Trusted German Insurance Cloud (TGIC)

Insurance Security Token Service (ISTS)

Trusted German Insurance Cloud®

Sicher. Effizient. Zukunftsorientiert.

FAQ
Frequently Asked Questions

Stand: 14.05.2021

Inhaltsverzeichnis

Einleitung und Links

Wir freuen uns, Sie als Nutzer in der TGIC und der Authentifizierungsdienste des Insurance Trust Centers (ITC) begrüßen zu dürfen. Da es sich um eine neue Kommunikationsinfrastruktur der deutschen Versicherungswirtschaft handelt, kommt es immer wieder zu Fragen zur Registrierung, zur Anbindung und zur Anwendung des Insurance Security Token Services (ISTS).

In diesem Dokument sollen typische Anwendungsszenarien in der Trusted German Insurance Cloud (TGIC) mit konkreten Beispielen beschrieben und die Nutzung der fachlichen Schnittstellen anhand von Schritt-für-Schritt-Anleitungen dargestellt werden. Hierzu zählen auch Vorschläge, in welchem Zusammenhang und mit welchen Attributen Nutzer, Organisationen und TGIC-Services im Rahmen der jeweiligen Szenarien angelegt werden sollten. Dadurch sollen neue TGIC-Service-Nutzer und -Betreiber bei der Schaffung der notwendigen fachlichen Voraussetzung unterstützt werden.

Links:

TGIC-Nutzerverwaltung: https://user.tgic.gdv.org/TGIC-Nutzerverwaltung
TGIC-Kennwortverwaltung: https://userpw.tgic.de/TGIC-Kennwortverwaltung_www/index.xhtml
TGIC Public Key Infrastruktur: https://pki.tgic.de/TGIC-PKI
TGIC-Services Registrierung: tgic-serviceregistrierung@gdv-dl.de
TGIC-Support Team: tgic-support@gdv-dl.de

1 Glossar der relevanten Begriffe im TGIC-Umfeld

In den folgenden Abschnitten werden die grundlegenden Konzepte der Trusted German Insurance Cloud (TGIC) und in diesem Zusammenhang verwendeten Begrifflichkeiten in Form eines Glossars erläutert.

1.1 Trusted German Insurance Cloud (TGIC)

Die Trusted German Insurance Cloud (TGIC) ist eine hochsichere Infrastruktur und bietet zur Unterstützung der sensiblen Prozesse innerhalb der Versicherungswirtschaft Services und Anwendungen für die sichere Kommunikation von den Nutzern mit Web-Diensten.

1.2 Insurance Trust Center (ITC)

Die zentrale Komponente der TGIC ist das Insurance Trust Center (ITC). Es hat die Aufgabe, die registrierten Nutzer zu identifizieren, die Nutzungsmöglichkeit der jeweiligen Services und die dafür notwendigen TGIC-Benutzerkonten zu verwalten und die nötigen Daten für eine Berechtigung durch den TGIC-Service zu liefern.

1.3 Insurance Security Token Service (ISTS)

Der Insurance Security Token Service (ISTS) ist die zentrale Instanz des ITC und ermöglicht die wechselseitige Authentifikation von Versicherungsunternehmen (VU), Vertriebs- und Kooperationspartnern oder Behörden. Der zentrale Anwendungsfall ist die Erteilung von Berechtigungsmerkmalen (Security Token), mit denen sich Service-Nutzer gegenüber Service-Betreibern sicher authentifizieren können. Die Vergabe von Token erfolgt ausschließlich an Kommunikationspartner, die in der TGIC registriert sind. Zudem wird durch diese Komponente die Kommunikation zwischen dem bewährten Branchennetz und der TGIC ermöglicht.

1.4 TGIC-Services

Im Rahmen des TGIC-Konzepts wird ein TGIC-Service (dies kann ein Webservice oder eine Webanwendung sein) von einem Versicherungsunternehmen oder einem Partner bereitgestellt. Um einen TGIC-Service nutzen zu können, muss ein Nutzer sich zunächst beim ITC registrieren und am ISTS authentifizieren. Nach erfolgreicher Authentifizierung werden das Security Token und ggf. weiterer Eigenschaften (sogenannte Claims) an den TGIC-Service übermittelt.

1.5 Organisationen

Im Rahmen der TGIC stellt eine Organisation ein Versicherungsunternehmen, einen Vertriebs- und Kooperationspartner oder eine Behörde dar.

1.6 Partner-Rollen

Partner-Rollen im Kontext der TGIC stellen Kategorien dar, die TGIC Nutzern zugeordnet werden können.

Ein TGIC-Service kann bestimmte Partner-Rollen für seine Nutzung voraussetzen. Ein Nutzer muss dann mindestens eine der geforderten Partner-Rollen (z.B. VU-Mitarbeiter, Rechtsanwalt etc.) besitzen, um den TGIC-Service nutzen zu können.

Die Vergabe der Partner-Rollen an Nutzer erfolgt durch den Organisations-Verwalter (siehe 1.8). Jedoch können nur die Partner-Rollen vergeben werden, die der Organisations-Verwalter selbst innehat. Es empfiehlt sich, bei der Beantragung eines Organisationsverwalters direkt im Registrierungsformular die für die Servicenutzung erforderlichen Partner-Rollen auszuwählen. Welche Partner-Rollen erforderlich sind, erfahren Sie bei dem jeweiligen Service-Anbieter.

1.7 Nutzertypen

Im TGIC-Umfeld wird zwischen den Nutzertypen „Natürliche Person“ und „Technischer Nutzer“ unterschieden. Hierbei ist zu beachten, dass eine „Natürliche Person“ die Authentifikationsarten mTAN, TOTP und nPA und ein „Technischer Nutzer“ die X.509-Authentifikation unterstützt.

Bei Nutzern mit dem Nutzertyp „Technischer Nutzer“, bezeichnen die Nutzerattribute Geschlecht, Titel, Vorname, Nachname, Geburtsdatum und E-Mail den Ansprechpartner für den technischen Nutzer.

1.8 Berechtigungsart

Es wird zwischen folgenden Berechtigungsarten unterschieden, die im Rahmen des Nutzerkonzepts der TGIC-Nutzerverwaltung relevant sind:

Organisations-Verwalter* (oder auch *VU-Verwalter): Ein Organisation-Verwalter ist berechtigt, über die Nutzerverwaltung neue Organisations-Nutzer anzulegen und zu pflegen bzw. Selbst-Pfleger anzulegen. Im zweiten Fall geschieht die Pflege entsprechend der Bezeichnung ausschließlich durch den Nutzer selbst.

Hinweis: Da die Benutzeroberfläche der TGIC-Nutzerverwaltung nicht offen über das Internet, sondern nur über das geschlossene GDV-Netz zu erreichen ist, steht dieser Zugangsweg ausschließlich GDV-Mitgliedsunternehmen zur Verfügung. Alle weiteren Organisationen können über einen User-Agenten (siehe 2.2) auf die Schnittstelle der TGIC-Nutzerverwaltung (API) zugreifen.

Organisations-Nutzer* (oder auch VU-eigene *Nutzer): beispielsweise Angestellte der Organisation; werden ausschließlich durch die Organisation gepflegt und sind der Organisation in der TGIC-Nutzerverwaltung zugeordnet.

Selbst-Pfleger* (oder auch *VU-übergreifende Nutzer): beispielsweise Rechtsanwälte, Werkstätten oder Makler; können von allen durch den Selbstpfleger benannten Organisationen angelegt werden, welche die Berechtigung zur Nutzeranlage besitzen. Die Pflege

ist anschließend nur durch den Selbstpfleger und ggf. durch den Support des Serviceanbieters möglich.

1.9 Authentifizierungsverfahren

In der TGIC stehen derzeit grundsätzlich vier Authentifizierungsmethoden zur Verfügung, die von jedem Serviceanbieter individuell für seine Servicenutzung vorausgesetzt werden können.

Natürlichen Personen stehen zur Authentifizierung die Verfahren „mobile Transaktionsnummer (mTAN), „Timebased Onetime Password“ (TOTP) sowie der „neue Personalausweis (nPA) zur Verfügung.

Bitte beachten Sie, dass nur in der Produktionsumgebung der TGIC reale SMS zur Ausstellung einer mTAN versendet und dem Serviceanbieter entsprechend in Rechnung gestellt werden. Für Tests in der Integrationstestumgebung wird eine immer gültige mTAN zur Authentifizierung simuliert.

Technische Nutzer authentifizieren sich ausschließlich mit X.509-Zertifikaten.

1.10 Security-Token

Im TGIC-Kontext sind Security-Token als Authentifizierungsnachweis in Form einer definierten XML-Struktur (SAML-Assertion), die durch den ISTS vergeben und zum Nachweis der Identität eines Service-Nutzers bei einem TGIC-Service genutzt werden, zu verstehen. Als Synonym für Security Token wird auch Authentication-Token verwendet, da das Security-Token, das der ISTS ausstellt, später zur Authentifikation gegenüber dem TGIC-Service verwendet wird.

1.11 Claims

Bestimmte Nutzerattribute können zur weiteren Auswertung (z.B. Berechtigung) durch einen TGIC-Service in das Security-Token aufgenommen werden. Dazu muss der Nutzer bei der Beantragung eines Security-Tokens beim ISTS diese Nutzerattribute in Form von sogenannten Claims bei der Token-Beantragung im Request mit angeben.

2 Systeme

2.1 Aufruf eines TGIC-Services

Zur Interaktion mit einem TGIC-Service (dies kann ein Webservice oder eine Webanwendung sein) authentisiert sich der Service-Nutzer zuvor beim ITC und übermittelt das durch den ISTS ausgestellte Security-Token als Nachweis seiner Identität und ggf. weiterer Eigenschaften (sogenannter Claims) an den TGIC-Service. Dieser sollte das Security-Token wiederum über den ISTS prüfen, bevor auf dessen Basis eine Berechtigung des Service-Nutzers erfolgen kann.

2.2 User Agent

Die Software, die ein Nutzer implizit verwendet, um auf die Schnittstellen des ITC zuzugreifen bzw. einen TGIC-Webservice zu nutzen, wird als User Agent (UA) bezeichnet. Dies betrifft vor allem Nutzer, die keine Mitgliedsunternehmen des GDV e.V. sind und deshalb nicht über das GDV-Netz auf das ITC zugreifen können. Der technische Aufruf eines TGIC-Services des Service-Betreibers in der TGIC durch den User Agent geschieht nach erfolgreicher Ausstellung eines Security Token durch den ISTS letztendlich direkt.

Es gibt keinerlei Vorgaben auf welcher technischen Basis ein User Agent zu implementieren ist. Hier ist eine Implementierung basierend auf z.B. Java, .NET, SAP oder einer Hardware-Appliance denkbar.

2.3 Akteure

2.3.1 Service-Nutzer

Service-Nutzer (oder Nutzer) rufen Services von Service-Betreibern in der TGIC auf und benötigen dazu einen Authentication-Token des ISTS. Authentication-Token wird hier synonym für Security-Token verwendet, da das Security-Token, das der ISTS ausstellt, später zur Authentifikation gegenüber dem TGIC-Service verwendet wird.

2.3.2 Service-Betreiber

Der Service-Betreiber (oder Betreiber) bietet Services in der TGIC an. Im Rahmen der Bereitstellung der Services müssen diese beim TGIC-Service-Register registriert werden. Betreiber von TGIC-Services sind insbesondere Versicherungsunternehmen (VU) oder in der TGIC registrierte Behörden sowie weitere Kommunikations- und Geschäftspartner der VU. Im Rahmen der Nutzerverwaltung werden allerdings auch durch den ISTS entsprechende Services betrieben, die als TGIC-Services registriert werden.

2.4 Schnittstellen

2.4.1 Insurance Security Token Service (ISTS)

Der ISTS stellt dem Nutzer die relevanten Schnittstellen für den Bezug und Widerruf eines Security-Tokens zur Verfügung.

Mit der Webservice-Operation “Issuance Binding“ kann der Nutzer einen Security-Token beim ISTS beantragen. Im Rahmen der Token-Beantragung muss der Nutzer sich, abhängig von den für den Nutzer aktivierten und vom ausgewählten TGIC-Service unterstützten Authentifizierungsmechanismen, mit einem der vier möglichen Verfahren mTAN, TOTP, nPA oder X.509 (bei Maschinen) authentifizieren.

Mit der Webservice-Operation “Cancel Binding“ kann der Nutzer einen Security-Token widerrufen/sperren, wenn der Verdacht besteht, dass ein Token kompromittiert wurde.

Die beiden genannten Operationen müssen von einem User Agent implementiert werden, damit die Webservice-Schnittstelle genutzt werden kann.

2.4.2 TGIC-Nutzerverwaltung

Über einen Zugang zum GDV-Netz steht Organisations-Verwaltern die TGIC-Nutzerverwaltung über eine Web-Applikation im vollen Funktionsumfang zur Verfügung. (https://user.tgic.gdv.org/TGIC-Nutzerverwaltung). Für berechtigte Personen wurde im Rahmen der Registrierung ein TGIC-Kennwort für die Nutzung der Web-Oberfläche generiert, dass ihnen via E-Mail zugeschickt wurde.

Verwalter einer Organisation mit entsprechenden Berechtigungen können über die Web-Oberfläche der Nutzerverwaltung Nutzerprofile anlegen, ändern, suspendieren und reaktivieren.

Organisations-Nutzern und Selbstpflegern steht ausschließlich der TGIC-Webservice der Nutzerverwaltung zur Verfügung.

Selbstpfleger können über die Webservice-Schnittstelle bestimmte eigene Attribute ändern, wohingegen ein Organisations-Nutzer nur lesenden Zugriff auf die eigenen Attribute hat.

2.4.3 Public Key Infrastruktur

Das ITC stellt eine an die Anforderungen des ISTS angepasste Public Key Infrastruktur (PKI) zur Verfügung. Die PKI ist die Komponente des ITC, die für das Ausstellen und Verteilen von digitalen Zertifikaten zuständig ist. Diese Zertifikate werden vor allem im Rahmen der Token–Beantragung mit dem X.509-Authentifizierungsverfahren genutzt.

Der Zugriff auf die PKI wird durch eine Web-Oberfläche ermöglicht.

Die für Webservice-Nutzer relevanten Schnittstellen sind im Folgenden beschrieben:

- Bereitstellung der CA-Zertifikate des ITC (https://pki.tgic.de/TGIC-PKI).

- Bereitstellung des Schlüsselspeichers (Keystore) zur X.509-Authentifizierung für einen Nutzer (https://pki.tgic.de/TGIC-PKI). Wurde im Rahmen der Nutzerregistrierung X.509 als Authentifizierungsverfahren aktiviert, wird durch die PKI ein privater Schlüssel und ein öffentliches Zertifikat generiert und in Form eines Schlüsselspeichers dem Nutzer zum Download bereitgestellt (https://pki.tgic.de/TGIC-PKI).

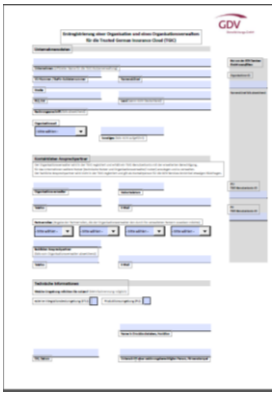
- Bereitstellung der jeweils aktuellen Certificate Revocation List (CRL) des ITC (https://pki.tgic.de/TGIC-PKI/TGIC-CA.crl).

3 Registrierungsprozess

Versicherungsunternehmen, die einen Service in der TGIC nutzen oder anbieten möchten, müssen erstmalig ihre Organisation bzw. ihren Service in der TGIC registrieren lassen. Die entsprechenden Registrierungsformulare können Sie unter tgic-serviceregistrierung@gdv-dl.de anfordern.

Partnerunternehmen und Kommunikationspartner, die kein Mitgliedsunternehmen des GDV e.V. sind, benötigen zuvor eine entsprechende Freigabe durch ein Mitgliedsunternehmen des GDV e.V. und können sich anschließend ebenfalls registrieren lassen.

3.1 Registrierung einer Organisation mit Organisations-Verwalter



Für die erstmalige Registrierung einer Organisation ist das entsprechende PDF-Formular auszufüllen, mit einem Unternehmensstempel zu versehen und durch eine im Unternehmen zeichnungsberechtigte Person unterschreiben zu lassen. Das gescannte Formular senden Sie anschließend bitte an tgic-serviceregistrierung@gdv-dl.de. Nach erfolgreicher Einrichtung und Freischaltung erhalten Sie eine E-Mail zur Bestätigung mit Angabe der Organisations-ID, unter der das Unternehmen in der TGIC geführt wird.

Wir empfehlen Versicherungsunternehmen, die einen Zugang zum GDV-Netz haben, direkt einen Organisations-Verwalter registrieren zu lassen. Dieser erhält die Berechtigung, weitere Nutzer (natürliche Personen oder technische Nutzer) für seine Organisation in der TGIC anzulegen und zu pflegen.

Bitte beachten Sie, dass einige TGIC-Services ihre Nutzung für einige Personenkreise einschränken und gewisse Partner-Rollen voraussetzen. Die notwendigen Informationen und Anforderungen zur Servicenutzung erhalten Sie bei dem jeweiligen Serviceanbieter bzw. entnehmen Sie der jeweiligen Projektdokumentation.

Bitte geben Sie daher bei der Registrierung des Organisations-Verwalters die Partner-Rollen an, die zur weiteren Nutzung benötigt und bei Nutzeranlage vergeben werden sollen. Die Partner-Rollen können nicht eigenständig erweitert, sondern nur zentral bei der GDV Dienstleistungs-GmbH gepflegt werden.

3.2 Nachträgliche Registrierung eines Organisations-Verwalters

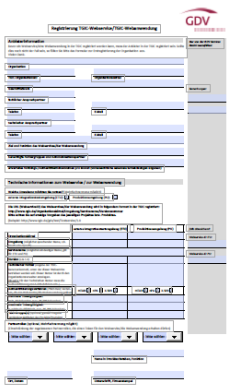
Hat ihre in der TGIC registrierte Organisation noch keinen Organisations-Verwalter, dann füllen Sie bitte das Formular zur Änderung einer Organisation aus. Da Ihre Unternehmensdaten bereits in der TGIC-Nutzerverwaltung vorhanden sind, ist es nicht notwendig, dass Sie nochmals alle Felder befüllen. Bitte geben Sie nur unter Organisation ihre Organisations-ID an, zu welcher der Organisations-Verwalter eingerichtet werden soll. Die Person erhält nach erfolgreicher Einrichtung eine automatische Willkommens-E-Mail mit den entsprechenden Zugangsdaten.

Bitte beachten Sie, dass einige TGIC-Services ihre Nutzung für einige Personenkreise einschränken und gewisse Partner-Rollen voraussetzen. Die notwendigen Informationen und

Anforderungen zur Servicenutzung erhalten Sie bei dem jeweiligen Serviceanbieter bzw. entnehmen Sie der jeweiligen Projektdokumentation.

Bitte geben Sie daher bei der Registrierung des Organisations-Verwalters die Partner-Rollen an, die zur weiteren Nutzung benötigt und bei Nutzeranlage vergeben werden sollen. Die Partner-Rollen können nicht eigenständig erweitert, sondern nur zentral bei der GDV Dienstleistungs-GmbH gepflegt werden.

3.3 Registrierung eines TGIC-Services



Registrierte Versicherungsunternehmen bzw. bereits angebundene Partnerunternehmen können Webservices und Webanwendungen in der TGIC registrieren lassen, um die sichere Infrastruktur und die Authentifizierungsmethoden des ITC nutzen zu können.

Dabei bestehen folgende Möglichkeiten:

- Sie bieten einen Branchenservice an, der von ihrer Organisation selbst betrieben wird. Die Nutzung des Service kann durch die Einschränkung der zulässigen Partner-Rollen reglementiert werden.

- Sie bieten einen unternehmensindividuellen Service an und nutzen ausschließlich die Authentifizierungsfunktion des ITC für Ihre Nutzer.

- Sie bieten einen Service an, der unter Einhaltung der Architektur- und Sicherheitsrichtlinien der GDV Dienstleistungs-GmbH, im sicheren, vom BSI zertifizierten Rechenzentrum im IT Verbund TGIC betrieben werden soll.

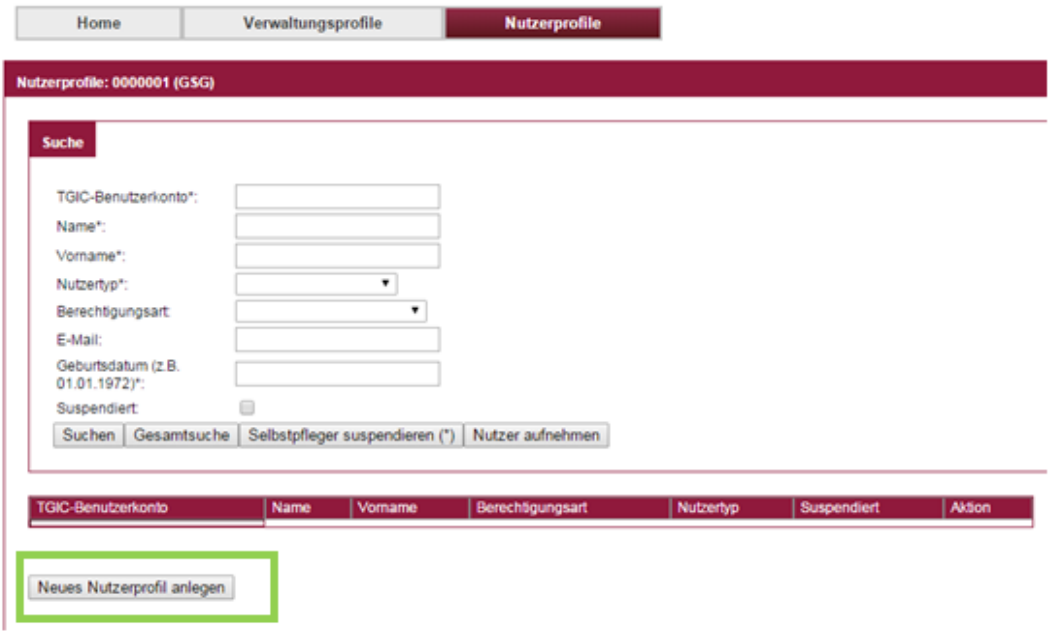
4 Typische Anwendungsfälle

4.1 Anlegen eines TGIC-Benutzerkontos

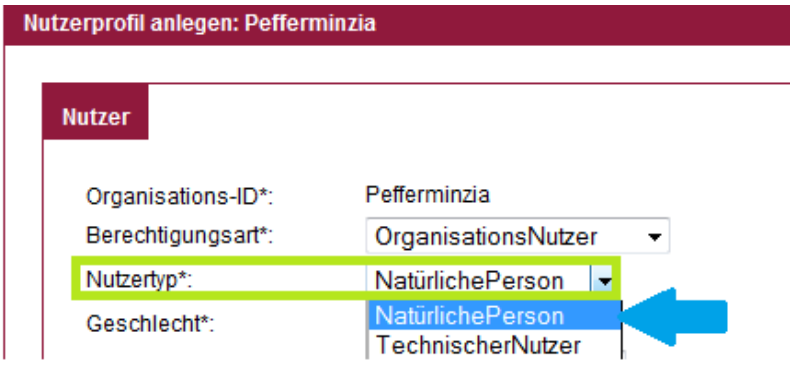
Sie können als Organisations-Verwalter neue Nutzerkonten (Organisations-Verwalter, Organisations-Nutzer, Selbstpfleger sowie technische Nutzer) mit verschiedenen Authentifizierungsoptionen anlegen. Bitte beachten Sie, dass Sie den Nutzern ausschließlich die Partnerrollen vergeben können, die bei Ihnen selbst im Profil aktiviert sind.

4.1.1 Anlegen eines Benutzerkontos als natürliche Person mit mTAN-Authentifizierung

Um ein neues Nutzerprofil anzulegen, klicken Sie zunächst auf "**Neues Nutzerprofil anlegen**".



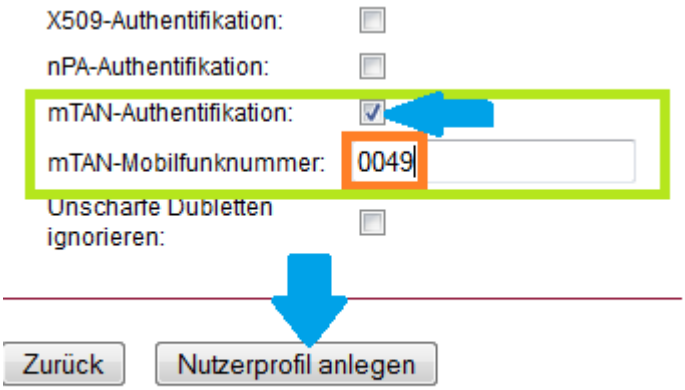
Bitte wählen Sie als Nutzertyp „Natürliche Person" aus.



Anschließend geben Sie die gesamten Nutzerdaten ein (die mit * markierten Felder sind Pflichtfelder). Für die Authentifikation wählen Sie in diesem Fall „mTAN-Authentifikation“ aus und geben die Telefonnummer an, mit der die mTAN-Authentifikation erfolgen soll.

Bitte beachten Sie bei der Eingabe der Mobilfunknummer die Vorwahl (0049). Es können ausschließlich deutsche Telefonnummern eine mTAN erhalten.

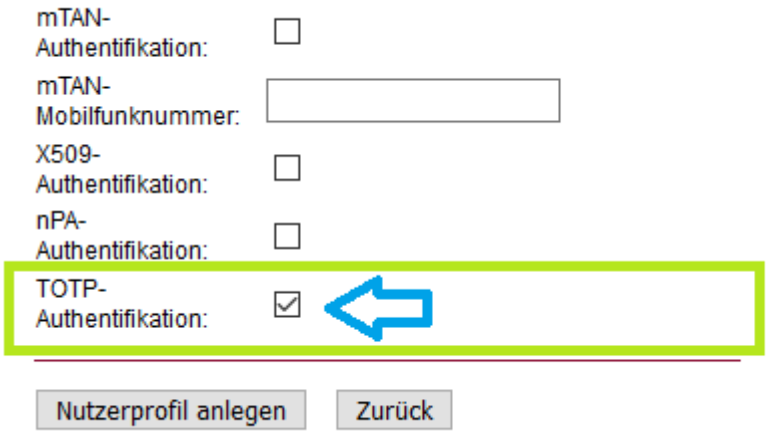
Zum Anlegen des Nutzerprofils betätigen Sie den Button „Nutzerprofil anlegen“.



4.1.2 Anlegen eines Benutzerkontos als natürliche Person mit TOTP-Authentifizierung

Gehen Sie bitte zur Anlage eines Nutzers mit TOTP-Authentifizierung bitte analog zum beschriebenen Prozess zur Anlage eines Nutzers mit mTAN-Authentifizierung vor.

Abweichend hierbei ist die Auswahl des Authentifikationsverfahrens: TOTP.



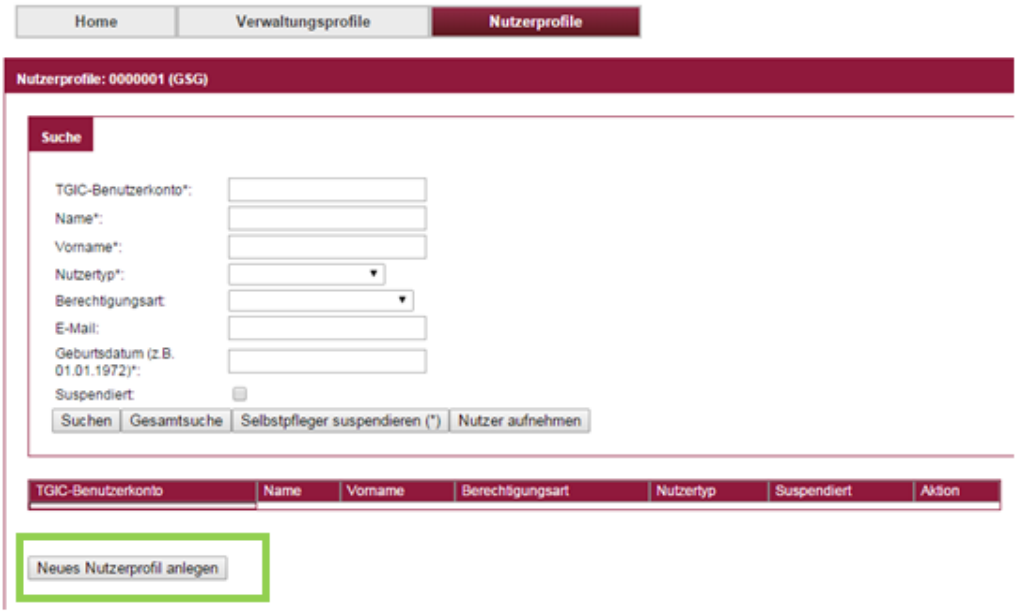
Nach einem Klick auf den Button „Nutzerprofil anlegen“ wird an den Nutzer automatisch eine E-Mail versendet, die u. A. den QR Code zum Einscannen in den TOTP Client enthält.

Hinweis: Das mTAN Verfahren und das TOTP Verfahren schließen sich NICHT gegenseitig aus. Es ich möglich einem Nutzer beide Verfahren gleichzeitig zuzuordnen!

4.1.3 Anlegen eines Benutzerkontos als technischer Nutzer mit X.509-Authentifizierung

Ein Technischer Nutzer mit aktivierter X.509-Authentifizierungsmethode ist zwingend erforderlich, um einen TGIC-Webservice nutzen zu können.

Um ein neues Nutzerprofil anzulegen, klicken Sie zunächst auf "**Neues Nutzerprofil anlegen**".



Bitte geben Sie die Daten des Ansprechpartners hinter dem Technischen Nutzer ein und wählen anschließend als Nutzertyp „Technischer Nutzer" sowie X.509-Authentifikation aus und betätigen abschließend „Nutzerprofil anlegen".

Möchten Sie nachträglich für den Nutzer die Authentifizierungsart „X.509" aktivieren, so rufen Sie das gewünschte Nutzerprofil auf und setzen einen Haken bei „Neuausstellung X.509" und gehen zum Download und zur Aktivierung des X.509-Zertifikates wie unter 3.6a beschrieben vor.

4.2 Bearbeitung des TGIC-Benutzerkontos

Zum Bearbeiten eines TGIC-Benutzerkontos geben Sie eines der benötigten Suchparameter ein und betätigen „Suchen". Danach sollte der gewünschte Benutzer unter der Suchmaske erscheinen, sofern Sie zur Verwaltung dieses Benutzers berechtigt sind.

Gehen Sie auf „Nutzerprofil bearbeiten" und ändern das gewünschte Attribut. Bitte vergessen Sie nicht, abschließend „Änderungen speichern" zu betätigen.

Hinweis zum Format von Telefonnummern:

Die Telefonnummer muss im Format 0049 1… eingetragen werden.
Es können ausschließlich deutsche Telefonnummern eine mTAN erhalten.

4.3 TGIC-Kennwörter

Nach erfolgreicher Registrierung in der TGIC geht dem Nutzer eine E-Mail zur Bestätigung zu. Direkt im Anschluss wird in einer gesonderten E-Mail initial das 12-stellige TGIC-Kennwort an den Nutzer verschickt. Über die Anwendungsoberfläche des Services oder direkt über die TGIC-Kennwortverwaltung (https://userpw.tgic.de/TGIC-Kennwortverwaltung_www/index.xhtml) besteht die Möglichkeit, das Kennwort zu ändern.

Das Initialkennwort, das bei der Registrierung vergeben wird, hat immer 12 Zeichen und kann anschließend nach den unten genannten Richtlinien geändert werden.

Bei 5 fehlgeschlagenen Login-Versuchen wird der Account temporär für 30 Minuten gesperrt. Für diesen Zeitraum sind der Zugang zur Nutzerverwaltung sowie die Authentifizierung mit mTAN nicht möglich.

Folgende Regeln für die Vergabe und Änderung von Kennwörtern gelten:

1. für Organisations-Nutzer und Selbst-Pfleger

a) Kennwörter müssen mindestens 8 Zeichen lang sein.

b) Kennwörter müssen eine Kombination aus Groß- und Kleinbuchstaben, Zahlen und Sonderzeichen sein:

- davon jeweils mindestens 1 Großbuchstabe, 1 Kleinbuchstabe, 1 Sonderzeichen und 1 Ziffer
- Leerzeichen sind nicht zulässig

c) Das Kennwort muss ein Mal pro Jahr geändert werden.

d) Das zuletzt verwendete Kennwort kann nicht wiederverwendet werden.

2. für Organisations-Verwalter

a) Kennwörter müssen mindestens 12 Zeichen lang sein.

b) Kennwörter müssen eine Kombination aus Groß- und Kleinbuchstaben, Zahlen und Sonderzeichen sein:

- davon jeweils mindestens 1 Großbuchstabe, 1 Kleinbuchstabe, 3 Sonderzeichen und 3 Ziffern
- Leerzeichen sind nicht zulässig

c) Das Kennwort muss ein Mal pro Jahr geändert werden.

d) Die letzten 6 genutzten Kennwörter können nicht wiederverwendet werden.

Das TGIC-Support-Team empfiehlt, längere und komplexe Kennwörter als oben erwähnt zu verwenden.

4.4 Zurücksetzung des TGIC-Kennwortes

Organisations-Verwalter haben die Möglichkeit, über das GDV-Netz das Kennwort in der Web-Oberfläche der TGIC-Nutzerverwaltung explizit für Nutzer Ihrer Organisation zurückzusetzen. Dies kann in der Web-Oberfläche der Nutzerverwaltung mit dem Button “Kennwort zurücksetzen“ erfolgen. Daraufhin wird vom System ein neues Kennwort generiert, das dem Nutzer in einer E-Mail mitgeteilt wird.

Eine Zurücksetzung des TGIC-Kennwortes kann auch über den Support des von Ihnen genutzten Services (Fachanwendung) erfolgen.

4.5 Widerruf von X.509-Zertifikaten

Ein X.509-Nutzerzertifikat kann durch den Verwalter einer Organisation widerrufen werden, wenn der Verdacht auf eine missbräuchliche Nutzung des privaten Schlüssels besteht.

Das Widerrufen eines Nutzerzertifikats kann in der Web-Oberfläche der TGIC-Nutzerverwaltung durchgeführt werden. Dafür ist der Button “Zertifikat sperren“ im Nutzerprofil des Technischen Nutzers zu betätigen.

Um den Nutzer von der Sperrung seines X.509-Zertifikats zu informieren, wird vom System automatisch eine E-Mail an ihn gesendet.

4.6 Neuausstellung von X.509-Zertifikaten

X.509-Zertifikate haben eine Maximalgültigkeit von einem Jahr ab Ausstellung. Um fortlaufend das hohe Sicherheitsniveau zu gewährleisten, muss gegen Ende dieses Zeitraums das jeweilige Zertifikat zwingend gegen ein neues ausgetauscht werden. Damit ein reibungsfreier Zertifikatsaustausch und unterbrechungsfreier Betrieb sichergestellt werden können, werden die Nutzer 30 Tage vorher über den Ablauf der Gültigkeit informiert.

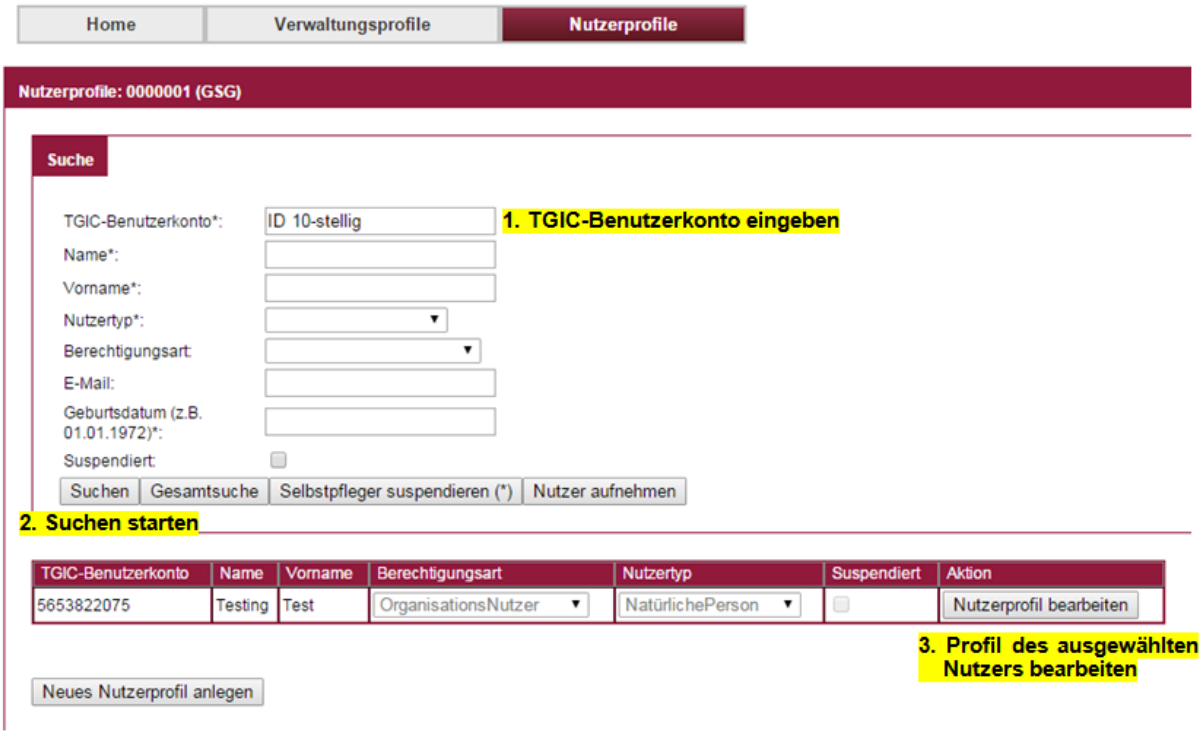
Sollten Sie die Webservice-Schnittstelle nicht nutzen, ist kein Zertifikatswechsel erforderlich. Ein Austausch des Zertifikats ist nur für Nutzer der Webservice-Schnittstelle relevant.

X.509-Zertifikate können in folgenden Fällen neu ausgestellt werden.

a) Sie möchten die X.509-Authentifizierung erstmalig aktivieren, ein Zertifikat wurde gesperrt oder ist abgelaufen, oder Sie möchten in dem Zeitraum ab 30 Tage vor Ablauf ihr X.509-Zertifikat erneuern.

b) Das Zertifikat wurde nicht innerhalb von 30 Tagen nach Erhalt der Registrierungs-E-Mail heruntergeladen bzw. aktiviert oder ist länger als 30 Tage gültig.

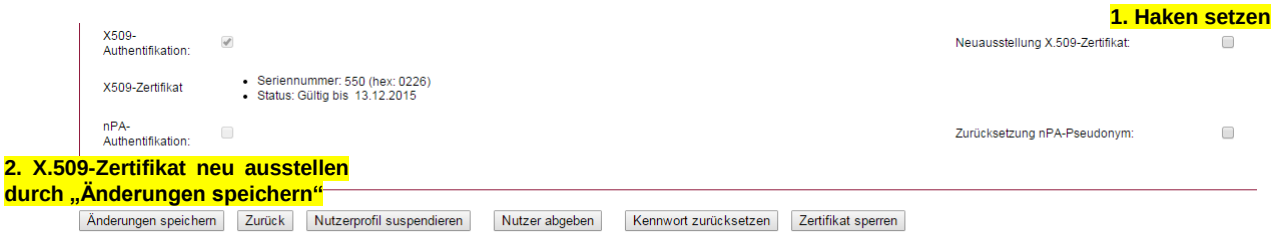
Die Neuausstellung von Zertifikaten für technische Nutzer einer Organisation kann durch einen für diese Organisation zuständigen Organisations-Verwalter über die Web-Oberfläche der TGIC-Nutzerverwaltung erfolgen. Zuerst trägt der Organisations-Verwalter die ID des TGIC-Benutzerkontos ein, für die er das Zertifikat neu ausstellen möchte. Nach Beendigung des Suchvorgangs wählt er die Aktion „Nutzerprofil bearbeiten“.



Zu a)

Sie möchten die X.509-Authentifizierung erstmalig für einen technischen Nutzer aktivieren, ein Zertifikat wurde widerrufen (gesperrt) oder Sie möchten in dem Zeitraum ab 30 Tage vor Ablauf ihr X.509-Zertifikat erneuern:

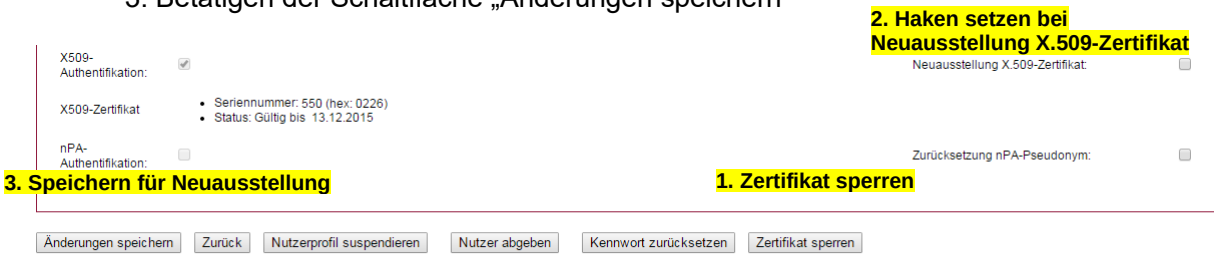
1. Setzen des Hakens bei „Neuausstellung X.509-Zertifikat“
2. Betätigen der Schaltfläche „Änderungen speichern“



Zu b)

Das Zertifikat wurde nicht innerhalb von 30 Tagen nach Erhalt der Registrierungs-E-Mail heruntergeladen bzw. aktiviert oder es ist noch länger als 30 Tage gültig:

1. Betätigen der Schaltfläche „Zertifikat sperren“
2. Setzen des Hakens bei „Neuausstellung X.509-Zertifikat“
3. Betätigen der Schaltfläche „Änderungen speichern“

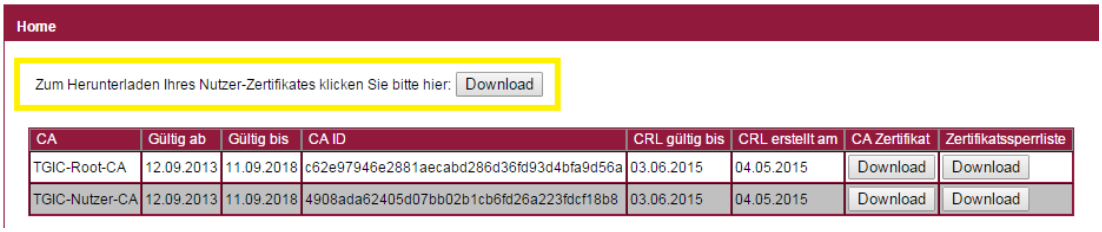


Nach Ausführen der Aktion „Zertifikat sperren“ ist das alte X.509-Zertifikat sofort ungültig und kann nicht mehr verwendet werden.

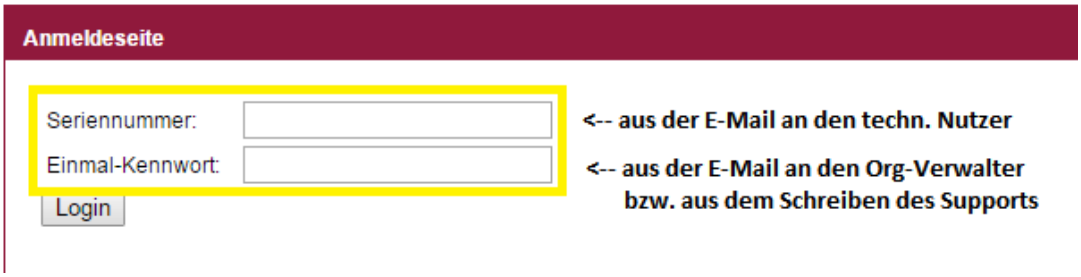
Nach Anforderung des neuen X.509-Zertifikats erhält der technische Nutzer an seine in der TGIC hinterlegte E-Mail-Adresse Informationen für das Herunterladen des neuen X.509-Zertifikats. Zusätzlich wird an den Organisations-Verwalter, der die Neuausstellung des X.509-Zertifikats über die TGIC-Nutzerverwaltung veranlasst hat, eine E-Mail mit einem „Einmal-Kennwort“ versendet, welches für das Herunterladen des neuen X.509-Zertifikats benötigt wird. Das Einmal-Kennwort verliert nach der Aktivierung des X.509-Zertifikates seine Gültigkeit.

Hinweis: Sofern die Neuausstellung des X.509-Zertifikats über den Support (also nicht durch einen Organisations-Verwalter der eigenen Organisation) veranlasst wurde, wird das Einmal-Kennwort aus Sicherheitsgründen auf dem Postweg an den technischen Nutzer versendet.

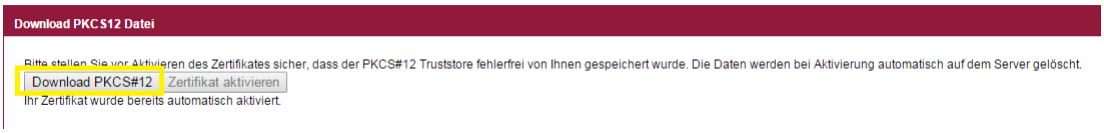
Nach Aufruf des Links für das Herunterladen des neuen X.509-Zertifikats im Webbrowser ist dort die obere Schaltfläche „Download“ auszuwählen:



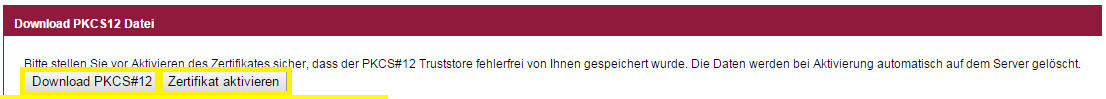
In der danach angezeigten Anmeldemaske sind dann die via E-Mail bzw. auf dem Postweg erhaltenen Daten einzugeben:



Sofern das X.509-Zertifikat erstmalig ausgestellt wurde oder vor der Neustellung gesperrt war, ist das neue X.509-Zertifikat automatisch aktiviert, das Zertifikat kann nach Download und Speicherung des PKCS#12 Truststores sofort genutzt werden:



Bei der Neuausstellung eines X.509-Zertifikats für einen technischen Nutzer, dessen altes X.509-Zertifikat innerhalb der nächsten 30 Tage abläuft, wird die nachstehende Maske zum Herunterladen und anschließenden Aktivieren angezeigt:



1. Download mit an-schließender Speicherung

2. Zertifikat aktivieren

In diesem Fall bleibt das alte X.509-Zertifikat so lange gültig, bis das neue X.509-Zertifikat durch Betätigung der Schaltfläche „Zertifikat aktivieren“ aktiviert wurde (oder das reguläre Ende der Gültigkeit des alten X.509-Zertifikats erreicht wurde). Bitte beachten Sie, dass Sie innerhalb der 30-Tages-Frist das heruntergeladene Zertifikat aktivieren müssen.

4.7 Löschung von Nutzer- und Organisationskonten in der TGIC

Die Löschung des TGIC-Benutzerkontos bewirkt, das Sie sich für sämtliche TGIC-Services nicht mehr authentifizieren können. Möchten Sie einzelne TGIC-Services nicht mehr nutzen, wenden Sie sich bitte an den Support des jeweiligen Serviceanbieters, der Sie aus seiner Nutzerverwaltung (falls vorhanden) löscht.

Nutzer und Organisationen können nicht direkt aus der TGIC-Nutzerverwaltung gelöscht werden, sondern müssen zunächst suspendiert werden. Dazu muss in der Web-Oberfläche der Nutzerverwaltung der Button “Nutzerprofil suspendieren“ betätigt werden. Dadurch wird der Nutzer deaktiviert und nach 30 Tagen aus dem System unwiderruflich gelöscht. Innerhalb dieser 30 Tage ist eine Reaktivierung von suspendierten Nutzern in der Nutzerverwaltung durch Betätigen des Buttons “Nutzerprofil reaktivieren“ jederzeit möglich.

Organisations-Nutzer können nur von einem Verwalter der entsprechenden Organisation suspendiert oder reaktiviert werden. Der Organisations-Verwalter muss dafür mindestens die Partnerrollen des Organisations-Nutzers besitzen.

Die Suspendierung von Organisationen kann nur zentral durch die GDV Dienstleistungs-GmbH vorgenommen werden. Der zugehörige Prozess kann über den Support des von Ihnen genutzten Services (Fachanwendung) oder mittels E-Mail an tgic-serviceregistrierung@gdv-dl.de initiiert werden.

Wird eine Organisation suspendiert, werden automatisch auch alle Nutzer der Organisation suspendiert. Bei der Reaktivierung einer Organisation werden automatisch auch alle suspendierten Verwalter der entsprechenden Organisation reaktiviert (nicht aber die übrigen Nutzer, die dann ggf. von den Verwaltern einzeln reaktiviert werden müssen). Es ist in diesem Zusammenhang auch zu beachten, dass für einen suspendierten Nutzer alle ausgestellten Security Token implizit widerrufen werden.

4.8 Änderung von Benutzerdaten für Selbstpfleger

Im Gegensatz zu Organisations-Nutzern, ist es Selbstpflegern möglich, einige ihrer Attribute über den TGIC-Webservice der Nutzerverwaltung selbst zu pflegen.

Folgende eigene Attribute können von Selbstpflegern geändert werden:

- Akademischer Grad
- Nachname
- Anschrift
- E-Mail
- mTAN-Telefonnummer

Darüber hinaus können Selbstpfleger ihr nPA-Pseudonym zurücksetzen.