ihre Teilnehmer registrierten, Funktionsstellen zu beantragen.

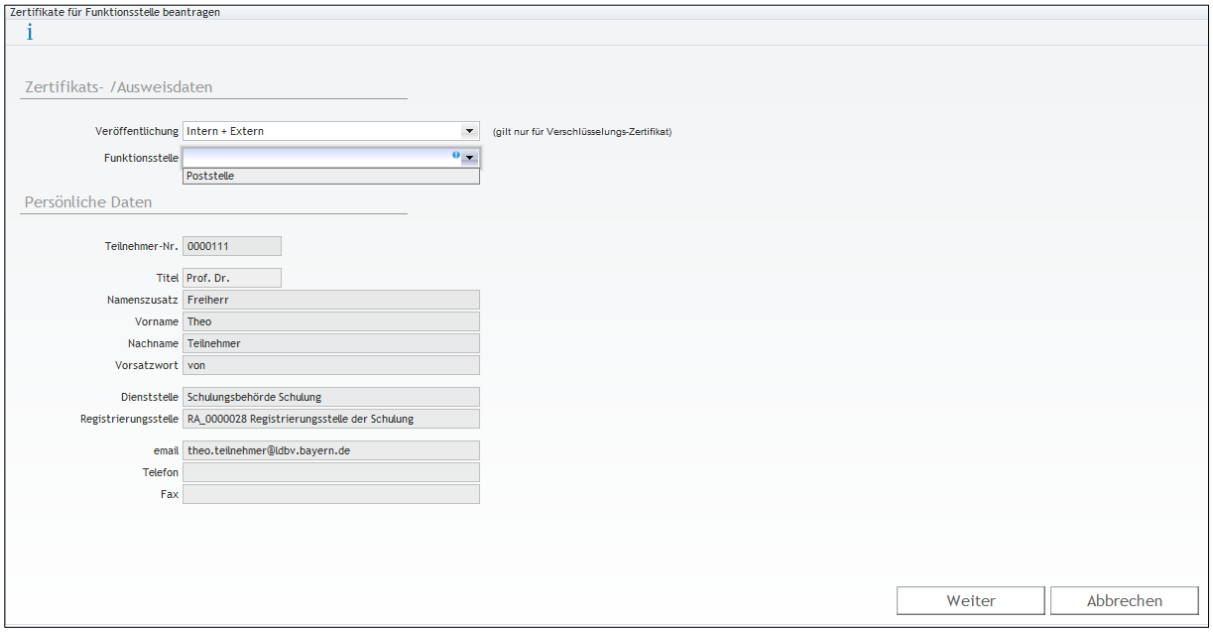
Diese Funktion ist für den Fall gedacht, dass Ihre Teilnehmer keinen Zugriff auf das Zertifikatsverwaltungssystem haben (z.B. kein Behördennetzzugriff) und daher die Zertifikate nicht selbst beantragen können.

In dem Fall wird durch die Wurzel-Registrierungsstelle ein Brief mit der Transport-PIN gedruckt und an den Teilnehmer versandt – ein Auslesen der PIN durch den Teilnehmer selbst ist nicht möglich.

Lassen Sie sich dazu über den **Menüpunkt „Erweiterte Suche“** mit der **Abfrage „RA Teilnehmer“** eine Übersicht aller registrierten Teilnehmer anzeigen und wählen den Teilnehmer aus, für dessen Funktionsstelle Sie Zertifikate beantragen möchten.



Klicken Sie auf **„Funktionsstellen Zertifikate beantragen“** unter „Was möchten Sie tun?“.



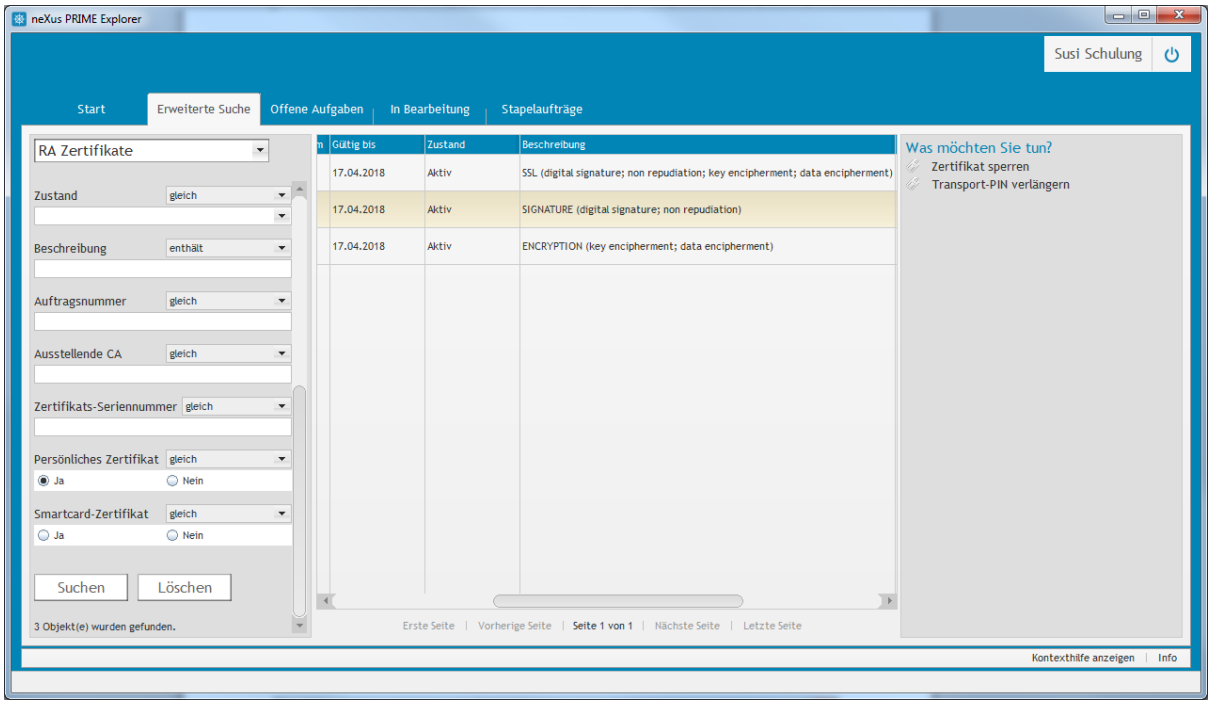
Wählen Sie dann noch die gewünschte Funktionsstelle aus und klicken Sie auf **„Weiter“**.

Hinweis: Sie sehen den Punkt nur sofern dem Teilnehmer Funktionsstellen zugeordnet sind, denen noch Zertifikate fehlen.

4.4 Zertifikate für einen Teilnehmer sperren

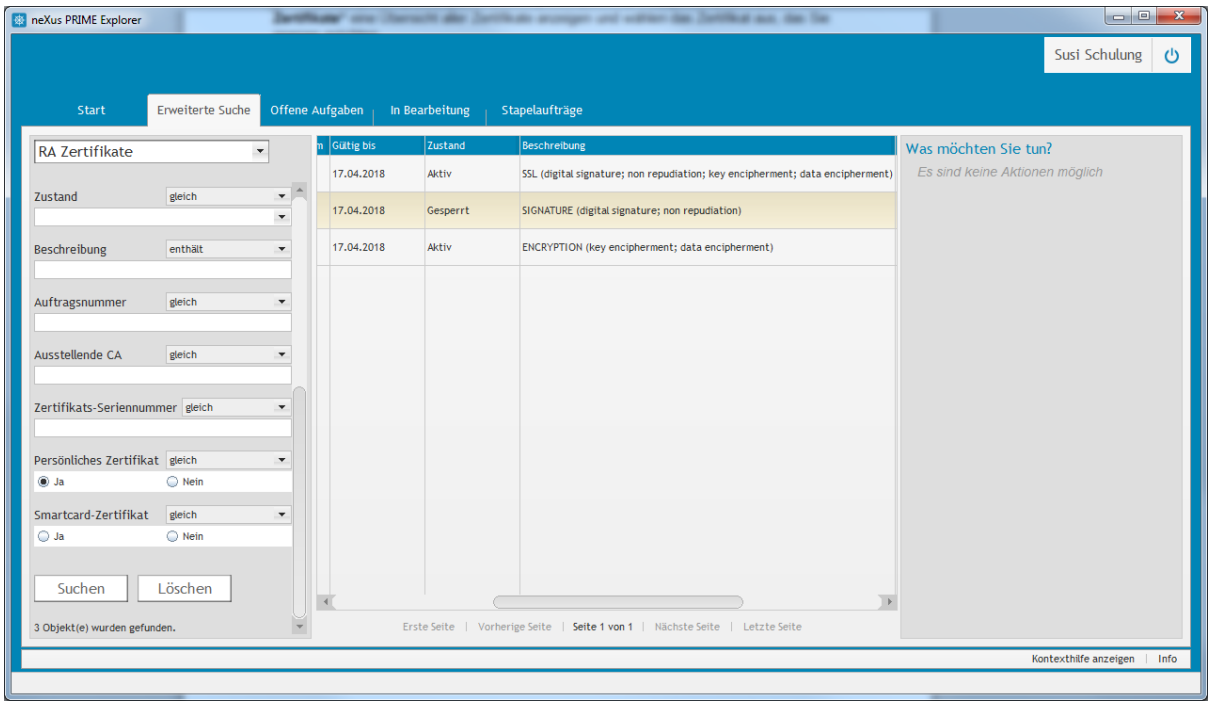
Sie können Zertifikate für Ihre Teilnehmer sperren, wenn diese nicht selbst dazu kommen oder Ihnen ein Sperrgrund (z.B. Missbrauch, privater Schlüssel weitergegeben) bekannt wird.

Lassen Sie sich dazu über den **Menüpunkt „Erweiterte Suche“** mit der **Abfrage „RA Zertifikate“** eine Übersicht aller Zertifikate anzeigen und wählen das Zertifikat aus, das Sie sperren möchten.



Hinweis: Nutzen Sie die Möglichkeit auf der linken Seite die Suchergebnisse zu filtern, da die Ausgabe ansonsten sehr viele Ergebnisse anzeigen wird.

Klicken Sie auf **„Zertifikat sperren“** unter „Was möchten Sie tun?“.



Als Ergebnis hat das Zertifikat den Zustand „Gesperrt“.

5 Smartcards

5.1 Allgemeine Informationen

Persönliche Zertifikate sowie Zertifikate für Funktionsstellen können auf einer Smartcard beantragt werden. Von Smartcards sprechen wir bei speziellen Plastikkarten mit einem Prozessorchip und einem Chip Betriebssystem (COS; z.B. CardOS oder Sm@rtCaféExpert).

Der Vorteil von Smartcards ist, dass die Zertifikate nur mit einer dem Inhaber bekannten persönlichen Identifikations Nummer (PIN) eingesetzt werden können. Diese Vorgehensweise stellt einen deutlichen Sicherheitsgewinn gegenüber dem Einsatz der Zertifikate auf reiner Softwarebasis dar. Softwarezertifikate verfügen über keinerlei Kopierschutz, so dass hier eine höhere Gefahr des Missbrauchs im Vergleich zum Einsatz von Smartcards gegeben ist.

Einen weiteren Vorteil bietet die Win-Logon Funktion, d.h. Sie können sich mittels Smartcard an einem Windows Rechner bzw. einer Windows Domäne anmelden.

5.2 Überblick

5.2.1 Registrierungsstelle für die Smartcard-Beantragung/-Produktion vorbereiten

5.2.1.1 Schritt 1: Smartcard Layout und AD Konnektor vom PKI Support zuweisen lassen

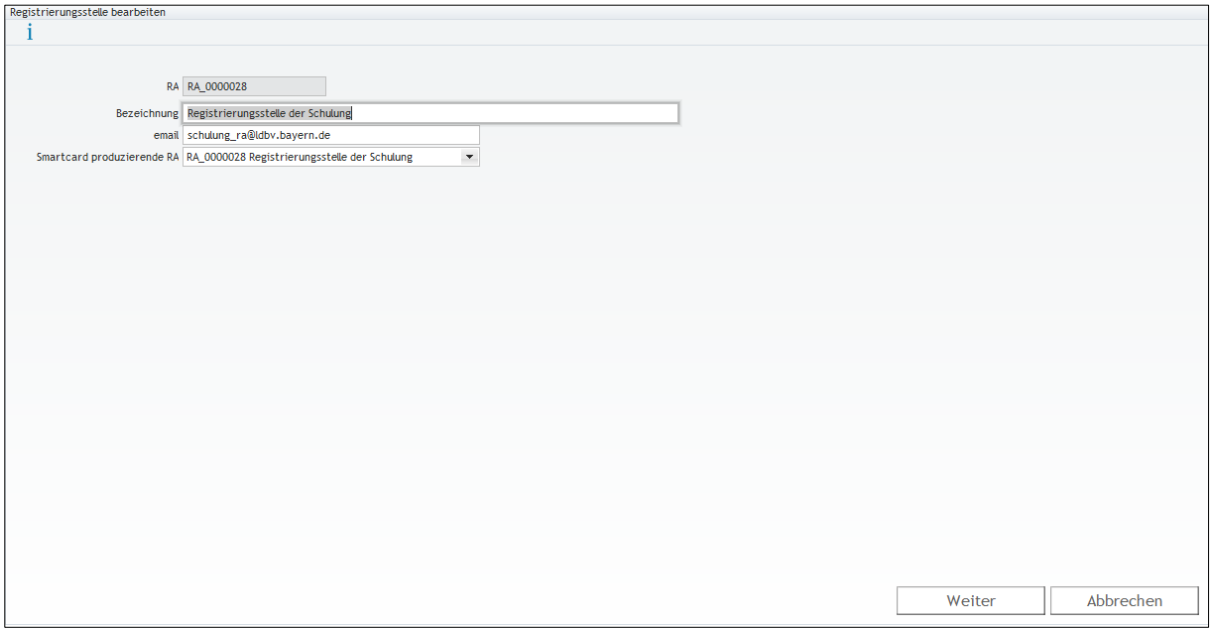
Sie können Ihre Smartcards mit verschiedenen Standard Layouts, einem individuellen Layout oder auch ohne Layout produzieren lassen. In jedem Fall werden bei der Produktion einer Smartcard Zertifikate der Bayern PKI geschrieben.

Eines dieser Zertifikate kann auch für Win-Logon verwendet werden, sofern ein funktionsfähiger AD Konnektor eingerichtet ist. Für die Einrichtung benötigt der PKI-Support eine Kennung, die berechtigt ist, User Objekte auszulesen, sowie den entsprechenden Servernamen des LDAP Servers (z.B. Domänencontroller).

Informieren Sie den PKI Support (pki-support@ldbv.bayern.de) über das gewünschte Layout, ob Win-Logon gewünscht ist und welche Behörden betroffen sind, bevor Sie mit Schritt 2 fortfahren.

5.2.1.2 Schritt 2: RA Stammdaten anpassen

Rufen Sie die Stammdaten Ihrer Registrierungsstelle, wie in Kapitel 2.1 beschrieben, auf.

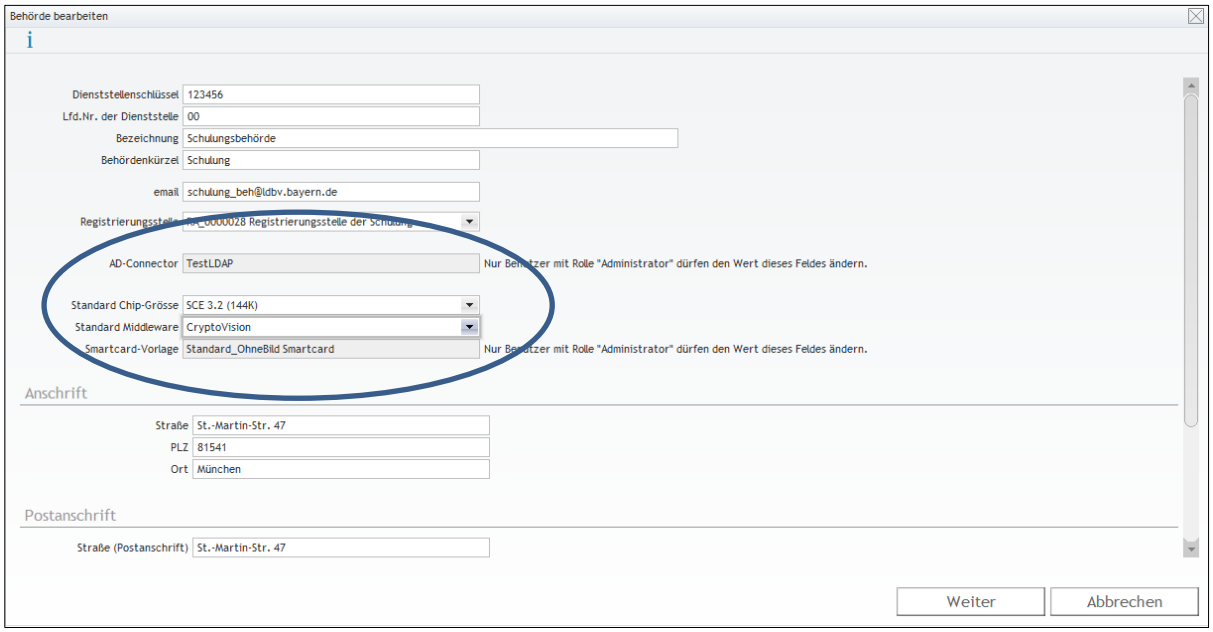


Wenn im Feld „Smartcard produzierende RA“ ihre eigene RA eingetragen ist, produzieren Sie die Smartcards selbst. Alternativ können Sie eine andere RA auswählen, die die Smartcards für Sie produziert. Wählen Sie dazu die gewünschte RA aus der Liste aus und speichern den Vorgang mit **Weiter**.

Hinweis: Unabhängig von der oben getroffenen Einstellung können Sie die Re-Initialisierung, d.h. das erneute Beschreiben einer vorhandenen Smartcard mit Zertifikaten, immer selbst durchführen.

5.2.1.3 Schritt 3: Behörden Stammdaten anpassen

Rufen Sie die Stammdaten aller Behörden, für die die Einstellungen gelten sollen, wie in Kapitel 2.2.2 2.1beschrieben, auf.



Die Felder „AD-Connector“ und „Smartcard-Vorlage“ werden durch den PKI Support nach Ihren Vorgaben konfiguriert (siehe Kapitel 5.2.1.1).

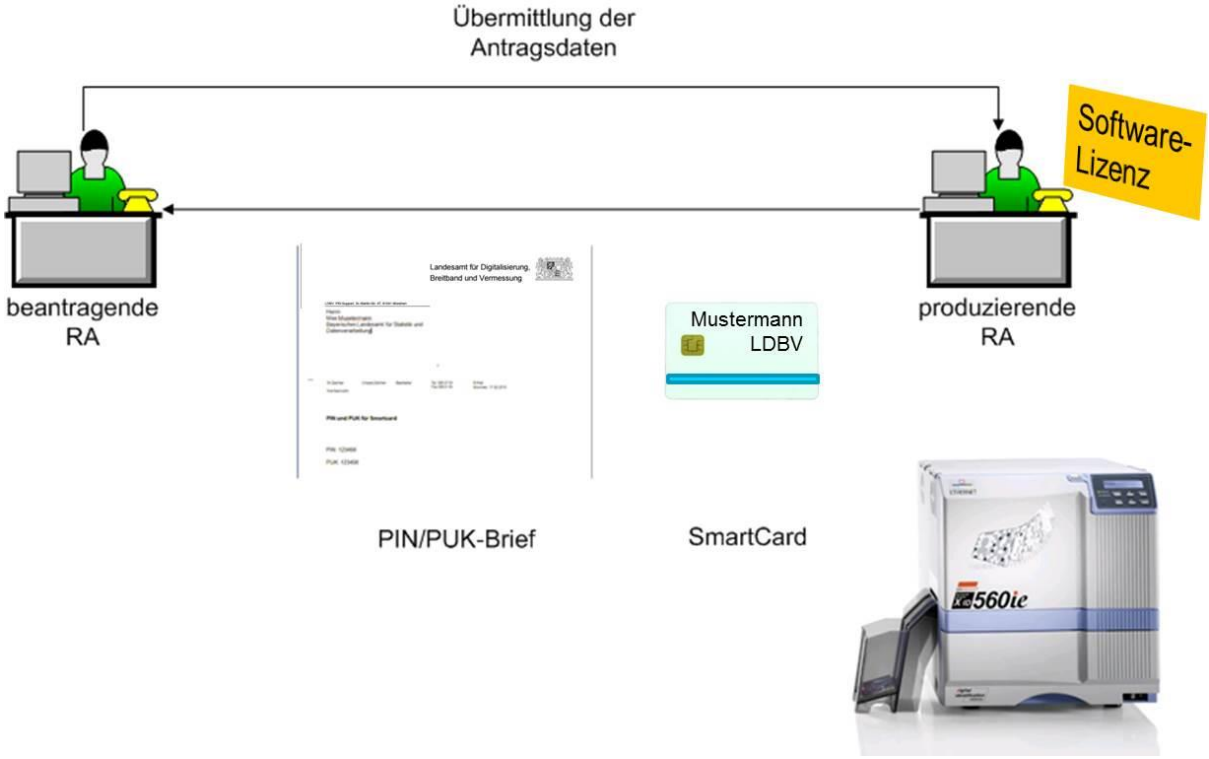
Im Feld „Standard Chip-Größe“ wählen Sie den in Ihrer Behörde verwendeten Smartcard Chip aus. Dieser entscheidet über die maximale Anzahl an Zertifikaten, die das System auf eine Smartcard zu schreiben versucht.

Bei der „Standard Middleware“ wählen Sie die Middleware aus, die Sie verwenden. Mit dieser Middleware wird die Smartcard Produktion durchgeführt.

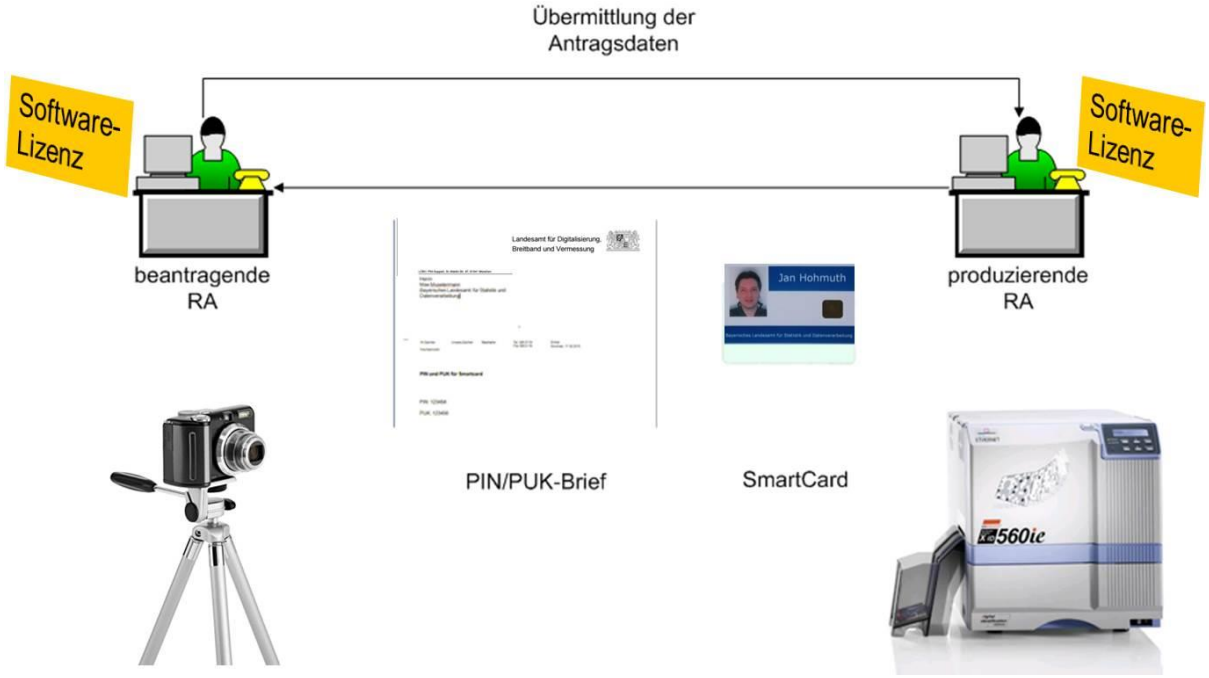
5.2.2 Produktionsvarianten

5.2.2.1 Variante 1: Kodierung des Chips

5.2.2.2 Variante 2: Variante 1 mit optischer Personalisierung



5.2.2.3 Variante 3: Variante 2 mit Bild oder Unterschrift



5.2.3 Kosten

Die Kosten für die Registrierungsstelle hängen von der gewählten Produktionsvariante (siehe 5.2.2) ab.

Für die Produktionsvariante 1 (siehe 5.2.2.1) ist keine weitere Software bzw. Lizenz notwendig.

Die Produktionsvarianten 2 (siehe 5.2.2.2), sprich mit Bedrucken der Karte, sowie 3 (siehe 5.2.2.3), sprich Aufnahme von Bild/Unterschrift und Bedrucken der Karte, benötigen die Installation des Nexus CardSDK sowie eine Lizenz mit dem entsprechenden Funktionsumfang. Die Lizenz für beantragende RAs wird für staatliche Behörden über das IT-DLZ bereitgestellt. Die Lizenz für produzierende RAs ist direkt beim Hersteller Nexus zu erwerben. Kommunale Behörden müssen jegliche Lizenz ebenfalls beim Hersteller Nexus erwerben.

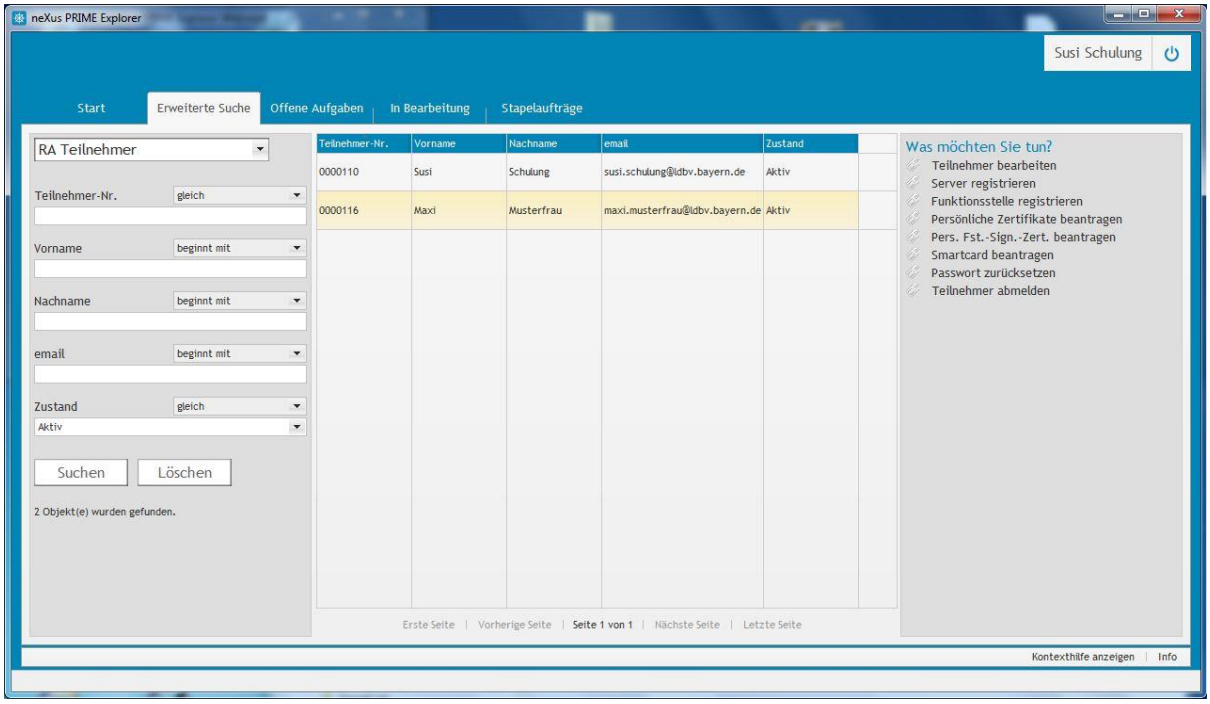
Für eventuell notwendige Hardware (Kartendrucker, Fotokamera etc.) ist die Kompatibilitätsliste der Firma Nexus bezüglich deren Nexus CardSDK zu beachten.

Die Endbenutzerausstattung (Smartcard, Kartenleser, Middleware) kann über Rahmenverträge des StMFLH mit den Firmen IDPendant und Charismathics sowie direkt über das IT-DLZ im Rahmen des SmartCard Produktionszentrums bezogen werden.

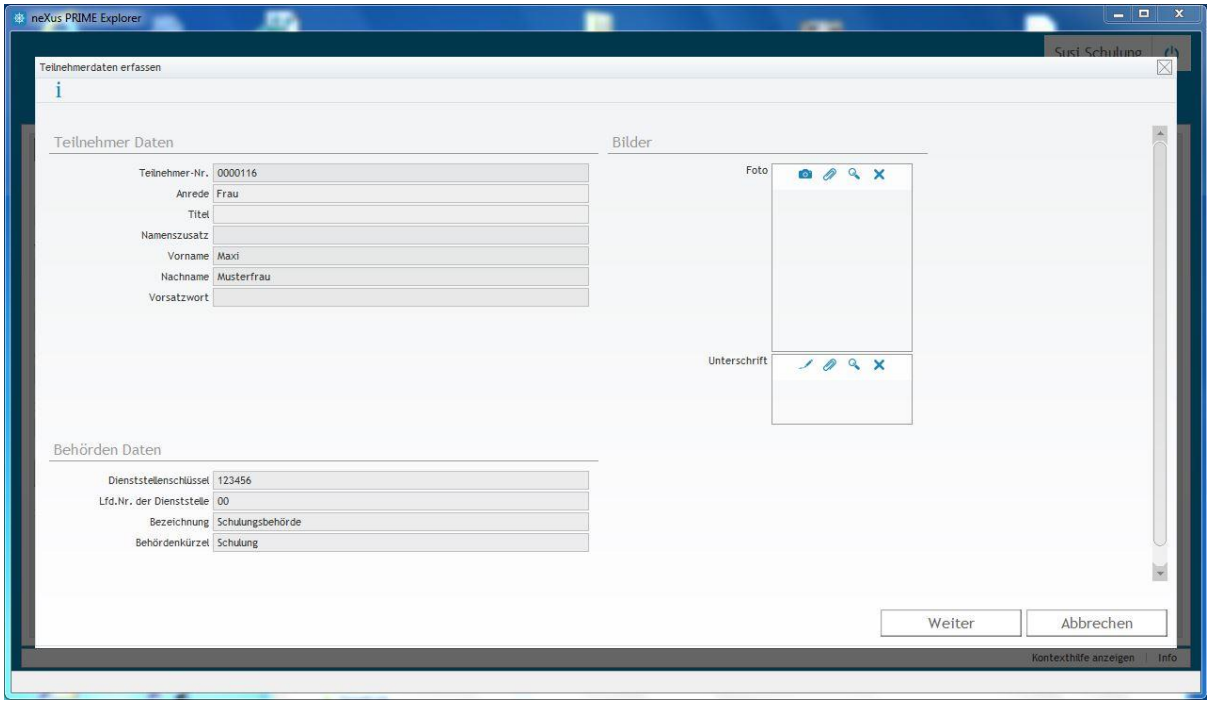
5.3 Smartcard beantragen (Neubeantragung und Re-Initialisierung)

Für das Beantragen oder Re-Initialisieren einer Smartcard ist die Registrierungsstelle zuständig, bei der der zukünftige Smartcard Inhaber registriert ist.

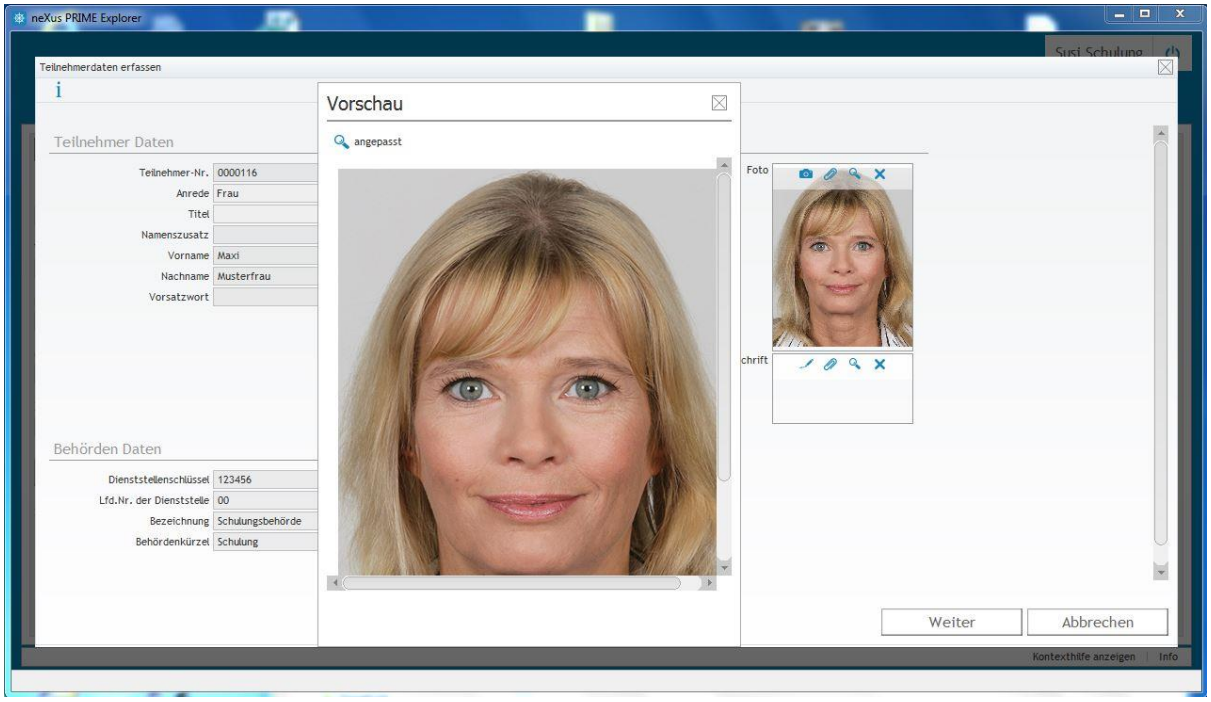
Lassen Sie sich über den **Menüpunkt „Erweiterte Suche“** mit der **Abfrage „RA Teilnehmer“** eine Übersicht aller Teilnehmer Ihrer Registrierungsstelle anzeigen und wählen den Teilnehmer aus, für den eine Smartcard beantragt werden soll.



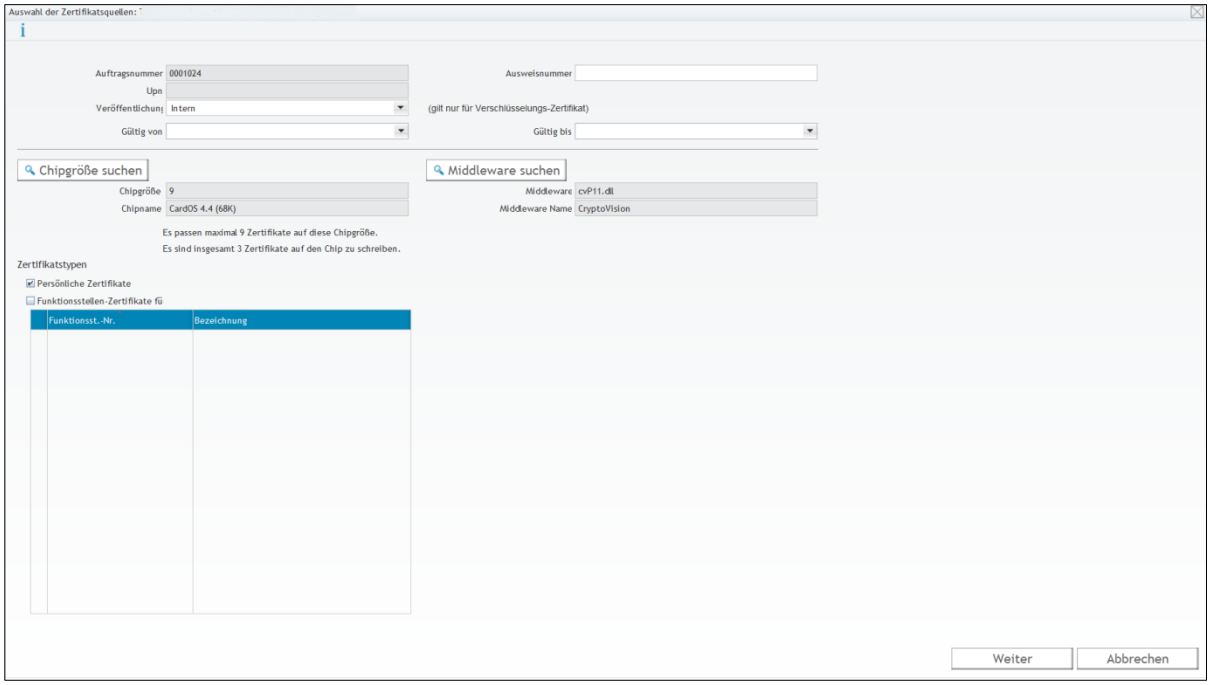
Klicken Sie auf **„Smartcard beantragen“** unter „Was möchten Sie tun?“.



Die angezeigten Daten werden den Teilnehmer- und Behördenstammdaten entnommen. Bei Bedarf können dem Antrag noch ein Foto und/oder eine Unterschrift hinzugefügt werden. Diese können entweder aus einer Datei oder live aus einer Kamera oder einem Unterschriftentablet (muss im Nexus CardSDK konfiguriert werden) eingelesen werden.



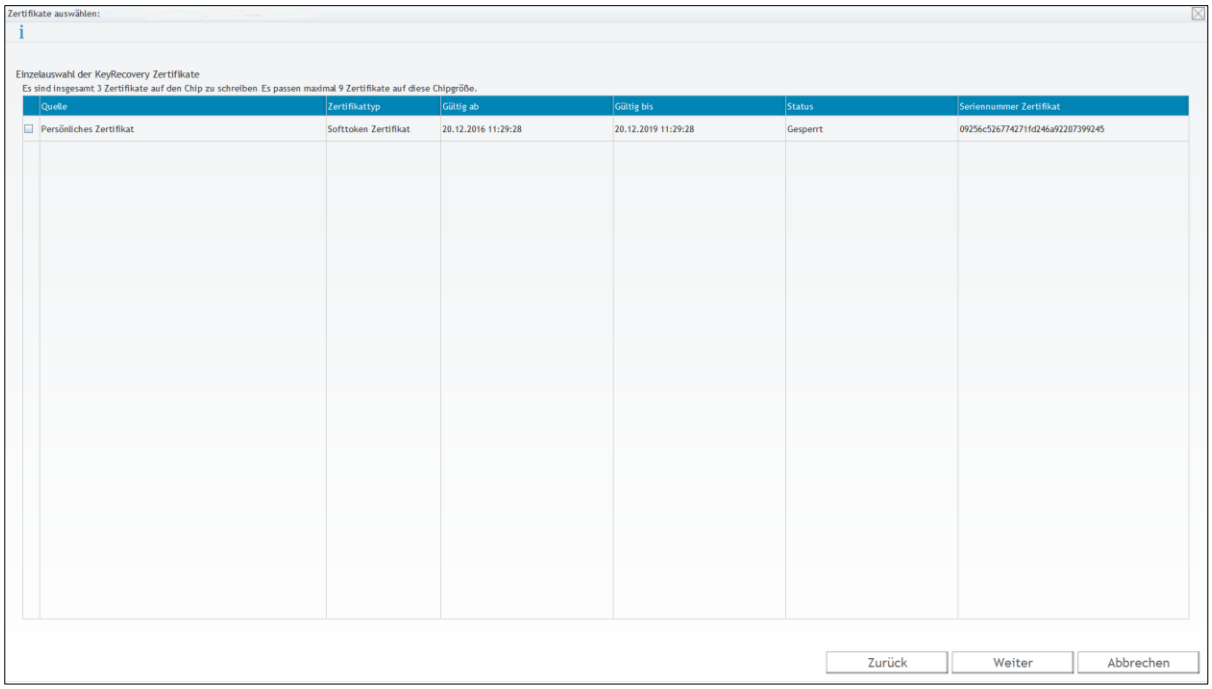
Klicken Sie auf **Weiter** um zur nächsten Seite zu gelangen.



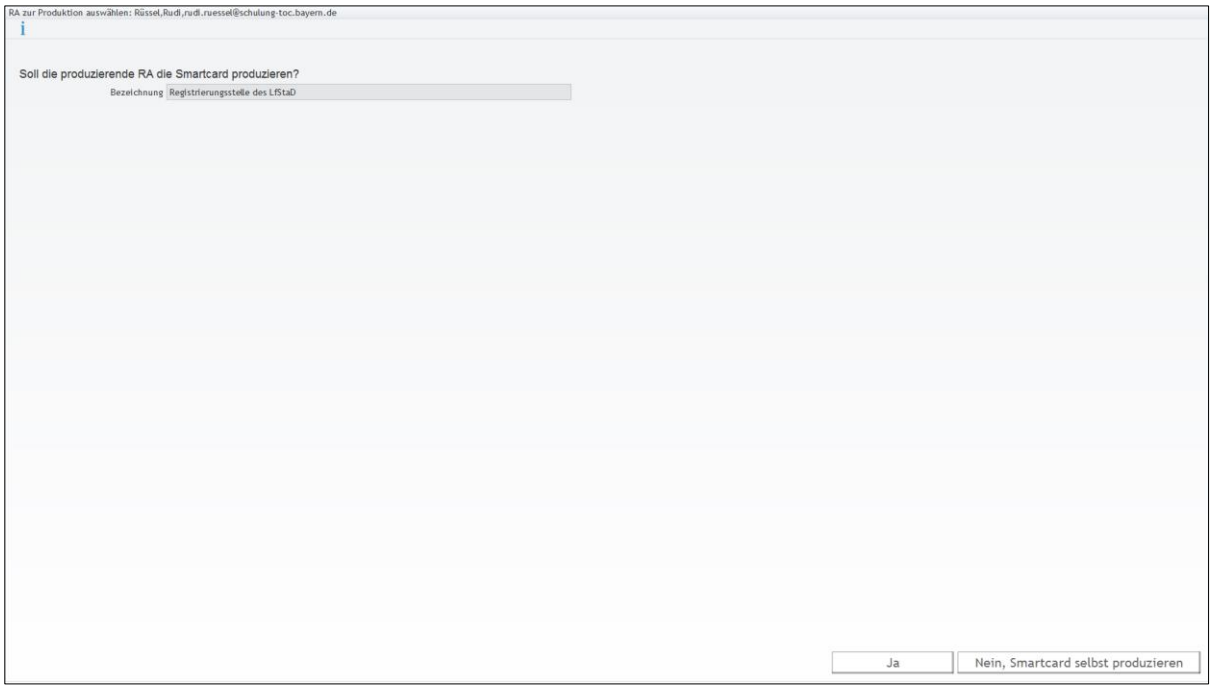
Sie können den Antrag hinsichtlich der Standard Middleware sowie des verwendeten Smartcard Chips modifizieren. Wählen Sie außerdem in Absprache mit dem Antragsteller die gewünschte **Veröffentlichungsstufe** für das **Verschlüsselungszertifikat** aus. **Intern** bedeutet dabei eine Zertifikatsveröffentlichung im Behördennetz. **Intern + Extern** bedeutet eine Veröffentlichung im Behördennetz und im Internet.

Elementar für den Antrag ist die Auswahl der Zertifikate, die auf die Smartcard geschrieben werden sollen. Falls die Smartcard auch Funktionsstellenzertifikate beinhalten soll, muss der Antragsteller vorher dafür berechtigt werden (siehe Kapitel 3.1.2). Sie sehen dann in der Tabelle alle zur Verfügung stehenden Funktionsstellen und setzen den Haken bei der oder den Funktionsstelle(n), die aus Smartcard geschrieben werden sollen (max. 4 erlaubt).

Anschließend gehen Sie mit **Weiter** zur nächsten Seite.

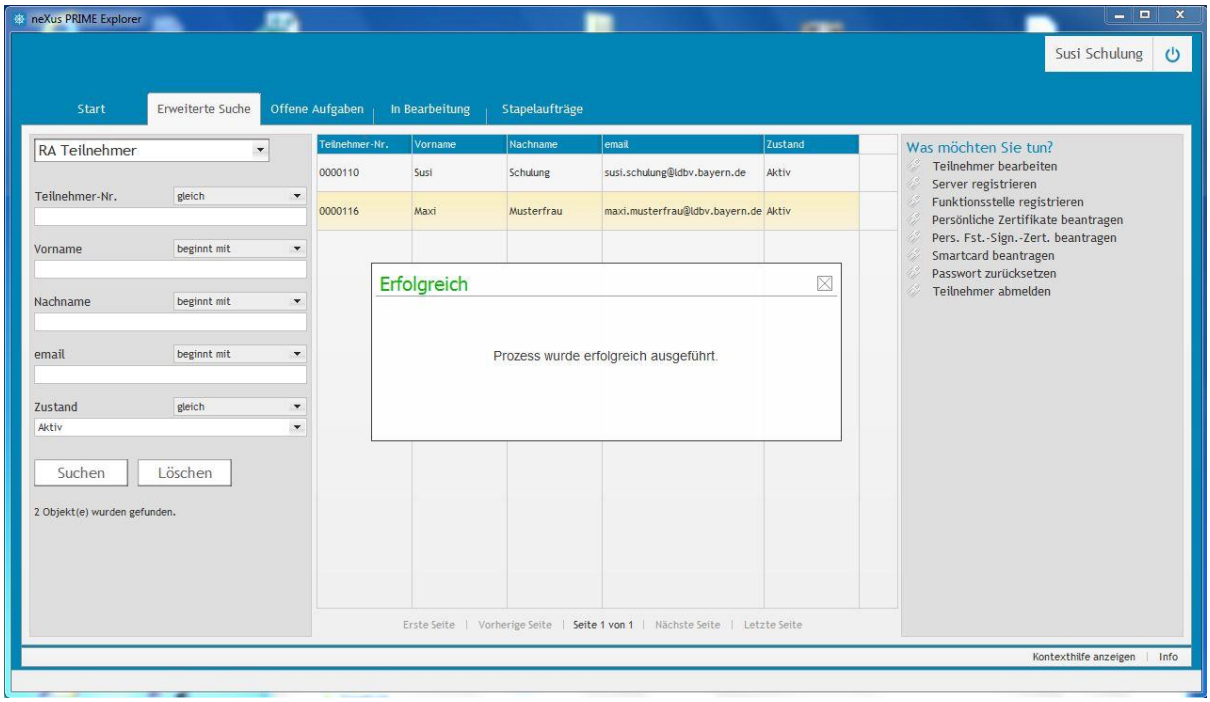


Auf der Seite bekommen Sie alle gesicherten Verschlüsselungszertifikate angezeigt und wählen die aus, die auf die Smartcard geschrieben werden sollen. Nach der Auswahl klicken Sie auf **Weiter**.



Klicken Sie auf **Ja** für eine neu zu produzierende Smartcard, deren Produktion in der bei Ihnen eingestellten Registrierungsstelle erfolgen soll.

Klicken sie auf **Nein, Smartcard selbst produzieren** falls Sie eine neue Smartcard selbst erzeugen möchten oder es sich um eine **Re-Initialisierung** handelt.



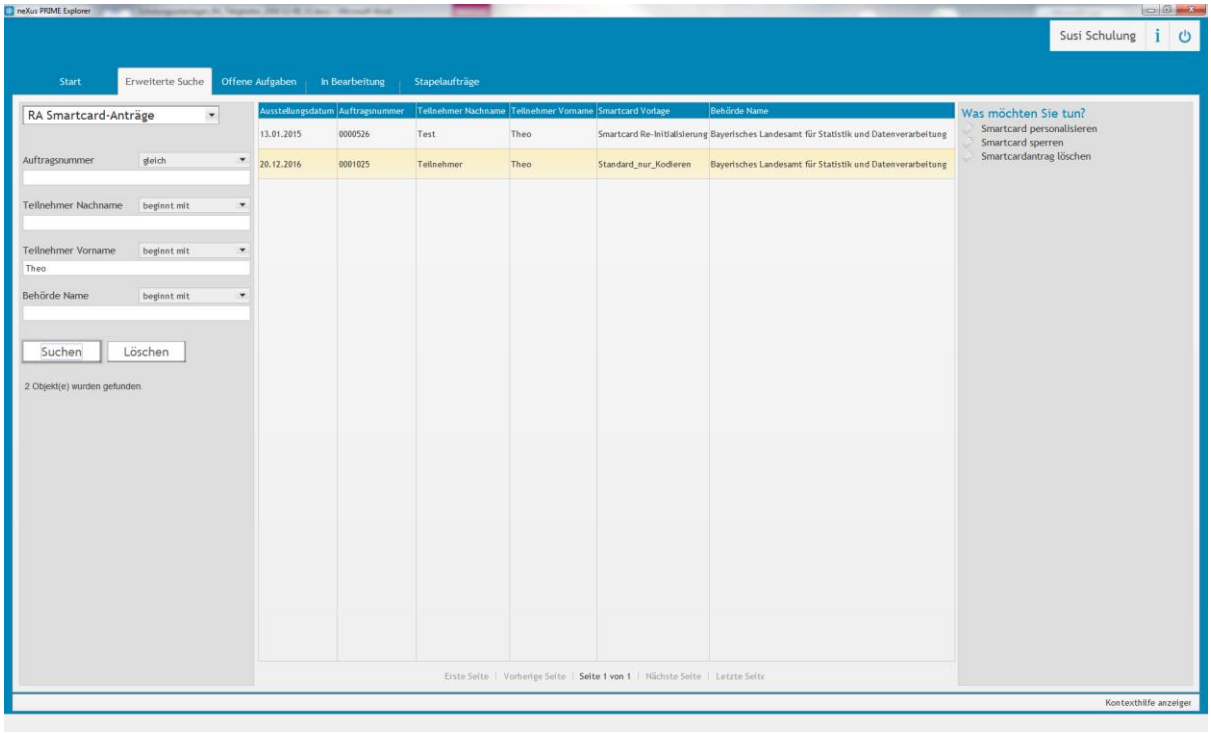
Die Beantragung ist abgeschlossen. Der Smartcard Antrag liegt damit der im vorherigen Schritt ausgewählten Registrierungsstelle zur Produktion vor.

5.4 Smartcard produzieren

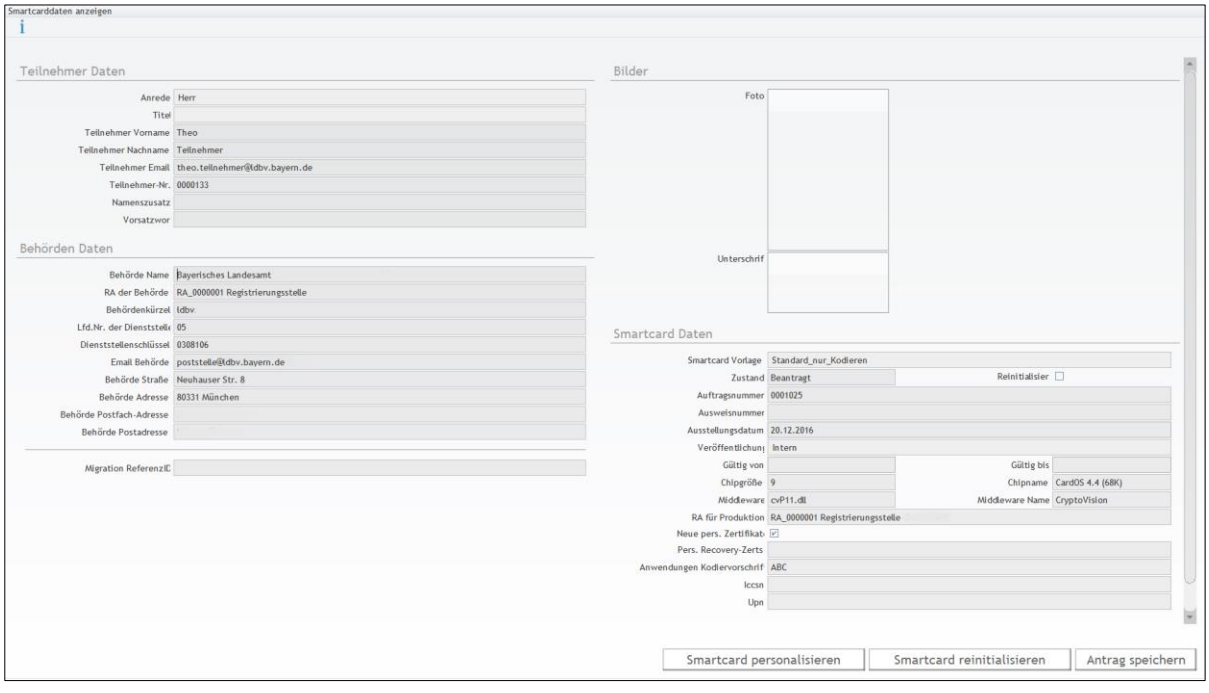
Nach der Beantragung der Smartcard kann diese von der produzierenden RA (siehe Kapitel 5.2.1.2) erstellt werden. Dabei können die Smartcard Anträge einzeln abgearbeitet oder zu einem Produktionsauftrag zusammengefasst werden.

5.4.1 Einzelauftrag

Lassen Sie sich über den **Menüpunkt „Erweiterte Suche“** mit der **Abfrage „RA Smartcard-Anträge“** eine Übersicht aller noch nicht produzierten Smartcards anzeigen und wählen den Antrag aus, der produziert werden soll.



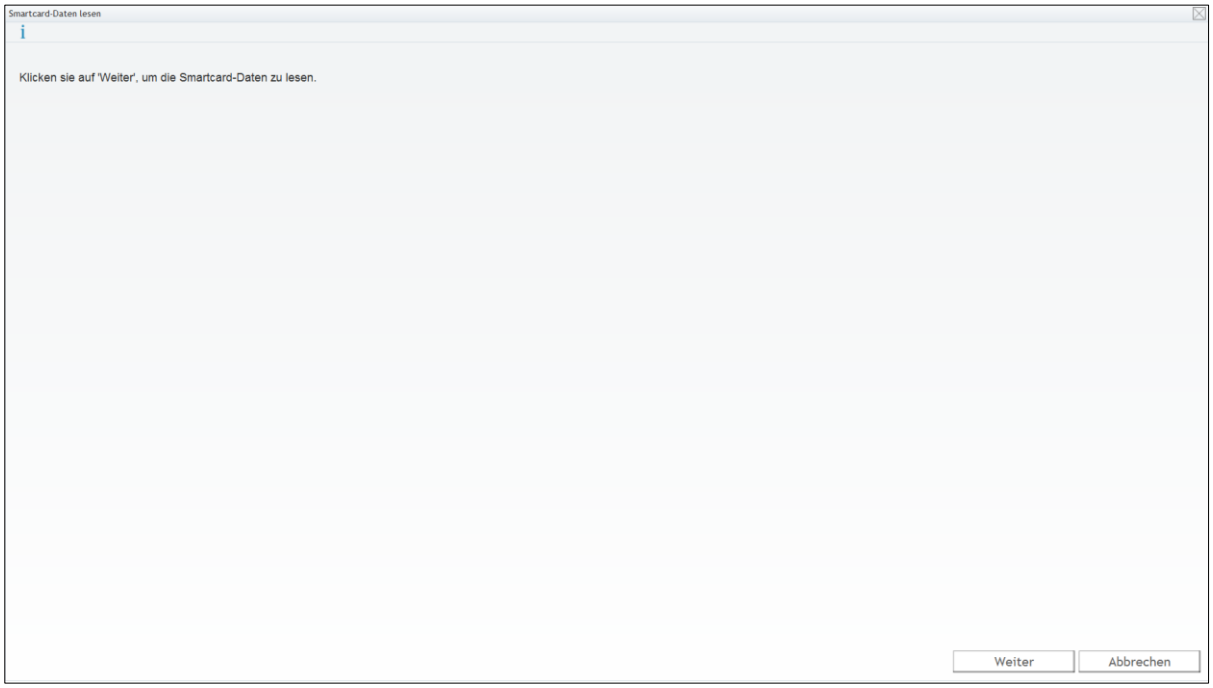
Klicken Sie auf **„Smartcard personalisieren“** unter „Was möchten Sie tun?“.



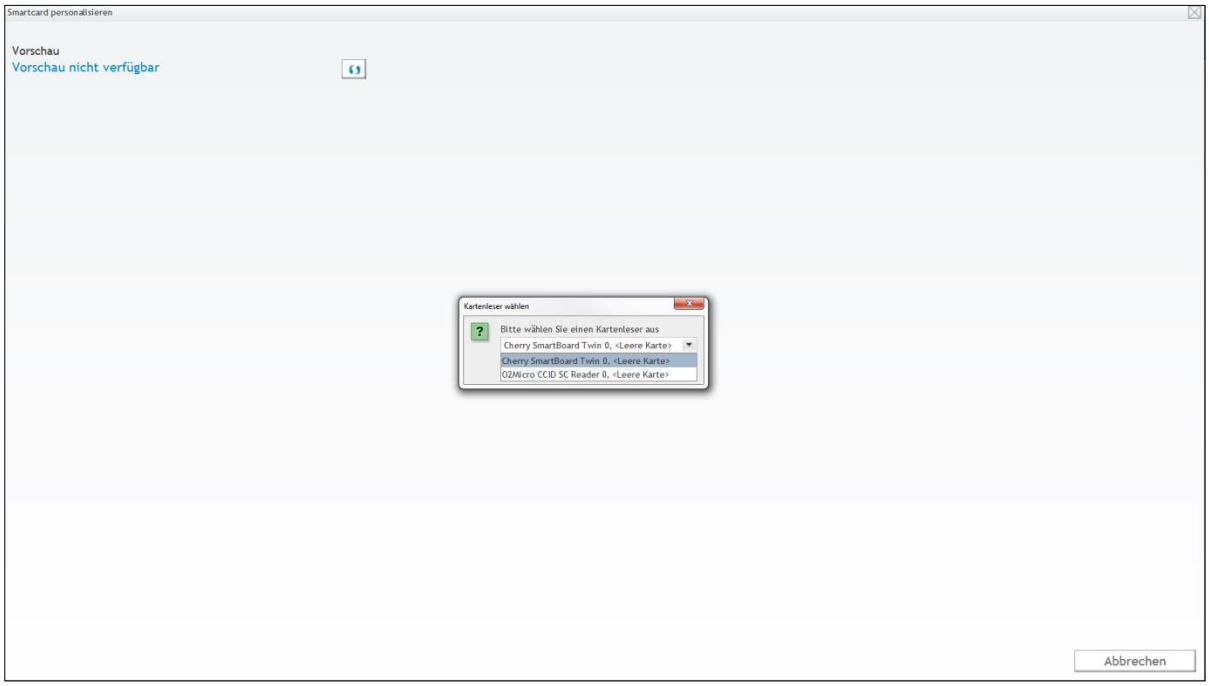
Kontrollieren Sie die Antragsdaten und geben Sie an ob Sie eine neue Smartcard (**Smartcard personalisieren**) oder eine bestehende Smartcard erneut (**Smartcard Re-Init**) beschreiben möchten.

Wenn Sie eine neue Smartcard beschreiben, wird eine Filestruktur auf die Smartcard aufgebracht sowie PIN und PUK gesetzt. Anschließend der PIN Brief gedruckt.

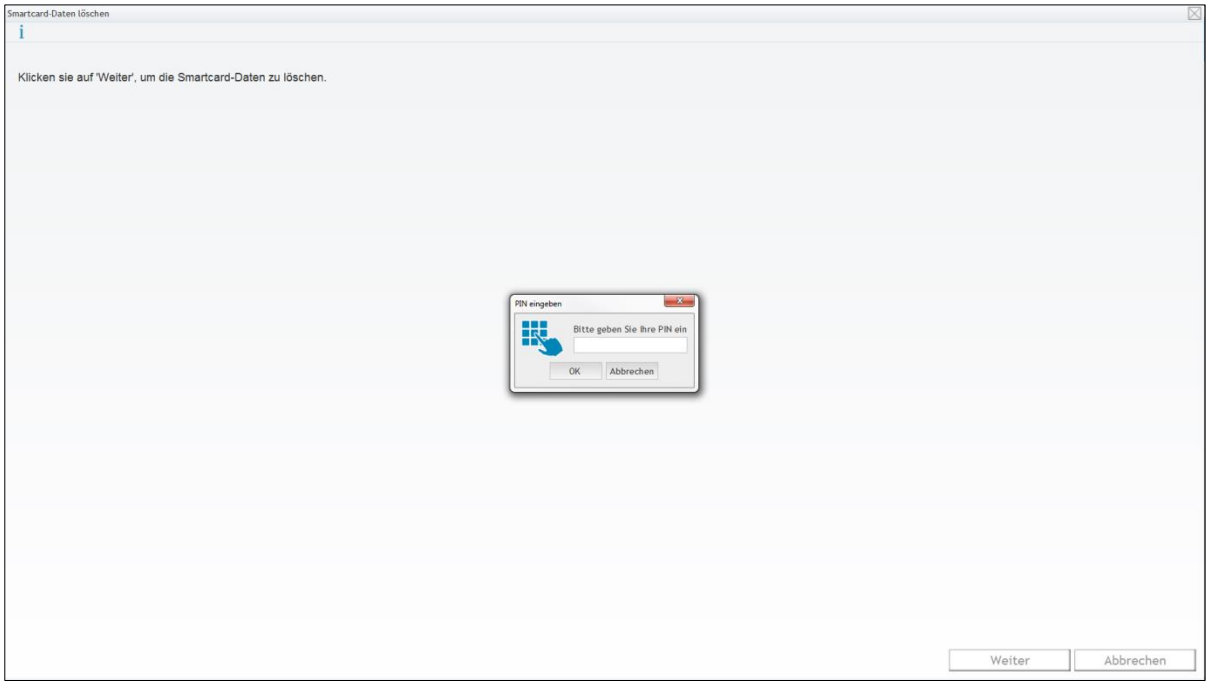
Sofern Sie eine bestehende Smartcard erneut beschreiben, wird der Inhalt der Smartcard gelöscht und zum Wiederbeschreiben der Karte deren PIN abgefragt.



Insofern Sie an Ihrem Rechner mehrere Kartenleser angeschlossen und Karten gesteckt haben erhalten Sie nachfolgend eine Abfrage nach dem Kartenleser, in dem die zu Re-Initialisierende Smartcard steckt.

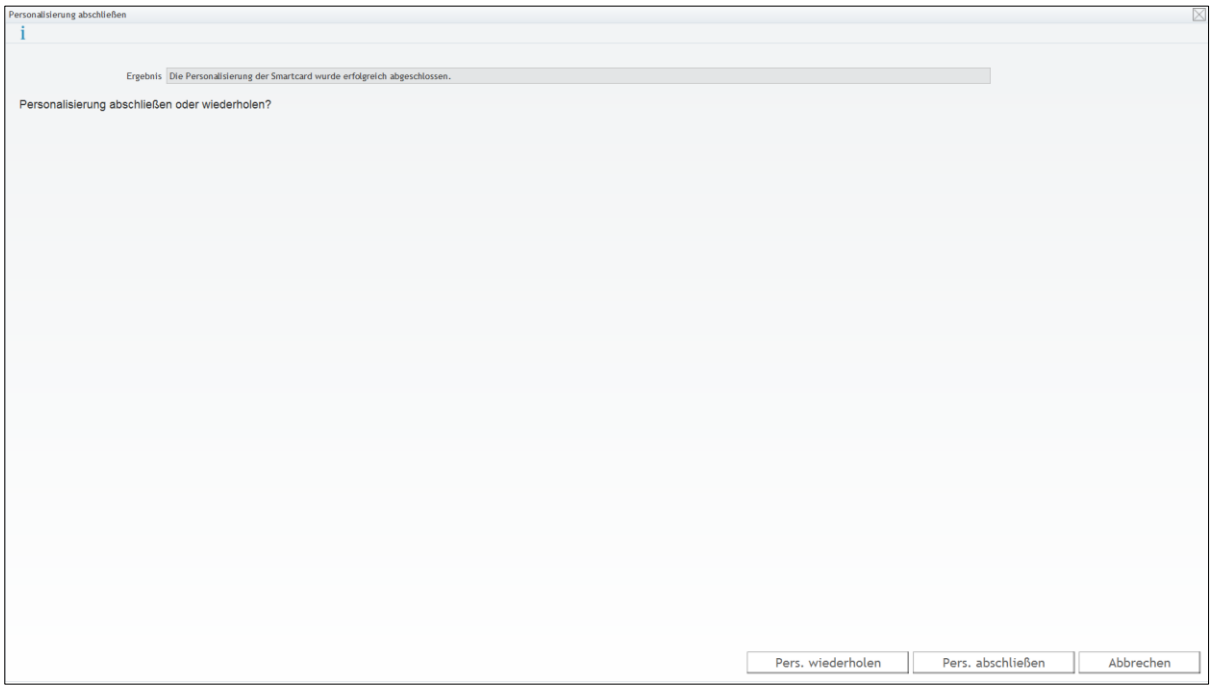


Lassen Sie nun den Karteninhaber die PIN eingeben, um den schreibenden Zugriff zu autorisieren.



Bei positiver Rückmeldung im Feld **Ergebnis** schließen Sie die Produktion der Smartcard ab, in dem Sie den Button **„Pers. abschließen“** drücken.

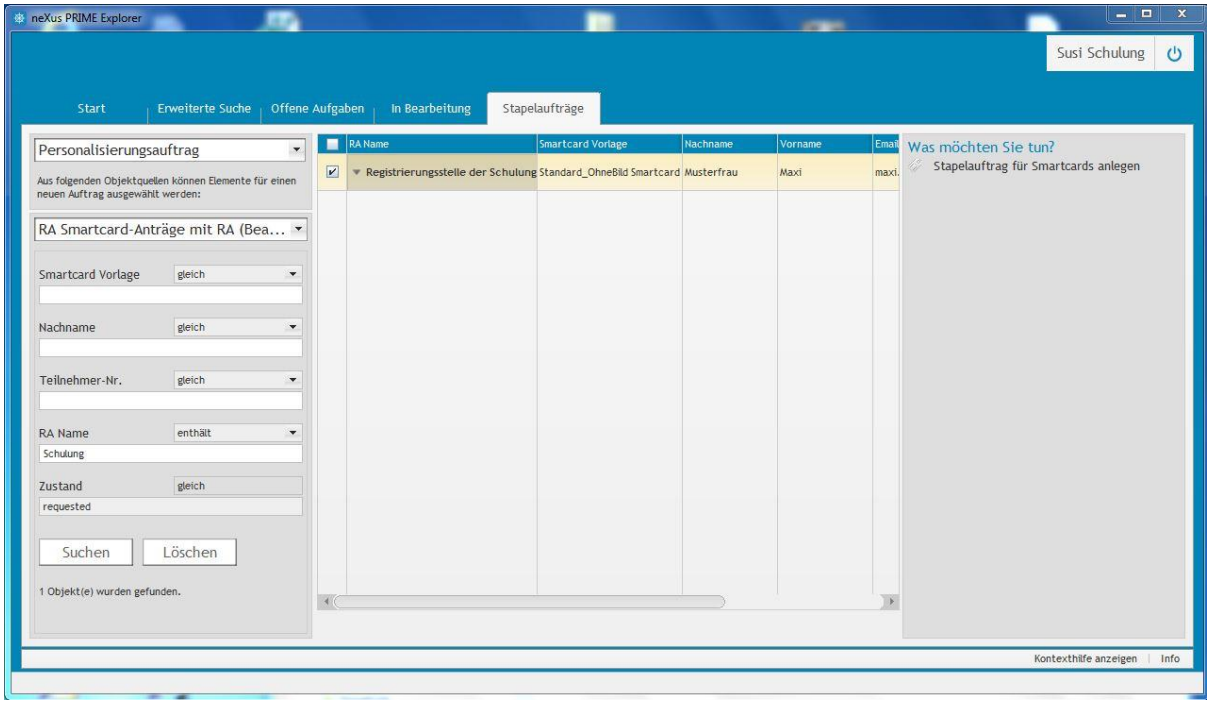
Bei einer Fehlermeldung können Sie die Personalisierung wiederholen (**Pers. wiederholen**) oder Sie wenden sich an den PKI-Support.



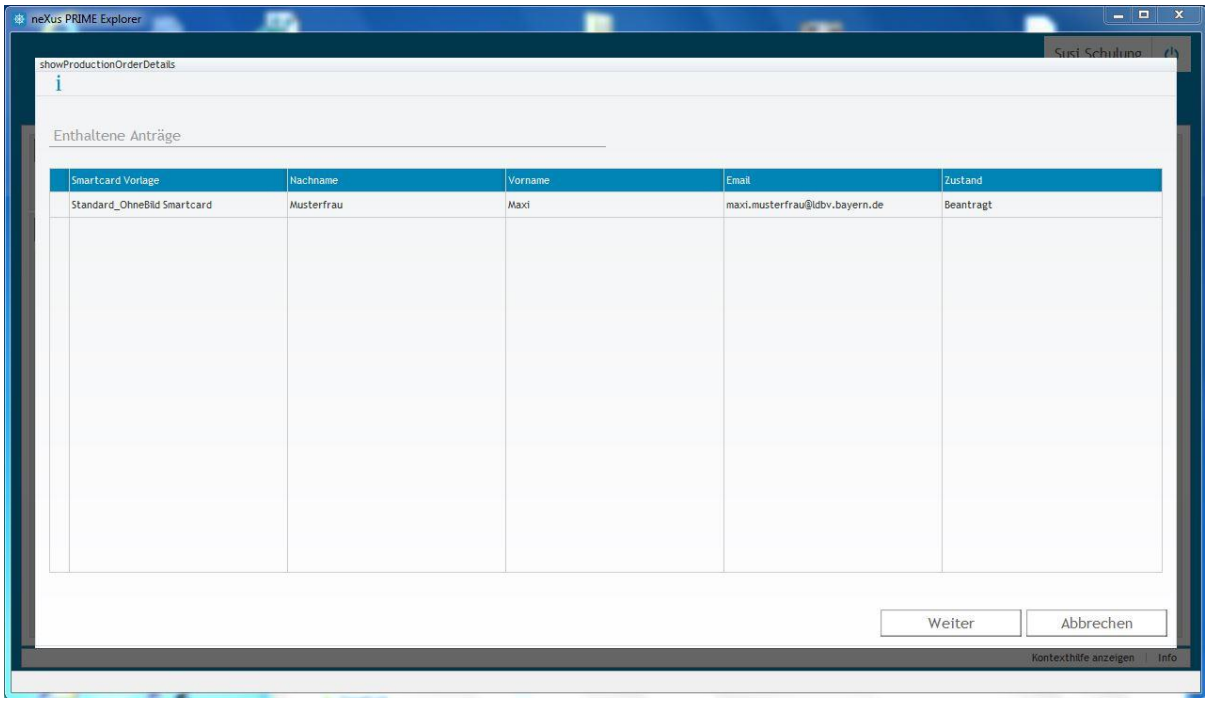
5.4.2 Sammelauftrag

Vor der Produktion der Smartcards können Sie mehrere Anträge zu einem Personalisierungsauftrag zusammenfassen, um die Produktion dann in einem Block abzuarbeiten.

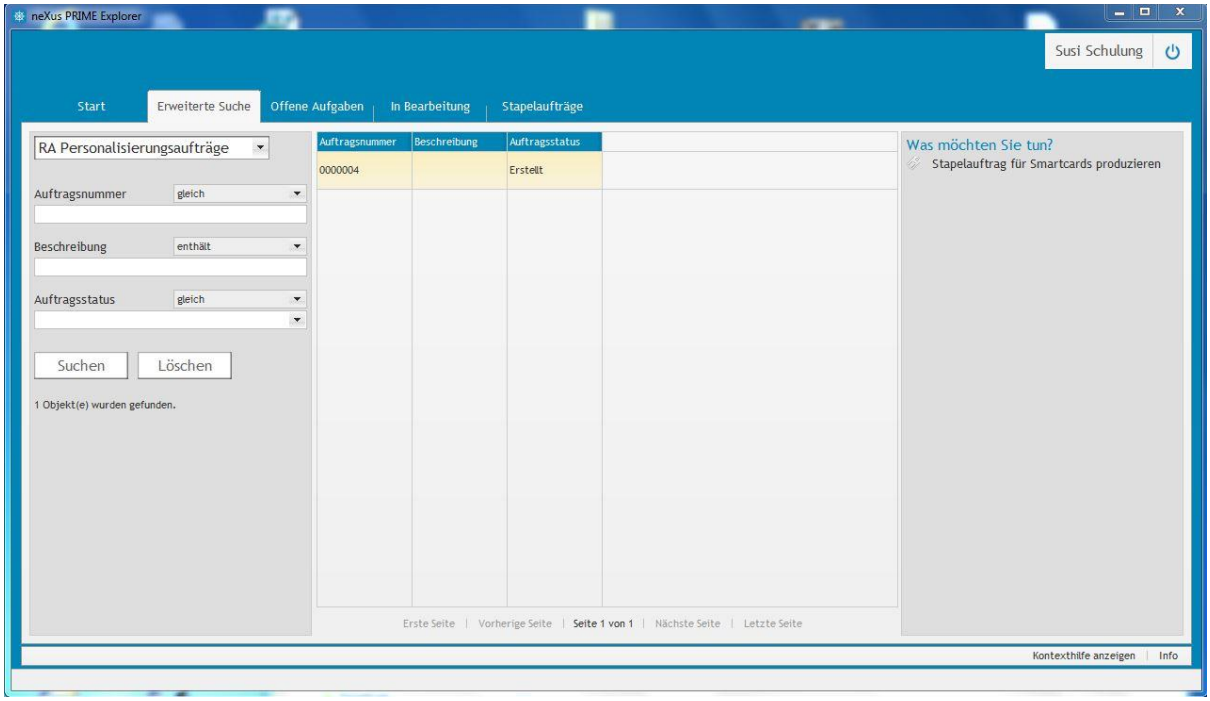
Gehen Sie dazu in den **Menüpunkt „Stapelaufträge“** und starten dort die **Abfrage „RA Smartcard-Anträge mit RA…“**



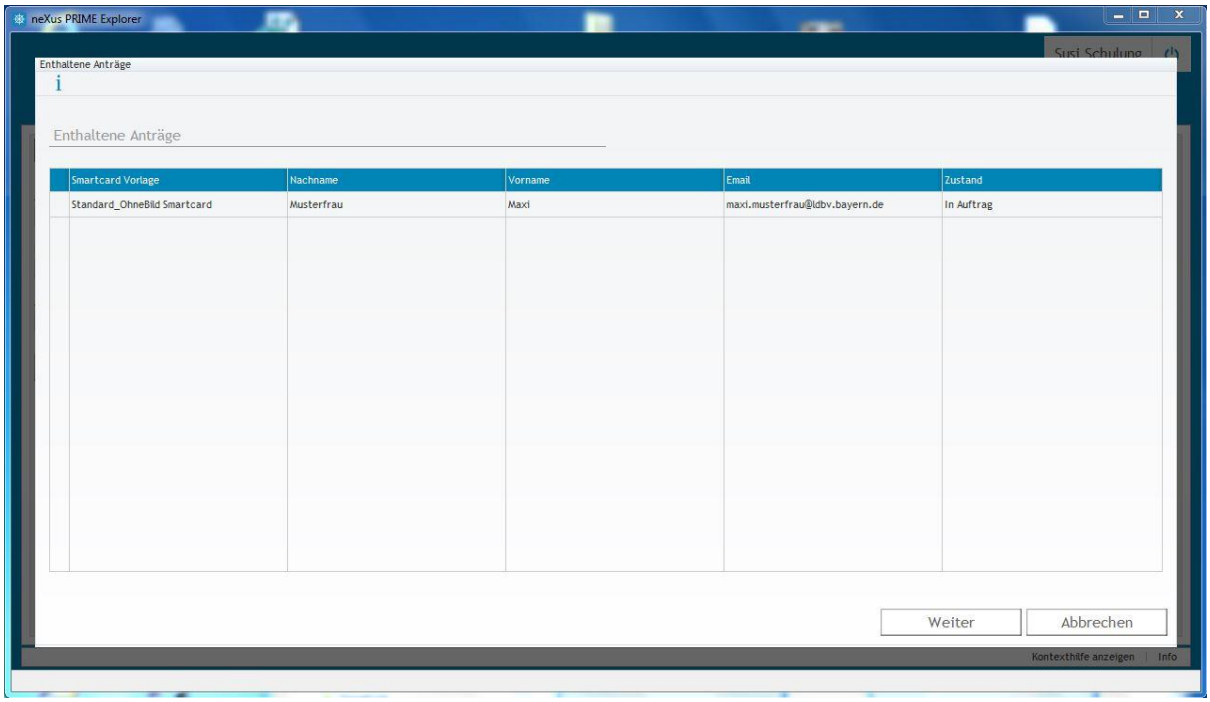
Setzen Sie bei allen Smartcardanträgen, die Sie zusammenfassen möchten, den Haken und klicken auf **„Stapelauftrag für Smartcards anlegen“** unter „Was möchten Sie tun?“.



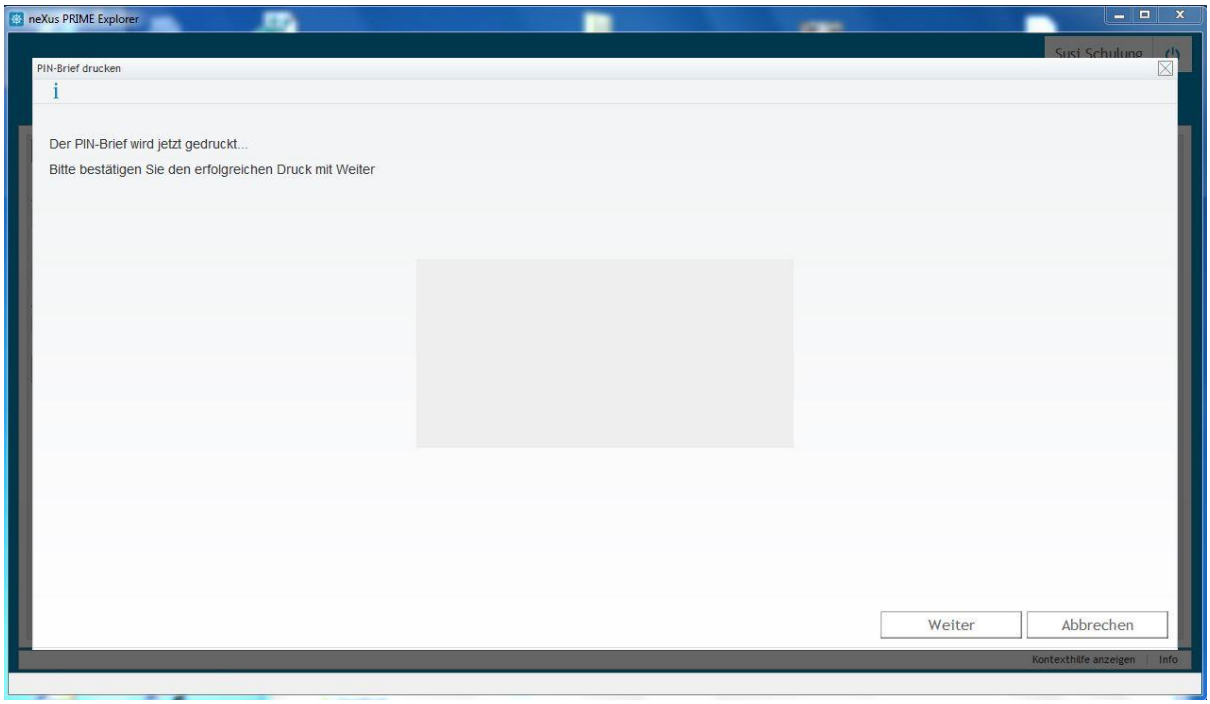
Gehen Sie dann auf den **Menüpunkt „Erweiterte Suche“** und starten dort die **Abfrage „RA Personalisierungsaufträge“**.



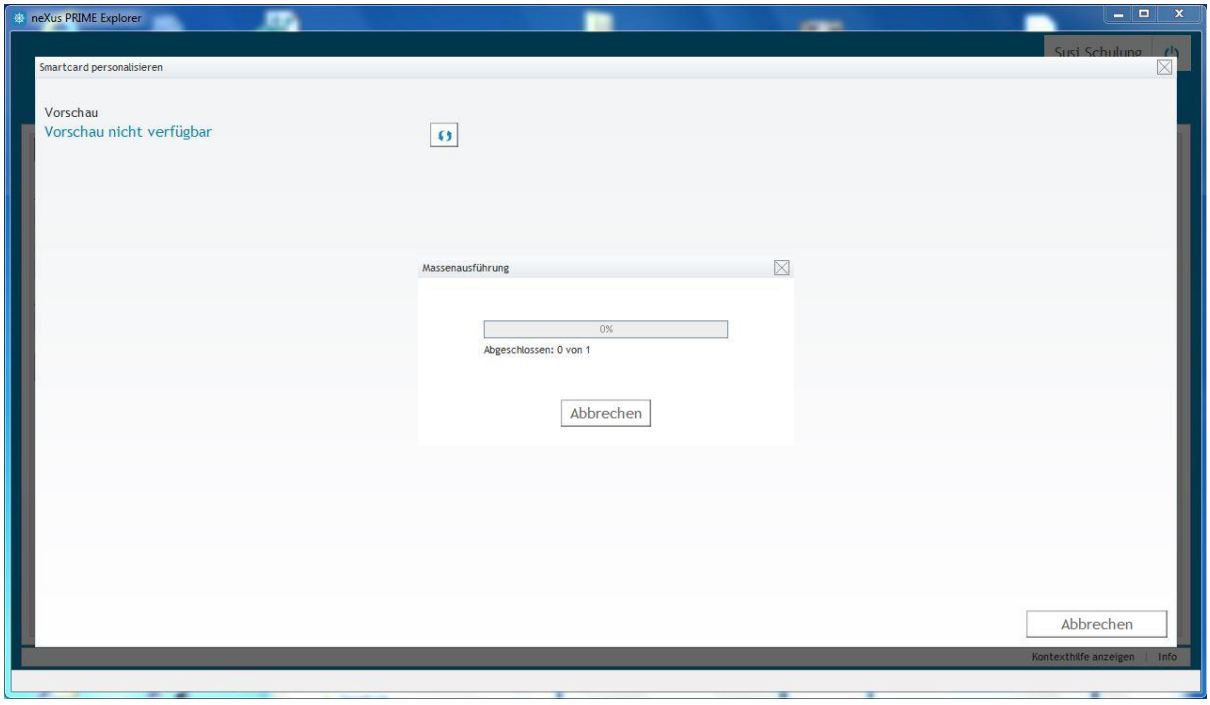
Markieren Sie den Personalisierungsauftrag und klicken auf **„Stapelauftrag für Smartcards produzieren“** unter „Was möchten Sie tun?“.

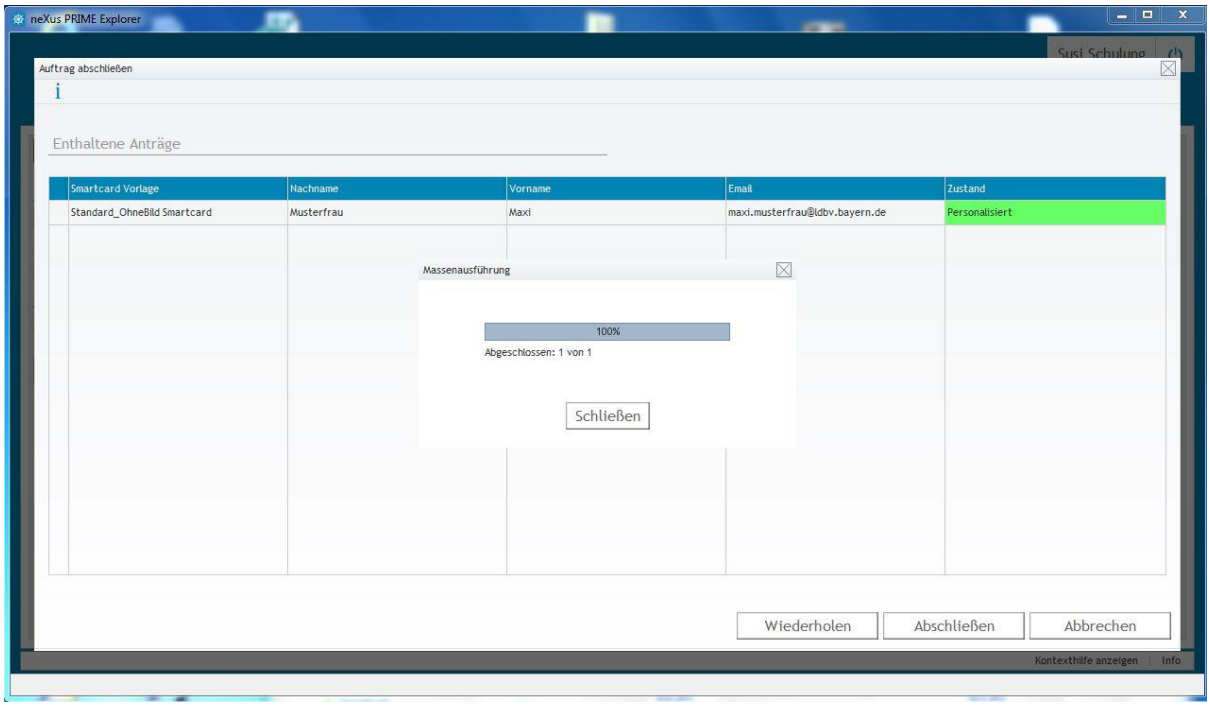


Sie sehen alle enthalten Smartcard Anträge. Klicken Sie auf **Weiter** und der PIN Brief wird gedruckt.



Anschließend werden die Smartcards produziert.





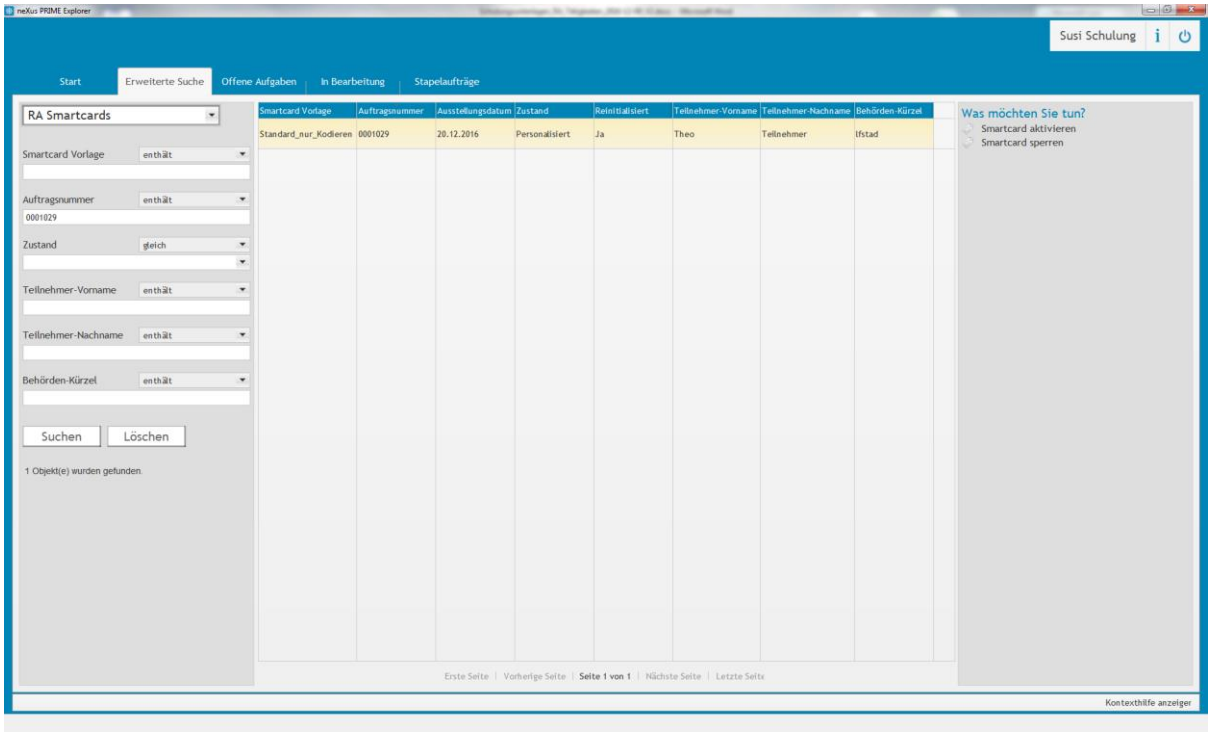
Beenden Sie den Vorgang in dem Sie auf **Abschließen** klicken.

5.5 Smartcard aktivieren

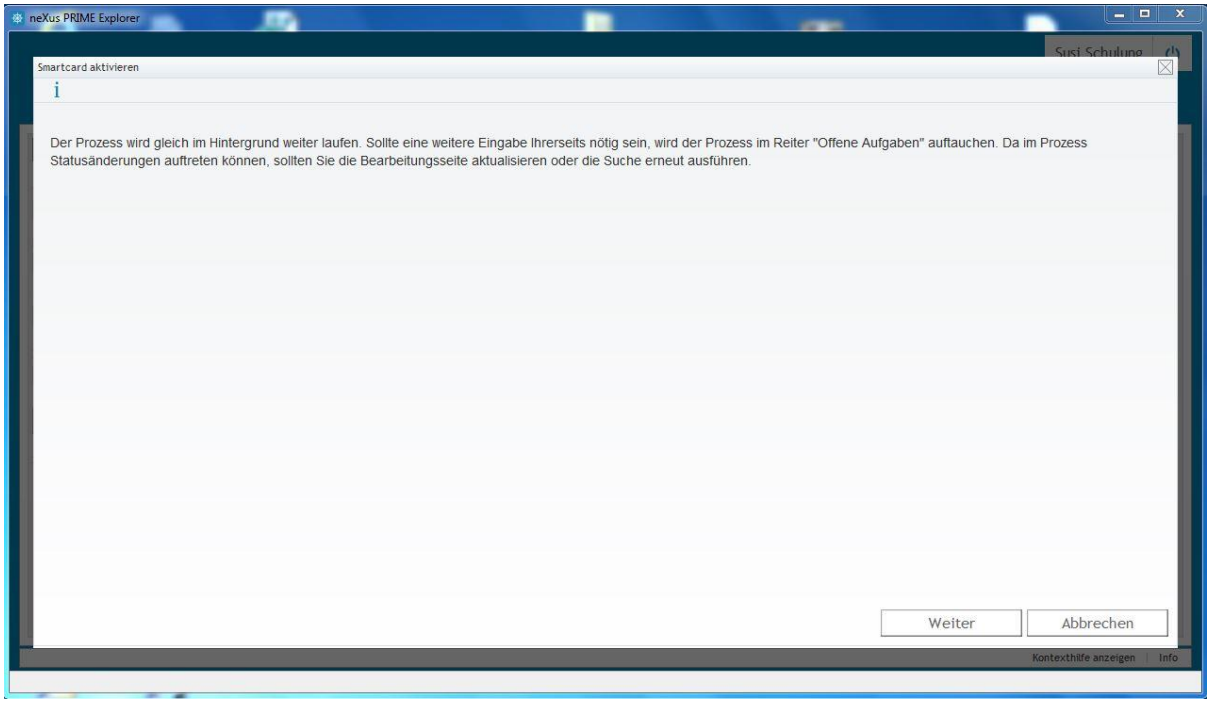
Nachdem die Smartcard produziert wurde, sind die darauf befindlichen Zertifikate noch temporär gesperrt. Somit können Sie eventuell vorhandene Softzertifikate oder eine Vorgänger Smartcard weiter verwenden. Erst wenn Sie die Smartcard aktivieren, werden die Zertifikate auf der Smartcard entsperrt und Vorgänger Zertifikate gesperrt.

Wichtiger Hinweis: Die Aktivierung der Smartcard muss innerhalb von 4 Wochen nach der Produktion bzw. dem Reinit erfolgen, sonst werden die Zertifikate auf der Karte dauerhaft gesperrt!

Lassen Sie sich über den **Menüpunkt „Erweiterte Suche“** mit der **Abfrage „RA Smartcards“** eine Übersicht aller Smartcards anzeigen und wählen die aus, die Sie aktivieren möchten.

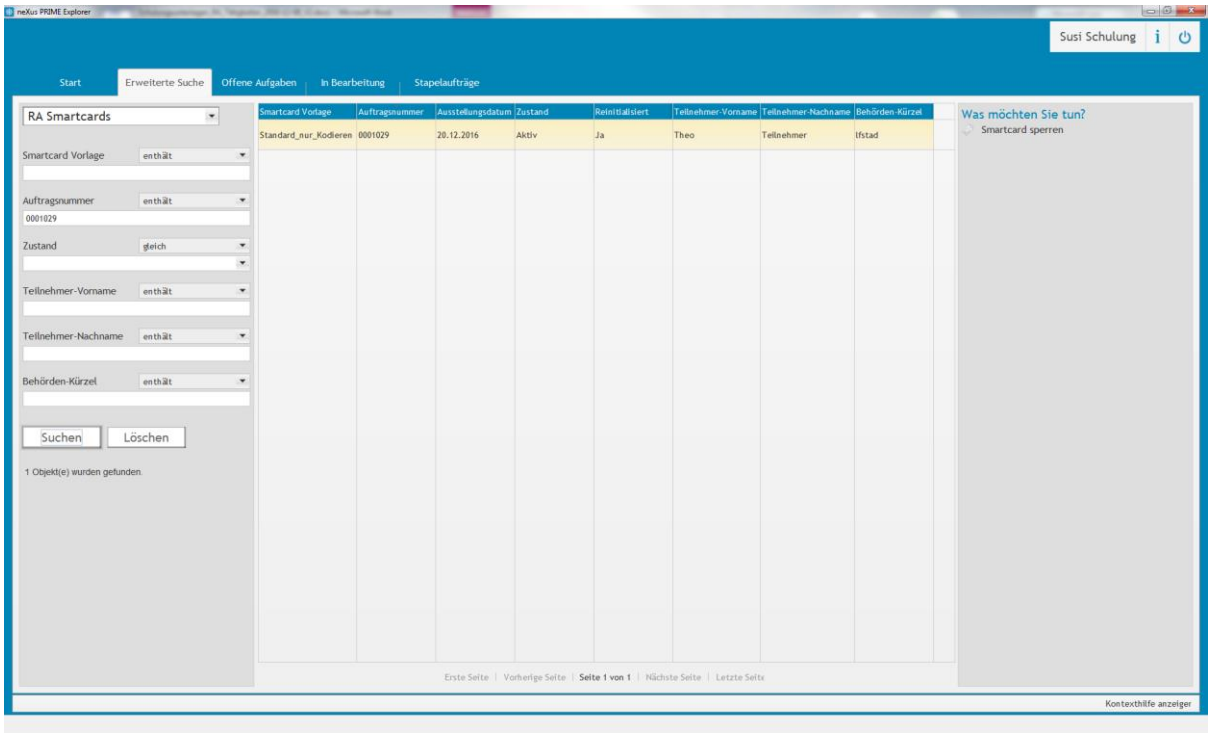


Klicken Sie auf **„Smartcard aktivieren“** unter „Was möchten Sie tun?“.

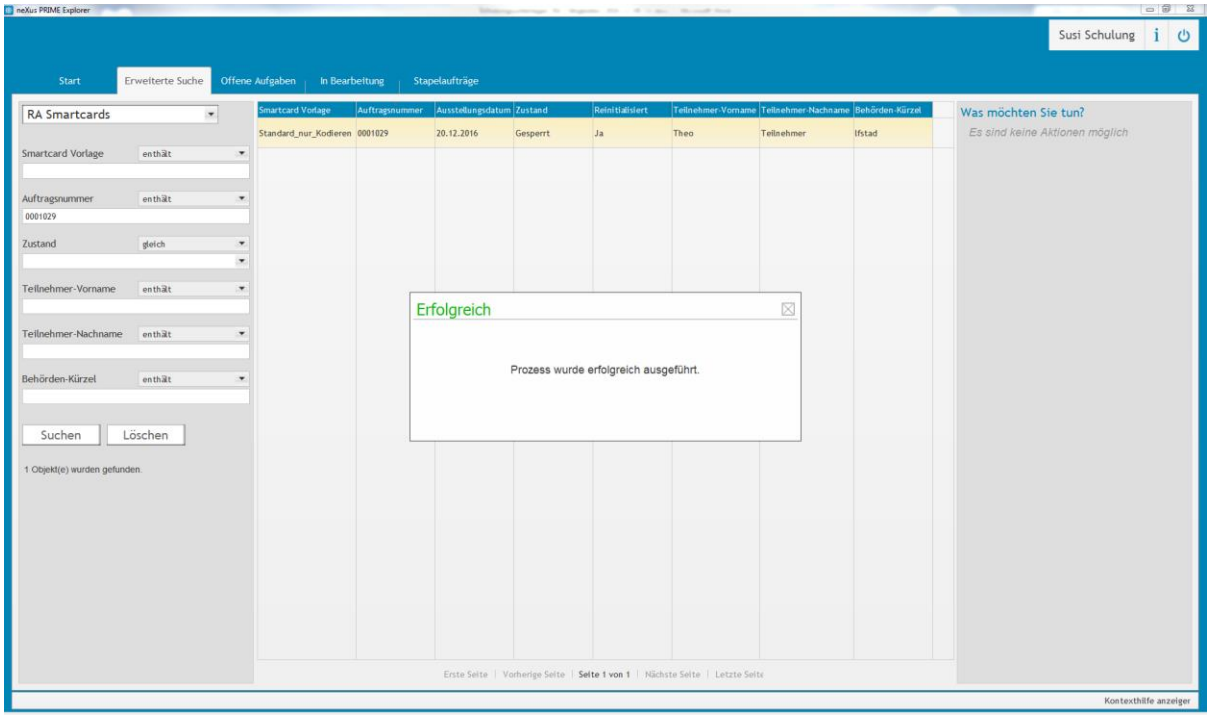


5.6 Smartcard sperren

Um eine Smartcard, und die darauf befindlichen Zertifikate, zu sperren, suchen Sie die Smartcard über den **Menüpunkt „Erweiterte Suche“** mit der **Abfrage „Smartcard“** aus der Übersicht.



Klicken Sie auf **„Smartcard sperren“** unter „Was möchten Sie tun?“.



6 Massenimport

Neben der Erfassung einzelner Teilnehmer, Funktionsstellen oder Clients gibt es auch die Möglichkeit diese in einer Liste zu sammeln und anschließend die Liste von den PKI Administratoren importieren zu lassen.

Für einen erfolgreichen Import müssen folgende Voraussetzungen erfüllt sein, bei deren Umsetzung Sie ggfs. einen IT-Administrator hinzuziehen.

- Enthält die in den nachfolgenden Kapiteln aufgeführten Felder in genau der Reihenfolge
- Dateityp: CSV
- Dateiformat: separiert durch Strichpunkt (Semikolon)
- Zeichensatz: UTF-8 (ohne BOM)

6.1 Teilnehmer

Für den Import von Teilnehmern werden die in der folgenden Tabelle aufgeführten Felder in dieser Reihenfolge benötigt. Sowohl Pflicht- als auch optionale Felder müssen vorhanden sein. Optionale Felder können aber leer sein. Sofern mögliche Werte angegeben sind, muss einer dieser Werte verwendet werden.

Feld	Pflicht (P) oder Optional (O)	Mögliche Werte	Anmerkungen
Anrede	P	Herr Frau	
Titel	O	Dr. Prof. Prof. Dr.	
Namenszusatz	O		z.B. von, van der, von und zu
Vorname	P		
Nachname	P		
Vorsatzwort	O		z.B. Gräfin, Freiherr, Baron
E-Mail	P		
Telefon	O		
Fax	O		
Dienststellen-schlüssel	P		Muss der Behörde entsprechen, in der der Teilnehmer arbeitet.
Lfd.-Nr. der Dienststelle	P		Muss der Behörde entsprechen, in der der Teilnehmer arbeitet.
Rolle	P	Kunde RA-Verantwortlicher RA-Mitarbeiter Clientverantwortlicher	Weitere Rollen können später durch das Bearbeiten des Teilnehmers ergänzt werden (siehe Kapitel 2.3.2).

Veröffentlichungsstufe	P	Intern Intern + Extern	

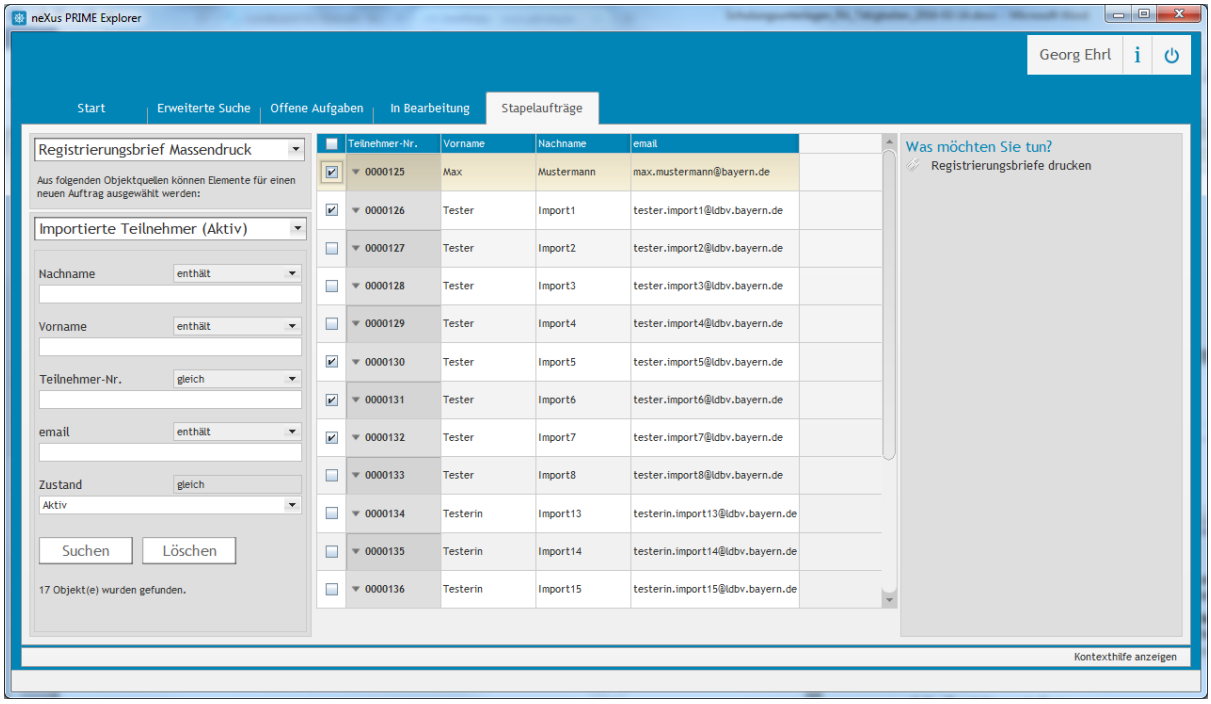
Beispiel für eine CSV Datei.

Massenimport_Teilnehmer_positiv.csv

```
1  Herr;;;Max;Mustermann;;max.mustermann@bayern.de;;;12345678;00;Kunde;Intern
2  Frau;Prof. Dr.;von und zu;Marianne;Musterfrau;Gräfin;marianne.musterfrau@bayern.de;(089) 2119-10;(089) 2119-0;12345678;00;Kunde;Intern + Extern
```

Nach dem Import der Teilnehmer in die Datenbank des Zertifikatsverwaltungssystems müssen Sie noch die Registrierungsbriefe für diese Teilnehmer drucken.

Lassen Sie sich dazu über den **Menüpunkt „Stapelaufträge“** mit der **Abfrage „Importierte Teilnehmer (Aktiv)“** eine Übersicht aller importierten Teilnehmer anzeigen und wählen durch Setzen des Häkchens die aus, für die Sie die Registrierungsbriefe drucken möchten.



Klicken Sie auf **„Registrierungsbriefe drucken“** unter „Was möchten Sie tun?“, um die das Drucken der Briefe für alle markierten Teilnehmer durchzuführen.

6.2 Funktionsstellen

Für den Import von Funktionsstellen werden die in der folgenden Tabelle aufgeführten Felder in dieser Reihenfolge benötigt.

Feld	Pflicht (P) oder Optional (O)	Mögliche Werte	Anmerkungen
Verantwortlicher	P		Entspricht der Teilnehmernummer des Zertifikatsverantwortlichen aus dem Zertifikatsverwaltungssystem
Bezeichnung	P		Bezeichnung der Funktionsstelle (z.B. Poststelle)
E-Mail	P		

Beispiel für eine CSV Datei.

Massenimport_Fkt_positiv.csv

```
1  0000157;Poststelle;poststelle-sct@import.bayern.de
2  0000157;Einkauf;einkauf-sct@import.bayern.de
3  0000157;Präsident;praesident-sct@import.bayern.de
4  0000157;Pforte;pforte-sct@import.bayern.de
```

6.3 Clients

Für den Import von Clients werden die in der folgenden Tabelle aufgeführten Felder in dieser Reihenfolge benötigt.

Feld	Pflicht (P) oder Optional (O)	Mögliche Werte	Anmerkungen
Verantwortlicher	P		Entspricht der Teilnehmernummer des Zertifikatsverantwortlichen aus dem Zertifikatsverwaltungssystem
Gerätename	P		URL/DNS/Name des Clients (z.B. nb001.finanzen.bayern.de)

Beispiel für eine CSV Datei.

Massenimport_Client_positiv.csv

```
1  0000158;sct-pc-1078.import.bayern.de
2  0000158;sct-pc-1079.import.bayern.de
3  0000158;sct-pc-1080.import.bayern.de
4  0000158;sct-pc-1081.import.bayern.de
```