GDV Dienstleistungs-GmbH

Trusted German Insurance Cloud (TGIC)
Insurance Security Token Service (ISTS)



FAQ
Frequently Asked Questions

Stand: 01.10.2025

Inhaltsverzeichnis

1 Einleitung, Links und Kontaktadressen 4
2 Glossar der relevanten Begriffe im TGIC-Umfeld (Alt) 5
2.1 Authentifizierungsverfahren 5
2.2 BranchenNetz / GDVnetz 6
2.3 Insurance Security Token Service (ISTS) 6
2.4 Insurance Trust Center (ITC) 7
2.5 Insurance Security Authorisation Service (ISAS) 7
2.6 Kategorie 7
2.7 Nutzer 7
2.8 Nutzerarten 8
2.9 Nutzertypen 8
2.10 Organisationen 8
2.11 OrganisationsNutzer 9
2.12 OrganisationsVerwalter 9
2.13 Partner-Rollen 9
2.14 Public Key Infrastruktur (PKI) 9
2.15 Security Token 9
2.16 SelbstPfleger 10
2.17 Service-Betreiber 10
2.18 Service-Nutzer 10
2.19 Technische Nutzer 10
2.20 TGIC-Nutzer 11
2.21 TGIC-Nutzerverwaltung 11
2.22 TGIC-Organisation 11
2.23 TGIC-Services 11
2.24 Token 12
2.25 Trusted German Insurance Cloud (TGIC) 12

2.26 Trusted Partner 12
2.27 User Agent 12
2.28 X.509 Zertifikat 12
2.29 Zertifikat 13
3 TGIC - Registrierungsprozesse 14
3.1 Registrierung einer Organisation mit OrganisationsVerwalter 14
3.2 Nachträgliche Registrierung eines Organisations-Verwalters 15
3.3 Registrierung eines TGIC-Services 15
4 TGIC - Systemkontext 17
4.1 Aufruf eines TGIC-Services 17
4.2 User Agent 17
4.3 Akteure 17
4.3.1 Service-Nutzer 17
4.3.2 Service-Betreiber 18
4.4 Schnittstellen 18
4.4.1 Insurance Security Token Service (ISTS) 18
4.4.2 TGIC-Nutzerverwaltung 18
4.4.3 Public Key Infrastruktur 19
5 Typische Anwendungsfälle 20
5.1 Anlegen eines TGIC-Benutzerkontos 20
5.2 Bearbeitung des TGIC-Benutzerkontos 20
5.3 TGIC-Kennwort ändern/zurücksetzen 21
5.4 Zurücksetzung des TGIC-Kennwortes 22
5.5 Widerruf von X.509-Zertifikaten 22
5.6 Neuausstellung von X.509-Zertifikaten 23
5.7 X.509-Zertifikats-Download 24
5.8 Löschung von Nutzer- und Organisationskonten in der TGIC 25

1 Einleitung, Links und Kontaktadressen

Wir freuen uns, Sie als Nutzer in der TGIC und der Authentifizierungsdienste des Insurance Trust Centers (ITC) begrüßen zu dürfen. Die TGIC Kommunikationsinfrastruktur ist fester Bestandteil der IT Landschaft der deutschen Versicherungswirtschaft, die von immer mehr Service genutzt wird. Aus diesem Grund 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.

Wichtige Links:

TGIC-Nutzerverwaltung: Nur im Branchennetz aufrufbar	https://user.tgic.gdv.org/TGIC-Nutzerverwaltung
TGIC-Kennwortverwaltung:	https://userpw.tgic.de/TGIC-Kennwortverwaltung_www/index.xhtml
TGIC Public Key Infrastruktur: z.B. für x.509 Zertifikate	https://pki.tgic.de/TGIC-PKI

Kontaktadressen:

TGIC-Support	tgic-support@gdv-dl.de

2 Glossar der relevanten Begriffe im TGIC-Umfeld (Alt)

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.

2.1 Authentifizierungsverfahren

Eine Authentifikation in der TGIC findet über eine Zwei Faktor Authentifikation (2FA) besonders sicher ab. Als 2 Faktor stehen dafür in der TGIC derzeit die folgenden Authentifizierungsverfahren zur Verfügung, die von jedem Serviceanbieter individuell für seine Servicenutzung vorausgesetzt werden können.
Für natürliche Personen stehen zur Authentifizierung das "Time-based One-time Password (TOTP)" sowie das „mobile Transaktionsnummer (mTAN)" Verfahren zur Verfügung.

Für technische Nutzer steht ausschließlich die X.509-Authentifikation zur Verfügung.

- TOTP-Verfahren
  für natürliche Personen kann das Verfahren „**T**imebased **O**ne**t**ime **P**assword“ (TOTP) verwendet werden. Hierzu gibt es mehrere Optionen:
  - Es besteht die Möglichkeit eine Applikation für den persönlichen Desktop, diese erhalten Sie über unseren TGIC-Support. Hier muss die persönliche TGIC-ID eingetragen werden, die Applikation erstellt alle 30 Sekunden einen neuen Zugriffscode.
  - Es besteht die Möglichkeit unterschiedliche Authenticator Apps auf dem Mobiltelefon zu nutzen u.a. den "Google-Authenticator", IOS-App "Passwords" und die IBM App "IBM-Verify".
- mTAN-Verfahren
  für natürliche Personen wird diese Zweifaktor-Authentifizierung dann ein sicheres Instrument, wenn der Nutzer ein zweites Gerät wie zum Beispiel sein mobiles Gerät verwendet um eine vom System generierte **m**obile **T**rans**a**ktions**n**ummer (mTAN), zugestellt zu bekommen, die dann vom Nutzer zusätzlich zum Passwort eingegeben wird.
  Hinweise:
  - Zur Nutzung des Verfahrens werden ausschließlich Nummern aus dem nationalen Raum (0049) zugelassen.

    - Bitte beachten Sie, dass beim mTAN-Verfahren nur in der Produktionsumgebung der TGIC reale SMS zur Ausstellung einer mTAN versendet und dem Serviceanbieter entsprechend in Rechnung gestellt werden. Für Tests in einer Testumgebung (ETU/ITU) wird eine immer gültige mTAN
      zur Authentifizierung simuliert, also auf eine reale SMS verzichtet.
- X.509-Authentifikation (Maschine ↔ Maschine Kommunikation)
  Technische Nutzer (Maschine-Maschine-Schnittstelle) authentifizieren sich ausschließlich über X.509-Zertifikaten.
- VU-Auth
  VU-Auth ist ein besonderes Authentifikationsverfahren, welches von TGIC Organisationen implementiert werden kann. Dieses komfortable Verfahren vereinfacht die Anmeldung für Nutzer an einem TGIC Service. Die Authentifikation findet im Hintergrund durch das eigene Unternehmen statt, wodurch sich der Nutzer ohne eigene Authentifikation an einen TGIC Service anmelden kann, ähnlich einem Single Sign On verfahren.

2.2 BranchenNetz / GDVnetz

Das Branchennetz arbeitet als geschlossener Kanal abgeschirmt vom sonstigen Datenverkehr über genau bekannte Leitungen. Das Branchennetz umfasst sowohl die gemeinsame technische Plattform GDVnetz als auch fachliche Services, u.a. AVmG, GDV-Schaden sowie Versicherungsvermittler, die ausschließlich über das GDVnetz zur Verfügung gestellt werden. Für die Nutzung der o.a. Services gelten einige grundlegende Regelungen. Diese sind notwendig, um eine störungsfreie und problemlose Kommunikationsbeziehung betreiben zu können.

Das Branchennetz ist für Versicherungsunternehmen und IT-Dienstleister interessant. Der Anschluss an das Branchennetz ist mit einigem Aufwand und auch mit Kosten verbunden. Der Anschluss an dieses Netz muss über den GDV beantragt werden. Bei Versicherern besteht dieser Zugang in der Regel bereits.

2.3 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.

2.4 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, die dafür notwendigen TGIC-Benutzerkonten zu verwalten und die nötigen Daten für eine Berechtigung durch den TGIC-Service zu liefern.

2.5 Insurance Security Authorisation Service (ISAS)

Der Insurance Security Authorisation Service ist eine Erweiterung zum ITC zur Abbildung von Autorisierungen für TGIC-Services. Der Service-Betreiber kann über den ISTS-Betreiber die Anlage und Zuordnung einer Berechtigungsgruppe mit Berechtigungsrollen beantragen.

2.6 Kategorie

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

Die Vergabe der Kategorie an Nutzer erfolgt durch den OrganisationsVerwalter. Jedoch können nur die Kategorien vergeben werden, die der OrganisationsVerwalter selbst innehat. Es empfiehlt sich, bei der Beantragung eines OrganisationsVerwalters direkt im Registrierungsformular, die für die Servicenutzung erforderlichen Kategorien auszuwählen. Welche Kategorien erforderlich sind, erfahren Sie bei dem jeweiligen Service-Anbieter.

2.7 Nutzer

Siehe TGIC-Nutzer

2.8 Nutzerarten

Es wird zwischen folgenden Nutzerarten unterschieden, die im Rahmen des Nutzerkonzepts der TGIC-Nutzerverwaltung relevant sind:
OrganisationsVerwalter: Ein OrganisationVerwalter ist berechtigt, über die Nutzerverwaltung neue OrganisationsNutzer anzulegen und zu pflegen bzw. SelbstPfleger 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 über das geschlossene GDVnetz zu erreichen ist, steht dieser Zugangsweg ausschließlich GDV-Mitgliedsunternehmen zur Verfügung. Alle Organisationen können ebenfalls übers Internet auf die Schnittstelle der TGIC-Nutzerverwaltung zugreifen.
OrganisationsNutzer: Beispielsweise Angestellte der Organisation, werden ausschließlich durch die Organisation gepflegt und sind der Organisation in der TGIC-Nutzerverwaltung zugeordnet.
SelbstPfleger: 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.

2.9 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 und TOTP 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.

2.10 Organisationen

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

2.11 OrganisationsNutzer

Organisationsnutzer sind TGIC-Nutzer einer Organisation die keine administrativen Aufgaben innerhalb der TGIC besitzen. Dabei handelt es sich um eine Berechtigungsart in der TGIC. Dies können natürliche Personen sein, die via Web-Auth die TGIC-Anwendung nutzen oder technische Nutzer, die über ein X.509-Zertifikate an die TGIC angebunden werden. Diese werden ausschließlich durch die OrganisationsVerwalter der TGIC-Organisation gepflegt und sind dieser in der TGIC-Nutzerverwaltung zugeordnet.

2.12 OrganisationsVerwalter

Organisationsverwalter sind natürliche Personen innerhalb des Rahmenvertragspartners, die administrativen Zugriff auf die Nutzerverwaltung erhalten. Diese können neue Nutzer in der TGIC registrieren oder löschen, und weitere Organisationsverwalter oder Organisationsnutzer innerhalb ihrer eigenen Organisation oder der Partnerorganisationen anlegen.

2.13 Partner-Rollen

Ersetzt durch Kategorie

2.14 Public Key Infrastruktur (PKI)

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.

2.15 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.

2.16 SelbstPfleger

Selbstpfleger sind TGIC-Nutzer die einer selbstständigen Tätigkeit in Verbindung mit der Versicherungsbranche nachgehen, die Organisationsunabhängig aggieren. Hierbei kann es sich z.B. um Makler oder Rechtsanwälte handeln. Im Rahmen der Nutzung eines TGIC-Service findet die Stammdatenpflege über den Serviceprovider oder dem TGIC-Support statt.

2.17 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.

2.18 Service-Nutzer

Service-Nutzer (siehe auch TGIC-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.

2.19 Technische Nutzer

Technische Nutzer sind angelegte TGIC-Nutzer für die Maschine-zu-Maschinekommunikation, also für automatisierte Abläufe innerhalb der TGIC (bspw. für die automatisierte Kommunikation zwischen Webservices). Das X.509-Authentifzierungsverfahren kann ausschließlich für technische Nutzer aktiviert werden, worüber er das technische X.509 Zertifikat erhält.

2.20 TGIC-Nutzer

Einzelpersonen (natürlichen Personen), die zur Nutzung der TGIC berechtigt werden und ein individuelles TGIC-Nutzerkonto erhalten. Dies sind bspw. Mitarbeiter/innen des Versicherungsunternehmens, Versicherungsvermittler, Mitarbeiter/innen von Gutachtern etc.

Ein TGIC-Nutzer kann entweder vom Typ: "Natürliche Person" oder "Technischer Nutzer" sein. Dabei kann jeder Typ als Nutzerart OrganisationsVerwalter, OrganisationsNutzer oder Selbstpfleger angelegt sein.

2.21 TGIC-Nutzerverwaltung

Eine Webanwendung für TGIC-Organisationsverwalter zur Stammdatenpflege der TGIC-Organisationsnutzer Ihrer TGIC-Organisation. Die TGIC-Nutzerverwaltung ist ausschließlich im GDVnetz erreichbar. Diese wird für jede vorhandene Umgebung vorgehalten und ist über folgende Adressen im GDVnetz erreichbar:

Umgebung	**Adresse**
Produktionsumgebung (PU)	https://user.tgic.gdv.org/TGIC-Nutzerverwaltung/
externe Testumgebung (ETU)	https://exttest-user.tgic.gdv.org/TGIC-Nutzerverwaltung/webpages/

2.22 TGIC-Organisation

Eine in der TGIC registrierte Organisation.

2.23 TGIC-Services

Im Rahmen des TGIC-Konzepts wird ein TGIC-Service (dies kann ein Webservice oder eine Webanwendung sein) von einem VU 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.

2.24 Token

Siehe: Security Token

2.25 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.

2.26 Trusted Partner

Trusted Partner sind Unternehmen, die als Organisation berechtigt werden, Nutzer in der TGIC zu registrieren und entsprechend auch die Nutzer zu identifizieren, damit der Organisationsverwalter die Nutzer in der TGIC anlegen kann.

2.27 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. Hierbei kann es sich z.B. um den Webbrowser handeln.

2.28 X.509 Zertifikat

X.509 Zertifikat werden bei Aktivierung der X.509-Authentifikation für einen im ITC registrierten Nutzer generiert. Neben dem Identitätsnachweis finden diese Zertifikate im Rahmen des Authentifizierungsverfahren durch den ISTS Anwendung, wenn Security Token für den – einem

TGIC-Webservice assoziierten – technischen Nutzer des Webservice-Betreibers verschlüsselt werden.

2.29 Zertifikat

Siehe: X.509 Zertfikate

3 TGIC - Registrierungsprozesse

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-support@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 OrganisationsVerwalter

Für die erstmalige Registrierung einer Organisation haben Sie neben dem TGIC Rahmenvertrag in der Regel das Formular "Erstregistrierung einer Organisation und eines Organisationsverwalters für die Trusted German Insurance Cloud (TGIC)" durch eine im Unternehmen zeichnungsberechtigte Person unterschreiben zu lassen. Dies wird mittels DocuSign zum Ausfüllen und elektronisch Signieren vom TGIC-Support zur Verfügung gestellt. 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 (BranchenNetz) haben, direkt einen OrganisationsVerwalter 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 Kategorien 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 OrganisationsVerwalters die Kategorien an, die zur weiteren Nutzung benötigt und bei Nutzeranlage vergeben werden sollen. Die Kategorien 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. Dies wird mittels DocuSign zum Ausfüllen und elektronisch Signieren vom TGIC-Support zur Verfügung gestellt. 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 OrganisationsVerwalter 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 Kategorien 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 Kategorien können nicht eigenständig erweitert, sondern nur zentral bei der GDV Dienstleistungs-GmbH gepflegt werden.

3.3 Registrierung eines TGIC-Services

Registrierte Versicherungsunternehmen 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 Kategorie und/oder Berechtigungsrollen des ISAS 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.

Die Parteien werden für jeden TGIC-Service, den der Vertragspartner anbieten möchte, einen separaten Leistungsschein zeichnen. Der Leistungsschein enthält eine Beschreibung des TGIC-Service, die im Hinblick auf den TGIC-Service geschuldete Vergütung und ggf. weitere Servicespezifische Details.

Setzen Sie sich gerne bei Interesse mit unserem TGIC-Support in Verbindung.

4 TGIC - Systemkontext

4.1 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 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.

4.2 User Agent

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.

4.3 Akteure

4.3.1 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.

4.3.2 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.

4.4 Schnittstellen

4.4.1 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.

4.4.2 TGIC-Nutzerverwaltung

Über einen Zugang zum GDV-Netz steht OrganisationsVerwaltern 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.

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

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

4.4.3 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 dafür die Folgenden:

- 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).
  HINWEIS: Dieser wurde im Rahmen der Nutzerregistrierung X.509 als Authentifizierungsverfahren aktiviert, wodurch die PKI ein privater Schlüssel und ein öffentliches Zertifikat generiert und in Form eines Schlüsselspeichers dem Nutzer zum Download bereitstellt.
- Bereitstellung der jeweils aktuellen Certificate Revocation List (CRL) des ITC (https://pki.tgic.de/TGIC-PKI/TGIC-CA.crl).

5 Typische Anwendungsfälle

5.1 Anlegen eines TGIC-Benutzerkontos

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

Dabei haben Sie die Möglichkeit folgende Varianten Auszuführen:

- Anlegen eines Benutzerkontos als natürliche Person mit mTAN-Authentifizierung
- Anlegen eines Benutzerkontos als natürliche Person mit TOTP-Authentifizierung
- Anlegen eines Benutzerkontos als natürliche Person mit VU-Auth Authentifizierung
- Anlegen eines Benutzerkontos als natürliche Person mit nPA (eID) Authentifizierung
- Anlegen eines Benutzerkontos als natürliche Person mit verschiedenen Möglichkeiten der folgenden Authentifizierungen (mTAN, TOTP, VU-Auth & nPA)
- Anlegen eines Benutzerkontos als technischer Nutzer mit X.509-Authentifizierung

Eine detaillierte Beschreibung dazu finden Sie in der Bedienungsanleitung zur TGIC-Nutzerverwaltung

5.2 Bearbeitung des TGIC-Benutzerkontos

Sie können als OrganisationsVerwalter die Stammdaten der Nutzerkonten Ihrer Organisation verwalten. Neben den Stammdaten können Sie dem Nutzerkonto Kategorien sowie Berechtigungsrollen zuordnen. Weiter können sie Änderungen an den Authentifizierungsverfahren vornehmen.

Eine detaillierte Beschreibung der Änderungsmöglichkeiten finden Sie in der Bedienungsanleitung zur TGIC-Nutzerverwaltung

5.3 TGIC-Kennwort ändern/zurücksetzen

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 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.

Hinweis

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

Das Initialkennwort, das bei der Registrierung vergeben wird, hat für Organisationsverwalter immer 12 Zeichen und für Organisationsnutzer immer 8 Zeichen. Das Kennwort kann jederzeit geändert werden, folgende Richtlinien sind dabei zu berücksichtigen:

Folgende Regeln für die Vergabe und Änderung von Kennwörtern gelten:

für OrganisationsNutzer und SelbstPfleger

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 Sonder-zeichen 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.

für OrganisationsVerwalter

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 Sonder-zeichen 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.

5.4 Zurücksetzung des TGIC-Kennwortes

OrganisationsVerwalter haben die Möglichkeit, über das GDVnetz 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.

5.5 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.

5.6 Neuausstellung von X.509-Zertifikaten

X.509-Zertifikate haben eine Maximalgültigkeit von 400 Tagen 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.

Ein X.509-Zertifikat und ein regelmäßiger Austausch des Zertifikats ist nur für Nutzer der Webservice-Schnittstellen 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.

b) Das Zertifikat wurde nicht innerhalb von 30 Tagen nach Erhalt der Registrierungs-E-Mail heruntergeladen.

Die Neuausstellung von Zertifikaten für technische Nutzer einer Organisation kann durch einen für diese Organisation zuständigen OrganisationsVerwalter über die Web-Oberfläche der TGIC-Nutzerverwaltung erfolgen.

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 OrganisationsVerwalter, der die Neuausstellung des X.509-Zertifikats über die TGIC-Nutzerverwaltung veranlasst hat, eine E-Mail mit einem „Download-Kennwort“ versendet, welches für das Herunterladen des neuen X.509-Zertifikats benötigt wird. Das Download-Kennwort verliert nach der Aktivierung des X.509-Zertifikates seine Gültigkeit.

Eine detaillierte Beschreibung finden Sie in der Bedienungsanleitung zur TGIC-Nutzerverwaltung.

Neuausstellung des X.509 Zertifikates über den TGIC Support

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

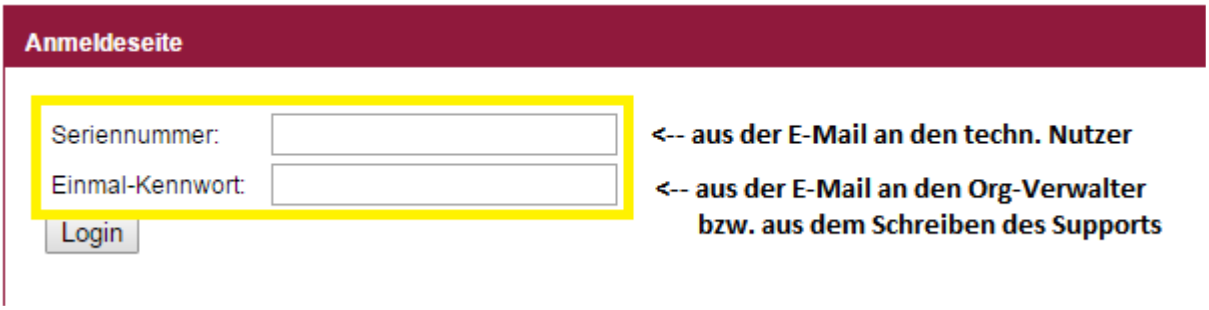
5.7 X.509-Zertifikats-Download

Über die Public Key Infrastruktur (PKI) (LINK: https://pki.tgic.de/TGIC-PKI/index.html) können die Verwalter der technischen Nutzer das X.509-Zertifikat herunterladen. Den Link finden diese ebenfalls in der Informationsmail der TGIC.

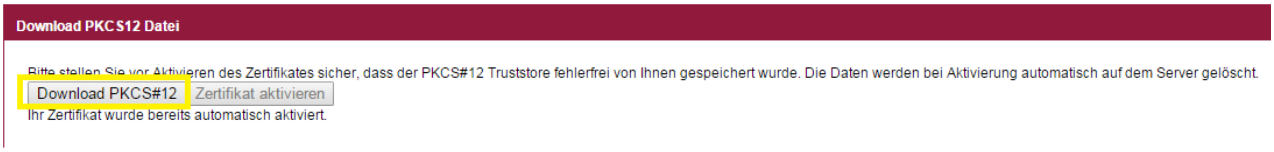
Nach Aufruf des Links für das Herunterladen des neuen X.509-Zertifikats im Webbrowser ist dort die obere Schaltfläche „Download“ auszuwählen:



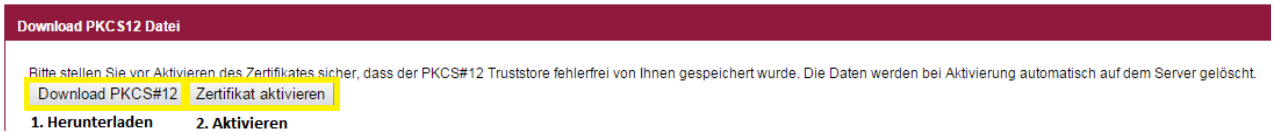
In der danach angezeigten Anmeldemaske sind dann die via E-Mail bzw. auf dem Postweg erhaltenen Daten einzugeben:



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 anschließender 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).

5.8 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.

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.

OrganisationsNutzer können nur von einem Verwalter der entsprechenden Organisation suspendiert oder reaktiviert werden. Der OrganisationsVerwalter muss dafür mindestens die Partnerrollen des OrganisationsNutzers 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.